Лирекс БГ ООД
1712 София, ж.к. Младост 3, бл. 306
Телефон: 02/ 9 691 691, Факс: 02/ 9 691 692
www.lirex.bg

ЕИК: 121057952
Банка: Алианц Банк България АД
IBAN: BG46BUIN95611010007719

П Р Е Д Л О Ж Е Н И Е З А И З П Ъ Л Н Е Н И Е

на обществена поръчка с предмет:

„Поддръжка на локална информационна инфраструктура на МТСП и Единната комуникационна инфраструктура на Министерството на труда и социалната политика и структурните звена“

Възложител: МИНИСТЕРСТВО НА ТРУДА И СОЦИАЛНАТА ПОЛИТИКА /МТСП/

гр. София
2019 г.

Лирекс БГ ООД
1712 София, ж.к. Младост 3, бл. 306
Телефон: 02/ 9 691 691, Факс: 02/ 9 691 692
www.lirex.bg

ЕИК: 121057952
Банка: Алианц Банк България АД
IBAN: BG46BUIN95611010007719

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

ЛИРЕКС БГ

По Образец № 2

ПРЕДЛОЖЕНИЕ ЗА ИЗПЪЛНЕНИЕ НА ПОРЪЧКАТА

от Манол Илиев (име и фамилия), представител на „Лирекс БГ" ООД (изписва се наименованието на участника), 121057952 (ЕИК), Република България, 1712 гр. София, жк. „Младост 3", бл. 306, вх. 2, тел.: 02 / 9691691, факс: 02 / 9691692, e-mail: office@lirex.bg (адрес на управление, тел., факс, e-mail)

УВАЖАЕМИ ГОСПОЖИ И ГОСПОДА,

С настоящото Ви представяме нашето предложение за изпълнение на обществена поръчка с предмет: **„Поддръжка на локална информационна инфраструктура на МТСП и Единната комуникационна инфраструктура на Министерството на труда и социалната политика и структурните звена"**

1. Заявяваме, че ще изпълним поръчката в съответствие с всички нормативни изисквания за този вид дейност, както и в съответствие с изискванията на възложителя, посочени в техническата спецификация, обявлението и документацията за възлагане на обществената поръчка.

2. При изпълнение на услугите се задължаваме да изпълняваме следните изисквания:

2.1. При необходимост да предоставяме указания и инструкции за инсталация и конфигуриране на специфичен за услугата приложен софтуер.

2.2. Дейностите по поддръжката ще включват и предоставяне при необходимост на консултантска помощ и експертна подкрепа за бъдещо технологично развитие.

2.3. Срокове за предоставяне на услугата/ите са съгласно техническата спецификация на възложителя

3. Заявяваме, че разполагаме с Help Desk система с гарантирана възможност за 24 часово приемане на заявки от оторизирани от възложителя лица, чрез всички изброени средства: web, e-mail и телефон, за която прилагаме описание.

4. За предоставянето и управлението на информационно-комуникационни услуги ще осигурим присъствие (на място на адрес гр. София, ул. "Триадица" № 2) на 2 техническа лица в рамките на работното време на МТСП, които да извършват консултации от типа HelpDesk и да подпомагат министерството при възникнали проблеми с информационната и комуникационна инфраструктура на МТСП.

5. Декларираме, че представляваното от мен дружество е ~~Global Gold,~~ Gold ~~или Premier~~ партньор на производителя на мрежовото оборудване Cisco, чиито продукти подлежат на поддръжка в настоящата процедура. Партньорството е видно от https://locatr.cloudapps.cisco.com/WWChannels/LOCATR/openBasicSearch.do (посочва страница/сайт на производителя, и/~~или се описва и прилага~~ заверено копие на партньорски сертификат ~~или друг еквивалентен документ от производителя, удостоверяващ изискването~~). Прилагаме сертификат за партньорство, както и оторизационно и сертификационно писмо от производителя Cisco.

6. Декларираме, че прилагаме система за управление на информационни услуги с обхват на сертификация, сходен с предмета на настоящата обществена поръчка, по стандарт ISO 20000-1:2011 ~~или еквивалентен~~, за установяване на което прилагаме заверено копие на валиден сертификат.

7. Декларираме, че прилагаме система за управление на сигурността на информацията с обхват на сертификация, сходен с предмета на настоящата обществена поръчка, по стандарт ISO 27001:2013 ~~или еквивалентен~~, за установяване на което прилагаме заверено копие на валиден сертификат.

8. Декларираме, че сме запознати напълно с всички условия и обстоятелства, необходими за изпълнение на обществената поръчка и приемаме да изпълним поръчката изцяло съобразно техническата спецификация на възложителя, приложена към документацията на обществената поръчка.

За ...: Радостина Маринова

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

9. Декларираме, че при изготвяне на офертата са спазени задълженията, свързани с данъци и осигуровки, опазване на околната среда, закрила на заетостта и условията на труд.

10. За обезпечаване изпълнението на задълженията си по договора за възлагане на обществената поръчка, преди подписването на договора ще предоставим на Възложителя гаранция за изпълнение в размер на 5% (пет на сто) от стойността на договора без ДДС при условията посочени в документацията за обществена поръчка.

Приложения:

1. Описание на Help Desk система – Приложение № 1;
2. Описание на функционалността на системата за on-line приемане и обработка на сервизни заявки / обслужване на клиенти https://portal.lirex.com – Приложение № 1.1
3. Заверени копия на партньорски сертификат и оторизационно писмо от производителя Cisco.
4. Заверени копия на сертификати по стандарт EN ISO 27001:2013 ~~или еквивалентен~~ за управление на сигурността на информацията и по стандарт EN ISO 20000-1:2011 ~~или еквивалентен~~ за управление на информационни услуги.
5. Описание на услугите (дейностите), съгласно техническа спецификация на Възложителя – Приложение №2
6. Предложение за управление изпълнението на поръчката – Приложение № 3
7. Предложение на план за управление на услугите – Приложение № 4
8. Предложение за управление на риска – Приложение № 5

Дата: 27.09.2019 г.
Гр. София
Място и дата на издаване

Подпис, печат: [redacted]

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

Манолиев
(име, длъжност)

Изготвил: В.Димитрова

Съгласувал: В.Стоев

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

Лирекс БГ ООД
1712 София, ж.к. Младост 3, бл. 306
Телефон: 02/ 9 691 691, Факс: 02/ 9 691 692
www.lirex.bg

ЕИК: 121057952
Банка: Алианц Банк България АД
IBAN: BG46BUIN95611010007719

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

ЛИРЕКС БГ

Приложение № 1
към Техническо предложение

Описание на Help Desk системата на „Лирекс БГ“ ООД

Лирекс БГ разполага с Център за помощ (Help Desk), където Възложителят да регистрира възникването на инцидент, чрез подаване на заявка по електронна поща, регистрация в електронна система, телефон или факс. Ползването на телефонните и факс услуги няма да поставя Възложителя пред необходимост да заплаща разговори по международни тарифи и тарифи на услуги с добавена стойност.

1.1. Център за връзка

Центърът за помощ (Help Desk) осигурява първо ниво на поддръжка на клиентите чрез екип от администратори и инженери. Центърът за връзка организира ескалацията на проблемите и решенията.

Центърът за връзка е наличен 24 часа в денонощието, 7 дни в седмицата, 365 дни в годината.

Служителите на дружеството в центъра за връзка са висококвалифицирани професионалисти с богат опит.

Центърът за връзка се грижи за по-голямата част от процесите на управление на инциденти, но също така е отговорен и за:

- Приемането и проследяването на съобщения за инциденти, повреди или въпроси от клиенти, по този начин се гарантира, че няма загуба на инциденти и заявки.
- Извършва първоначална класификация, за да гарантира, че инцидентите са с правилния приоритет и по тях работи точният ресурс.
- Проучване и диагностика на инцидентите.
- Решаване и затваряне на инцидента и вписване на решението, което е приложено в базата данни.

Процесите в центъра за връзка се покриват от два основни потока:

1. Получаване на информация от клиента чрез:
   - Стационарен телефон.
   - Мобилен телефон.
   - Факс.
   - Електронна поща (e-mail).
   - Автоматизирана система за online приемане и обработка на сервизни заявки.
   - Друг начин (среща с клиента).

Специалистите от центъра за връзка събират информация с цел да идентифицират лицето от страна на клиента (име, отдел, местоположение). На тази фаза първоначалната идентификация на получената информация е направена. Информацията може да бъде:

- Съобщение за нов проблем - Специалистът отваря нов случай и започва да го анализира.
- Допълнителна информация за вече отворен инцидент - Новата информация се добавя към текущата за случая в проследяващата система.
- Друга информация или обратна връзка - В този случай екипът предава информацията на ръководството за допълнителни анализи.

2. Анализ и решаване на инцидент

След като информацията е получена от клиента, центърът за връзка определя вида на инцидента, приоритета, съгласуваните нива на обслужване и проверява за вече документирана процедура за решаване на случая. Ако няма такава и решението на случая е извън обхвата на знания на инженерите, се осведомяват вътрешните експерти в съответствие с процеса на управление на вътрешната ескалация.

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

След като решението се разработи и тества, то се документира във вътрешната база данни, с цел да се предотврати повторното му решаване, при възникване на същия инцидент.

1.2. Център за обслужване

Центърът за обслужване работи в тясна връзка с центъра за връзка и поема грижата за цялостната поддръжка на заявките или графици, както и разпределението им по райони.

Дружеството разполага с обслужваща мрежа в цялата страна – **София, Варна, Пловдив, Русе, Бургас, Габрово, Стара Загора, Козлодуй, Девня, Плевен.**

Тази обслужваща инфраструктура позволява покритие върху цялата територия на страната и гарантира централизирано управление на всички ресурси, с цел да се удовлетворят нуждите на клиентите.

Освен стандартното работно време на поддръжка – 5 дни в седмицата, 9 часа в денонощието. В случай на необходимост дружеството предлага поддръжка 7 дни в седмицата, 24 часа в денонощието и с време за реакция до 1 час и реакция на място до 4 часа в цялата страна.

В центъра за обслужване работят добре обучени специалисти, с голям опит и сертифицирани според високите стандарти на лидерите в световните ИТ технологии.

1.3. Система за обслужване на клиенти

Услугите по обслужване на заявки за интервенции или разрешаване на инциденти се изпълняват след регистриране на заявка/инцидент в Web-базираната система на дружеството (описание на системата и начина на работа с нея са представени в Приложение№ 1.1) или чрез свързване по някой от комуникационните канали с Центъра за обслужване на клиенти. Всяка интервенция приключва с отчет, който се изпраща на клиента автоматично от системата при затварянето на заявката/инцидента.

Отчетът на интервенцията съдържа следната информация:

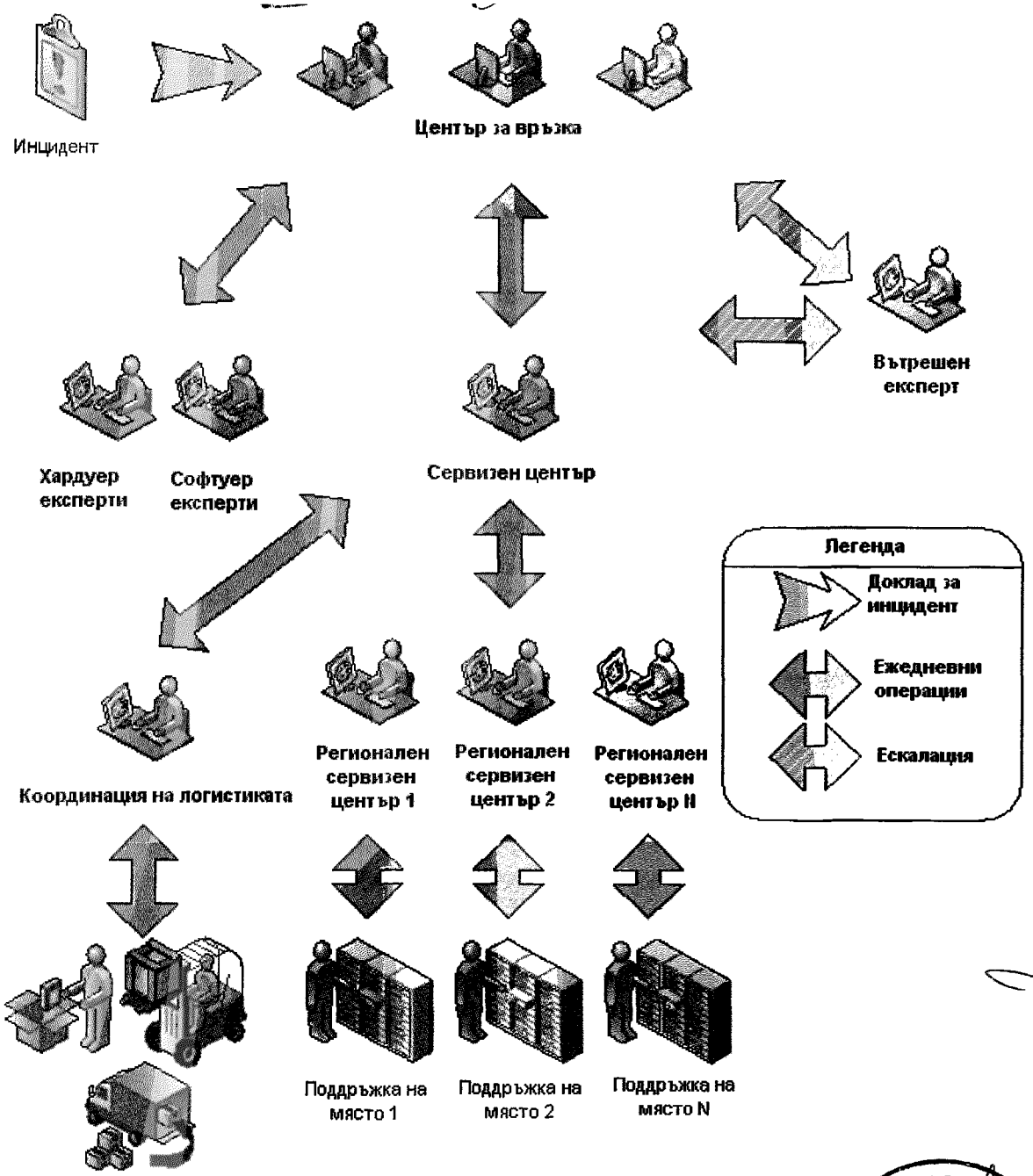
- Детайли от нотификацията за заявката / инцидента:
  - Име на заявителя от МТСП;
  - Дата и час на заявката;
  - Първоначално описание на инцидента.
- Детайли от реакцията на центъра за обслужване:
  - Дата и час на отдалечената реакция / Дата и час на пристигане на място;
  - Диагностициран проблем;
  - Причина за инцидента.
- Приложено решение / workaround.
- Описание на установени неработещи части, включително:
  - Описание на устройството;
  - Тип;
  - Сериен номер / продуктов номер.
- Препоръки от сервизния специалист на дружеството относно възможности за бъдещо предотвратяване на повторен инцидент.
- Дата и час на разрешаване на инцидента.

1.4. Организация на поддръжката между отделните звена

Организацията на поддръжката в Лирекс БГ и връзките между звената – център за връзка, сервизен център и хардуерни и софтуерни експерти е представена на графиката долу:

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679



Дата: 27.09.2019 г.
Гр. София
Място и дата на издаване

Подпис, печат:

ЛИРЕКС БГ ООД

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

Манол Илиев
(име, длъжност)

Изготвил:В.Димитрова

Съгласувал: В.Стоев

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

Лирекс БГ ООД
1712 София, ж.к. Младост 3, бл. 306
Телефон: 02/ 9 691 691, Факс: 02/ 9 691 692
www.lirex.bg

ЕИК: 121057952
Банка: Алианц Банк България АД
IBAN: BG46BUIN95611010007719

Приложение№ 1.1
към Техническо предложение

ОПИСАНИЕ НА ФУНКЦИОНАЛНОСТТА НА СИСТЕМАТА ЗА ON-LINE ПРИЕМАНЕ И ОБРАБОТКА НА СЕРВИЗНИ ЗАЯВКИ / ОБСЛУЖВАНЕ НА КЛИЕНТИ https://portal.lirex.com

за участие в открита процедура за възлагане на обществена поръчка с предмет:

„Поддръжка на локалната информационна инфраструктура на МТСП и Единната комуникационна инфраструктура на Министерството на труда и социалната политика и структурните звена“

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

Съдържание

ИЗИСКВАНИЯ ЗА ИЗПОЛЗВАНЕ НА ПОРТАЛА 3

РЕГИСТРИРАНЕ НА ЗАЯВКА 3

ПРОВЕРКА НА СТАТУСА НА ЗАЯВКА 4

ПРОМЯНА НА ПАРОЛАТА 5

ИЗХОД ОТ СИСТЕМАТА 6

МЕНЮ „СПОДЕЛЕНИ ДОКУМЕНТИ“ 6

МЕНЮ „СНИМКИ“ 7

МЕНЮ „КОНТАКТИ“ 8

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

Изисквания за използване на портала

Изискванията за използване на Портала за клиенти се определят от използвания продукт - SharePoint Server 2013. Порталът има възможност да се използва със следните уеб браузъри:

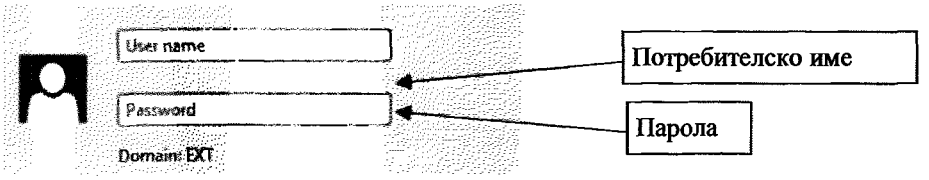
- **Уеб браузъри от ниво 1** - уеб браузърите от ниво 1 имат достъп до разширените функции, предоставяни от ActiveX контроли, и предлагат най-обширни възможности за работа. Браузърите от ниво 1 предлагат пълна функционалност на всички сайтове на SharePoint Server 2013.
  - Windows клиент с **Internet Explorer 8**, **Internet Explorer 9**, **Internet Explorer 10** или **Internet Explorer 11**
- **Уеб браузъри от ниво 2** - уеб браузърите от ниво 2 предлагат основна функционалност, така че потребителите да могат да четат и пишат в сайтовете на SharePoint Server 2013. Но тъй като ActiveX контролите се поддържат само в браузъри от ниво 1 и поради различията във функциите на различните браузъри, работата на потребителите може да е различна и може да има различия спрямо работата с браузъри от ниво 1.
  - Windows клиент с Mozilla Firefox (latest released version) или Google Chrome (latest released version)
  - Unix/Linus с Mozilla Firefox (latest released version) или Google Chrome (latest released version)
  - Mac OS-X с Mozilla Firefox (latest released version) или Google Chrome (latest released version) или Apple Safari (latest released version)

Въпреки че потребителските задачи на сайтовете на SharePoint Server 2013 са оптимизирани за браузъри от ниво 1, SharePoint Server 2013 предоставя също поддръжка за други често използвани браузъри. За да сте сигурни, че имате пълен достъп до всички функции, препоръчваме да използвате браузър от ниво 1.

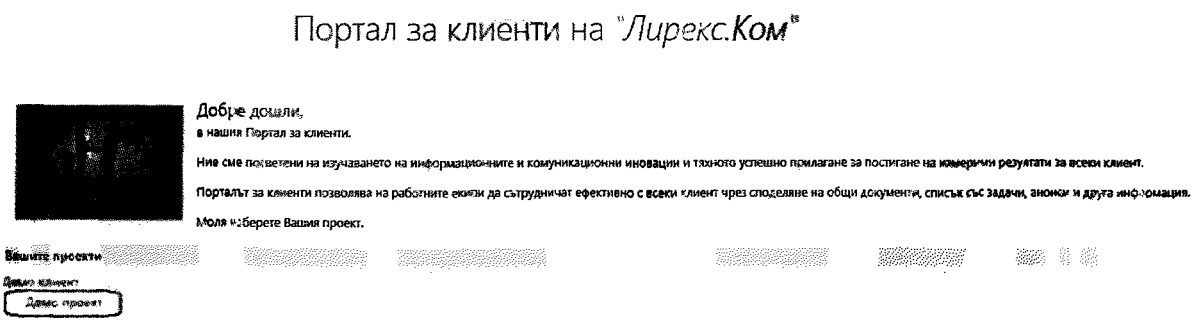
Ако браузърът не е нито в списъка на ниво 1, нито в този на ниво 2, то той не се поддържа!

Регистриране на заявка

1. Въведете потребителско име и парола на началната страница https://portal.lirex.com .

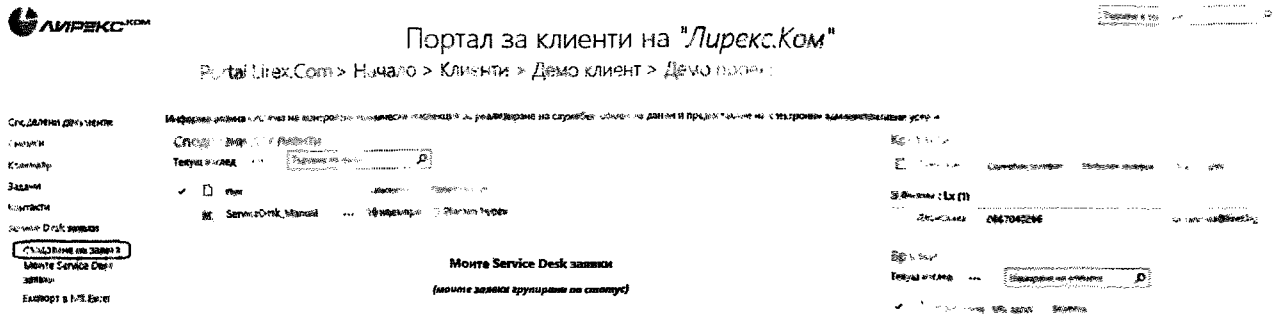


2. Изберете Вашия Проект

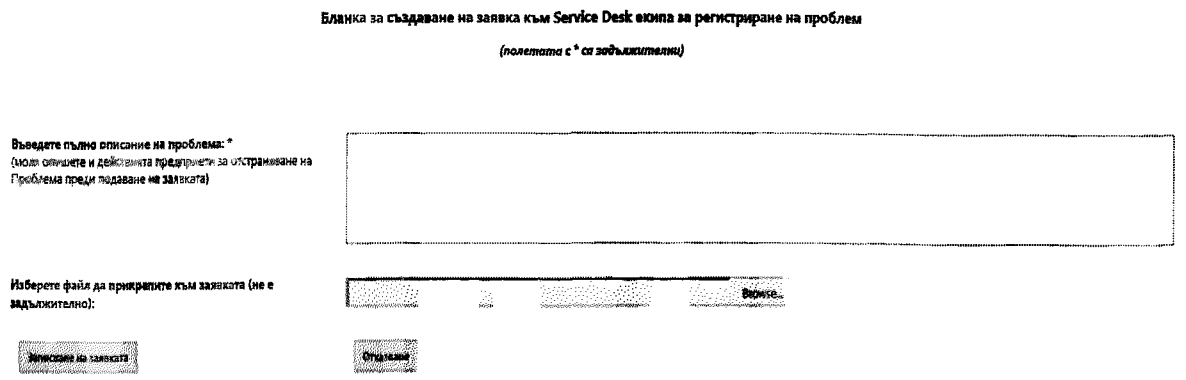


3. Изберете **Създаване на заявка** от менюто вляво.

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

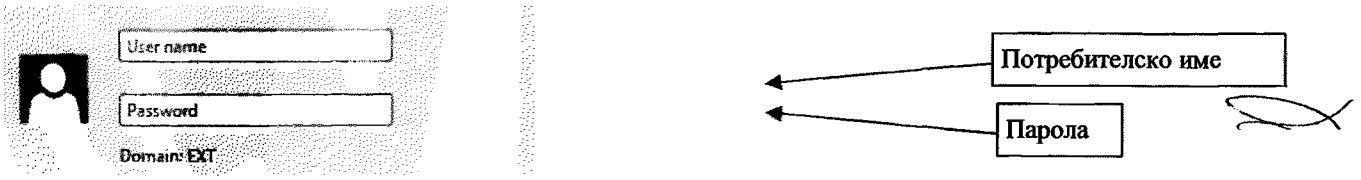


4. Въведете **Описание на проблема** и изберете **Записване на заявката**.

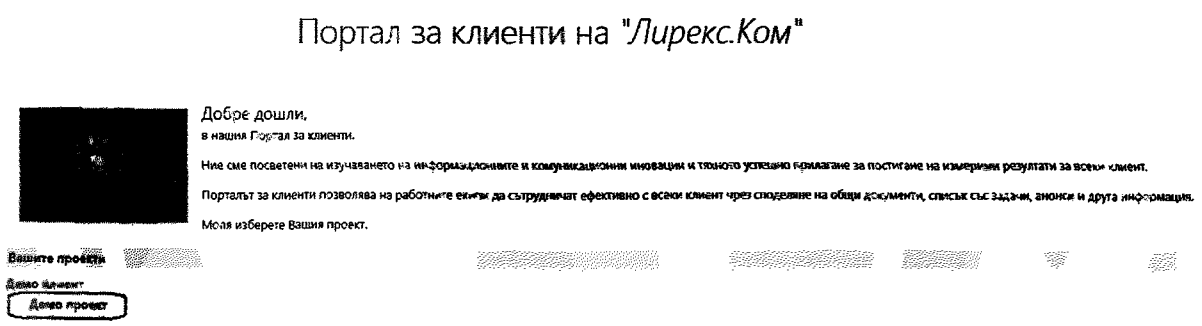


Проверка на статуса на заявка

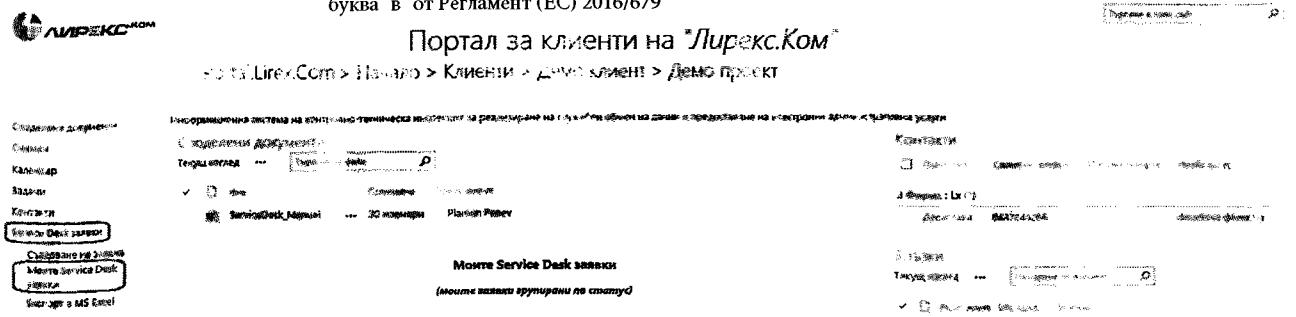
1. Въведете потребителско име и парола на началната страница https://portal.lirex.com .



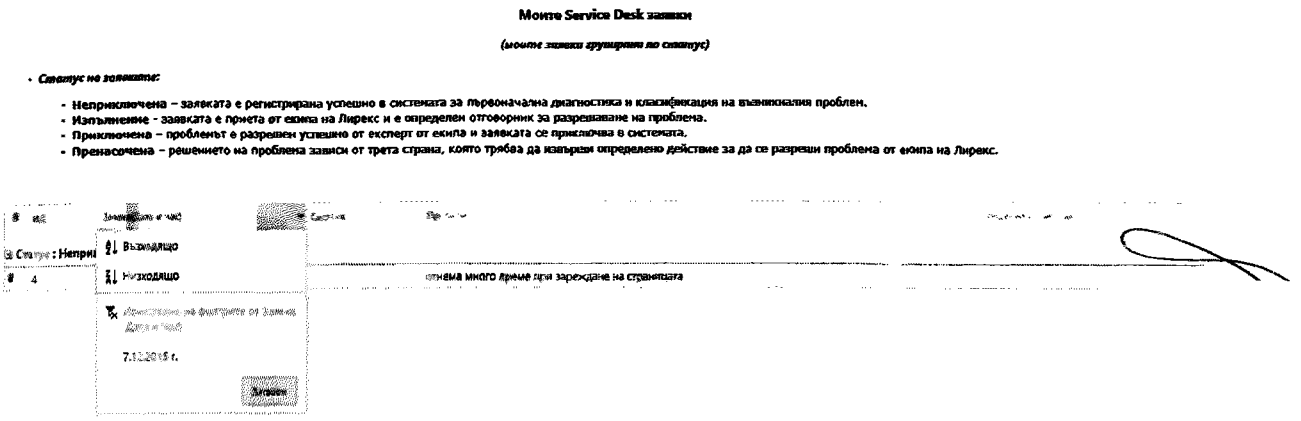
2. Изберете Вашия Проект



3. Изберете **Моите Service Desk заявки** или **Service Desk заявки** за всички заявки.

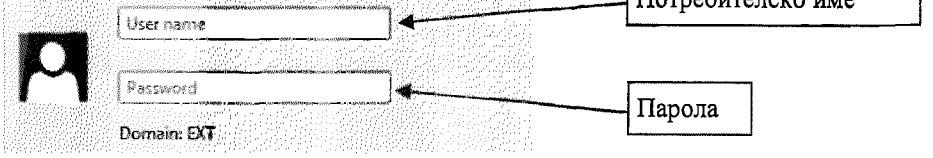


4. Изберете заглавието на колоната, за да сортирате или филтрирате по определена стойност. Заявките са групирани по статус:
   - **Неприключена** – заявката е регистрирана успешно в системата за първоначална диагностика и класификация на възникналия проблем.
   - **Приключена** – проблемът е разрешен успешно от експерт от екипа и заявката се приключва в системата.
   - **Пренасочена** – решението на проблема зависи от трета страна, която трябва да извърши определено действие за да се разреши проблема от екипа на Лирекс.

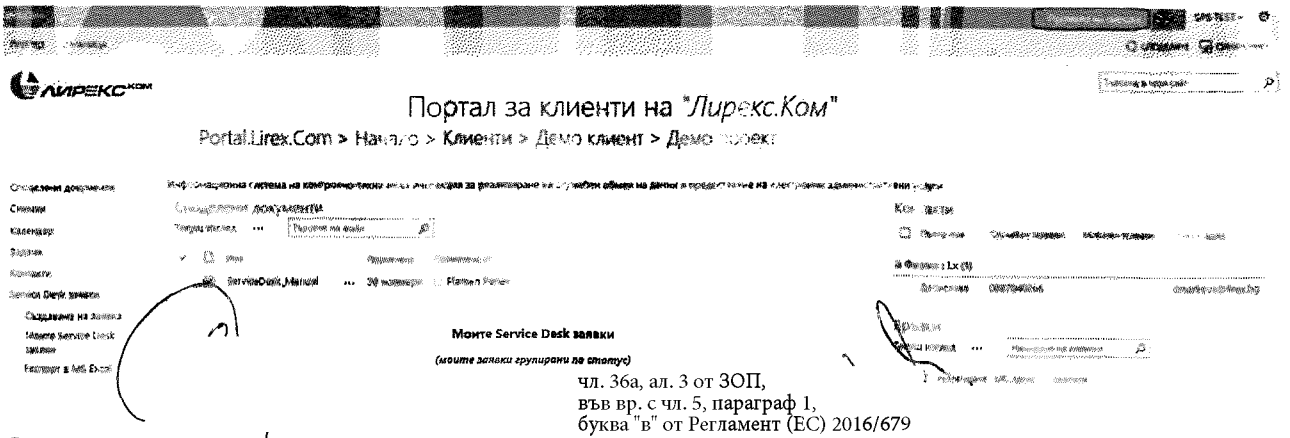


Промяна на паролата

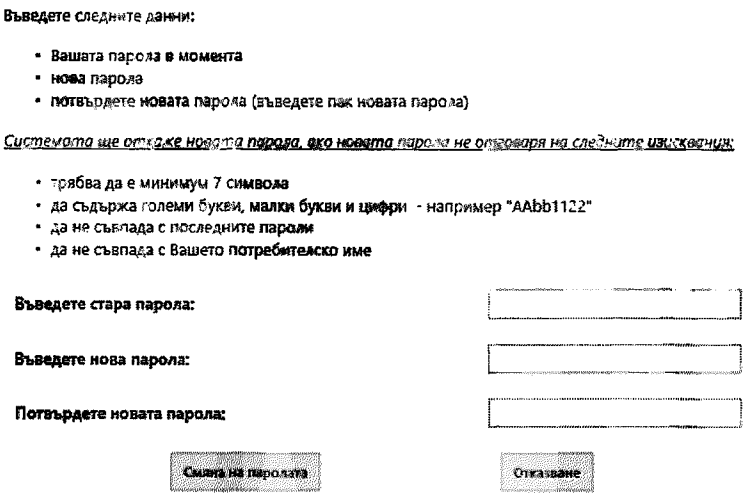
1. Въведете потребителско име и парола на началната страница https://portal.lirex.com .



2. Изберете **Промяна на парола**.



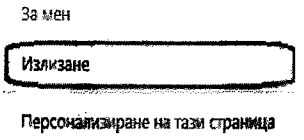
3. Въведете **стара парола, нова парола, потвърдете новата парола** и изберете **Смяна на паролата.**



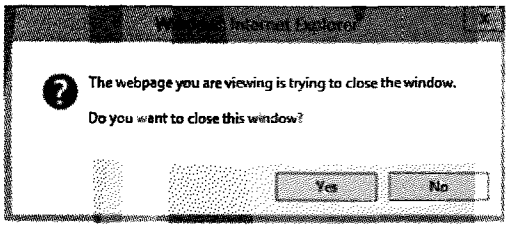
Изход от системата

1. Изберете **Вашето име** от горния десен ъгъл.

2. След това изберете **Излизане**.



3. Изберете **Yes**.

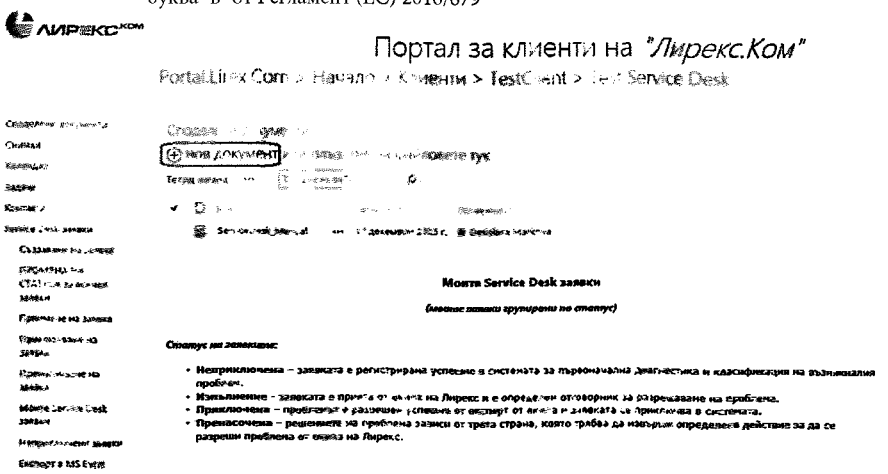


Меню „Споделени документи“

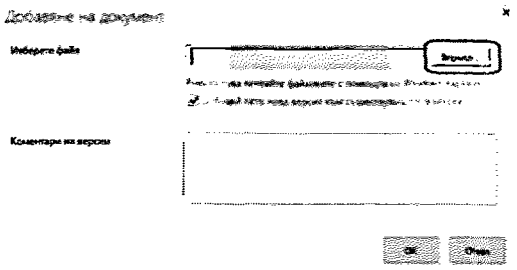
Меню „Споделени документи“ предоставя на потребителите възможност да ъплоудват и споделят с останалите потребители на портала за регистриране на заявки различни типове документи, общи за проекта.

Споделяне на документи:

1. Изберете секция „**Споделяне на документи**“ от лявото навигационно меню;
2. Изберете електронната препратка „**Нов документ**“



3. В диалоговия прозорец маркирайте бутон **"Browse"** и изберете документа, който желаете да приложите.



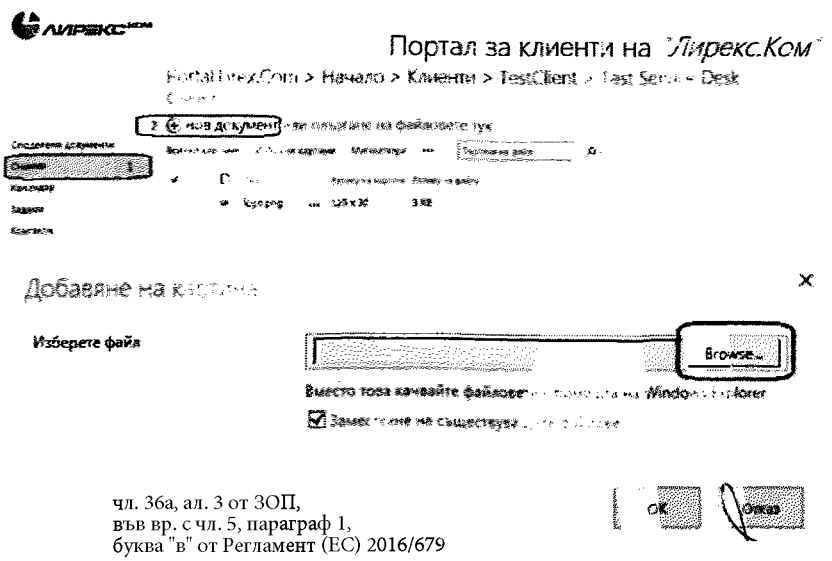
4. Потвърдете Вашия избор с бутон **„ОК"**

5. Ако желаете да откажете ъплоуда, натиснете бутон **„Отказ"**

Меню „Снимки"

За да приложите снимки към проекта на портала е необходимо да:

1. Изберете секция **„Снимки"** от лявото навигационно меню;
2. Системата позволява да приложите снимки по два начина:
   2.1. Чрез клик с десния бутон на мишката върху електронна препратка „Нов документ" и последващ избор на файл, който желаете да прикачите;



2.2. Чрез приплъзване на избрания от Вас файл с мишката в текущата страница „Снимки"

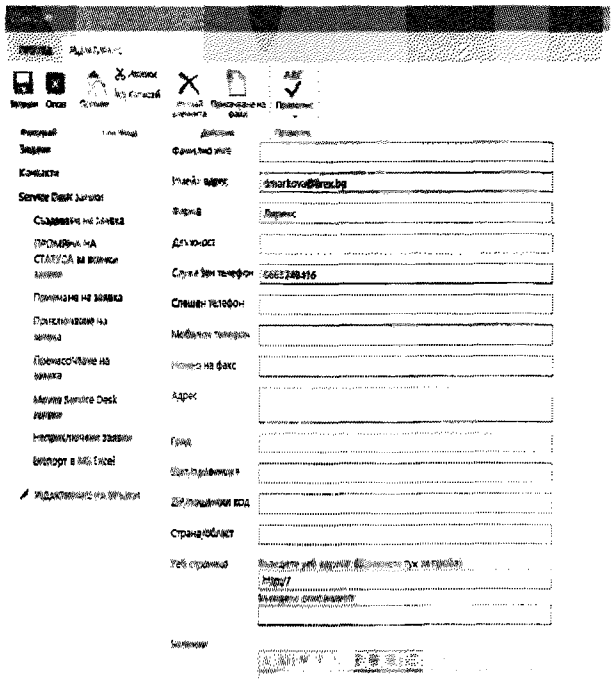
Меню „Контакти"

Меню „Контакти" предоставя на потребителите възможност за бърз достъп до детайлно описание на комуникационните канали, използвани при реализацията на проектите;

По подразбиране, контактите на участниците в проекта са обособени в отделни групи.

Добавяне на контакти

1. За да добавите нов контакт, е необходимо да изберете електронна препратка „Добавяне на нов елемент".
2. На екрана се визуализира форма, в която да попълните информацията, с която разполагате (име на лицето, имейл адрес, организация/фирма, длъжност, телефони за контакт (в т. число спешен, служебен, мобилен, личен, номер на факс, адрес, уеб адрес и друга индивидуализираща информация) или да прикачите файл, в случай на необходимост.

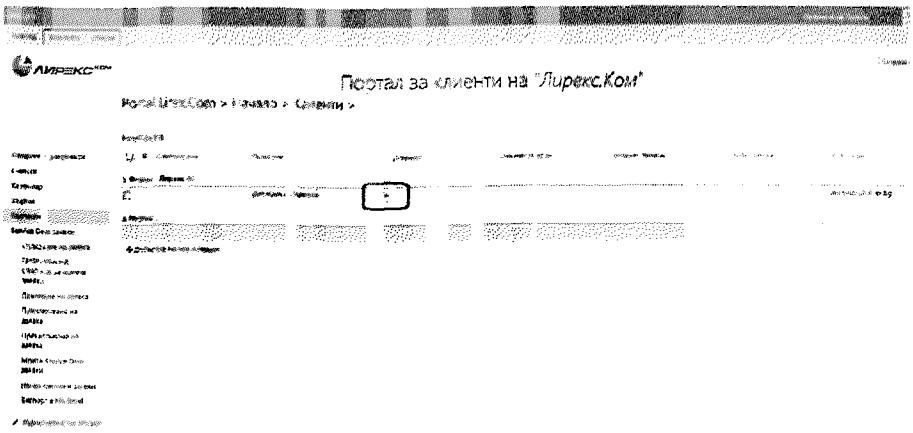


3. Потвърждаването/отхвърлянето на текущо въведената информация се осъществява от бутони „Запис/Отказ"

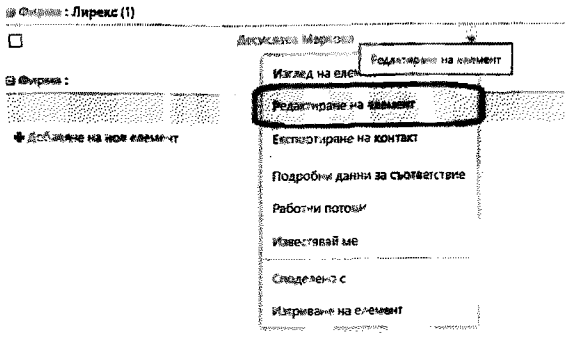
Редактиране на контакти

1. За да редактирате вече въведен в системата контакт е необходимо да маркирате същия с мишката и да изберете бутон „**Стрелка**", разположен непосредствено до името на лицето.

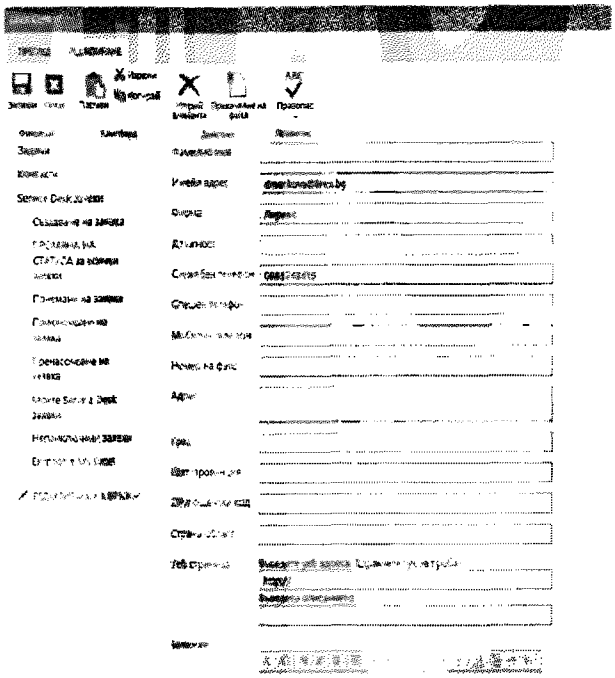
чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679



2. От падащото навигационно меню изберете „**Редактиране на елемент**“

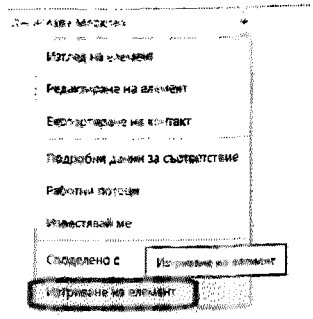


3. На екрана се визуализира формата за контакти, в която можете да отразите и потвърдите желаните от Вас корекции чрез клик върху бутон „Запис“.

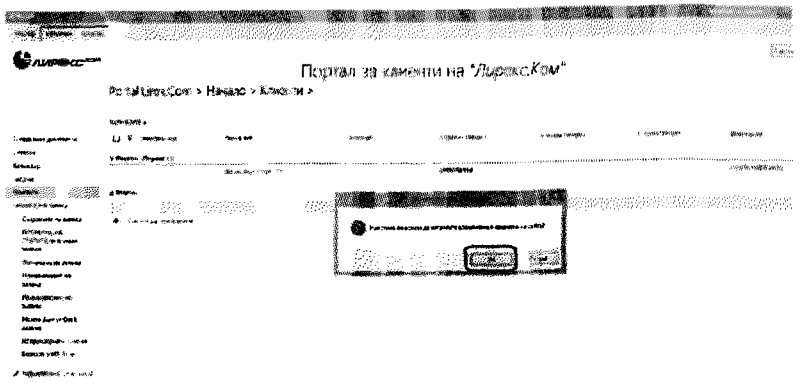


Заличаване на контакт

1. За да заличите вече въведен в системата контакт е необходимо да маркирате същия с мишката и да изберете бутон „**Стрелка**“, разположен непосредствено до името на лицето.
2. От падащото навигационно меню изберете „**Изтриване на елемент**“

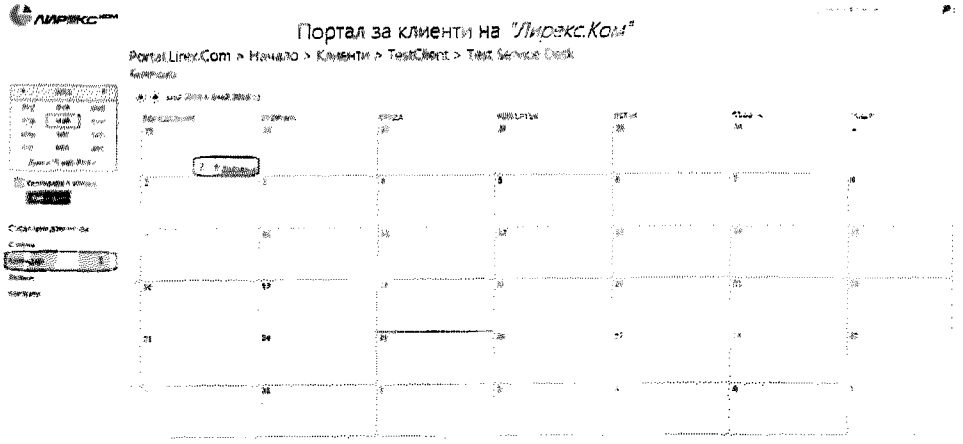


3. Потвърдете заличаването с избор на бутон „**ОК**“

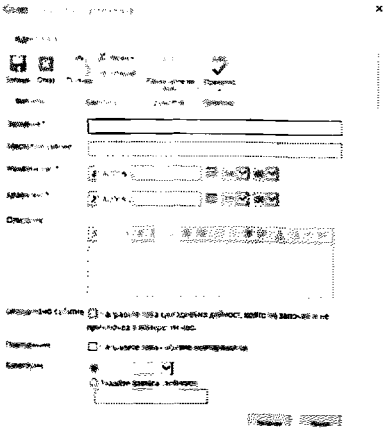


Меню „Календар“

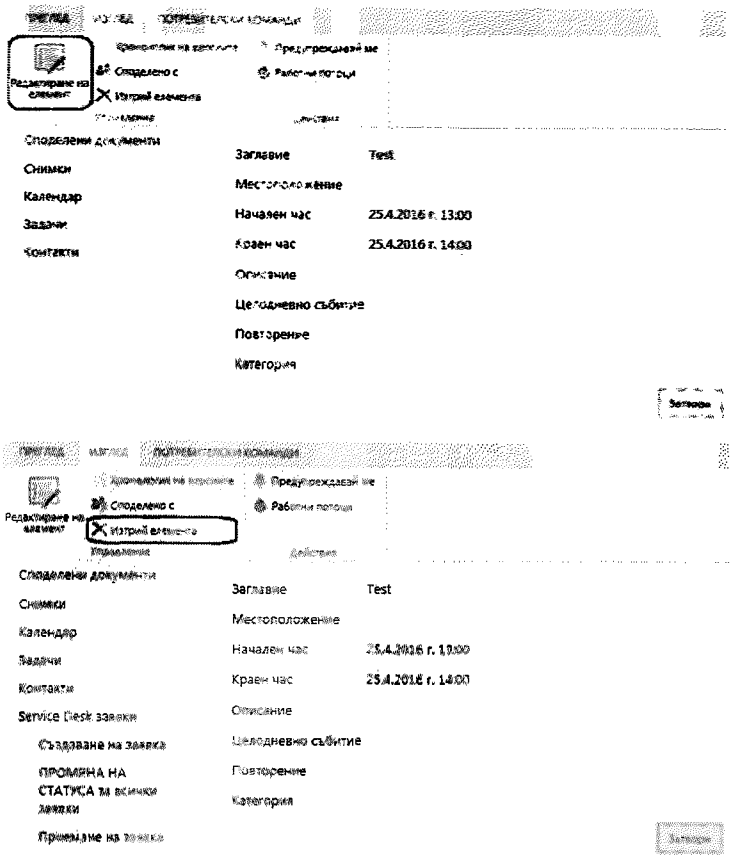
1. За да въведете събитие в календара на проекта следва да използвате меню „Календар“ от дясното навигационно меню и маркирайте електронна препратка „Добави“, разположена в долния десен ъгъл на избрания от Вас ден.



2. Въведете информацията за събитието (заглавие, местоположение, време на провеждане, а при необходимост и повтаряемост) и потвърдете информацията с клик върху бутон „**ОК**“



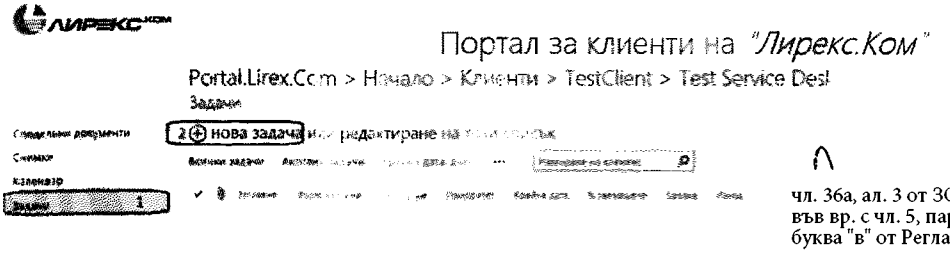
3. За да редактирате или заличите въведена информация за събитие от календара, кликнете с десния бутон на мишката върху същото и изберете съответното действие от хоризонталното навигационно меню.



Меню „Задачи“

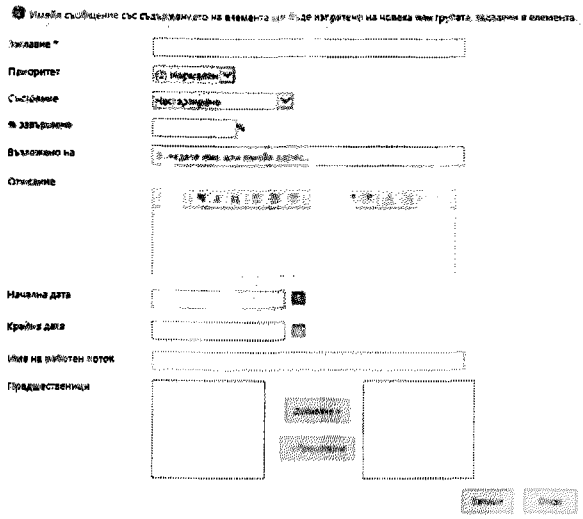
Меню „Задачи“ предоставя възможност на потребителите на портала да създават задачи към проекта, да определят техни отговорници и да следят статуса им на изпълнение.

1. За да създадете нова задача изберете последователно секция „Задачи“ от лявото навигационно меню и електронна препратка „Нова задача“.

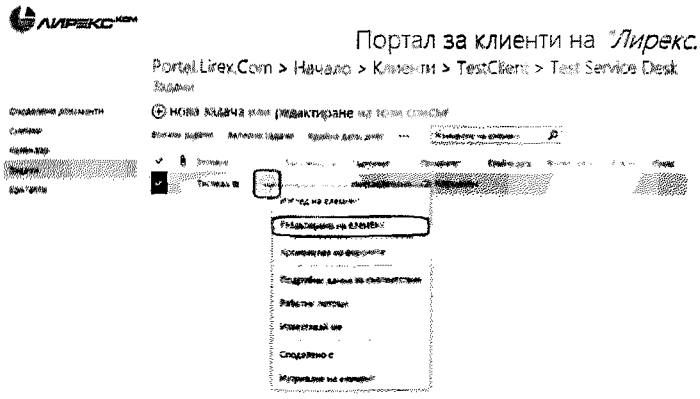


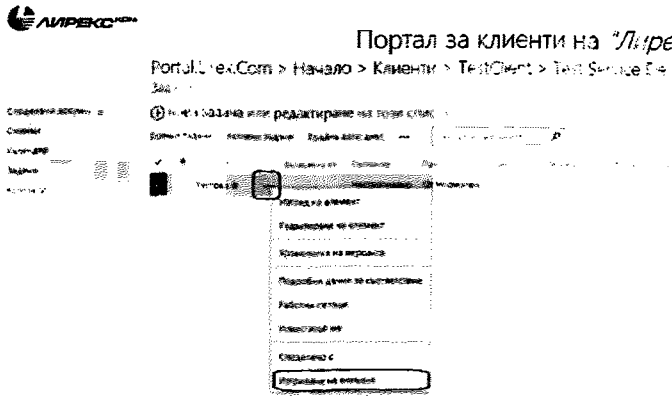
чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

2. Във формата въведете информация за наименование на задачата, описание, приоритет, срок за изпълнение и др.



3. Редакцията/заличаването на създадена задача се осъществява след маркиране на същата от списъка със задачи, клик с десния бутон на мишката върху меню „...“ и изберете съответното действие – редактиране/заличаване





Дата: 27.09.2019 г.
Гр. София
Място и дата на издаване

Подпис, печат: .....

Манол Илиев
(име, длъжност)

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

Изготвил: В.Димитрова

Съгласувал: В.Стоев

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

ТЕЗА ООД
ЦЕНТЪР ЗА ПРЕВОДИ

София 1784, Младост-1,54А
факс: +359 2 9 691 599
тел.: +359 2 9 691 598
office@teza.bg; www.teza.bg

TEZA

Превод от английски език

[На бланка на Cisco]

Програма за канален партньор на Сиско

[Cisco Channel Partner Program]

Сертифициран Златен Партньор

[Gold Certified Partner]

Присъден на

ЛИРЕКС БГ ООД

Югоизточна Европа

Валиден до 29 Октомври 2020

Проверете валидността на:
cisco.com/go/partnerlocator

Сиско Екосистемни Партньорски Програми
[Cisco Partner Ecosystem Programs]
Глобална Партньорска организация
[Global Partner Organization]

Удостоверявам верността на извършения от мен превод от английски на български език, на приложения документ Сертификат Валиден до 29 Октомври 2020. Преводът се състои от 1 /бр/ стр.

Преводач: Мая Танева ***подпис: ..... /печат/***

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

ТЕЗА ООД
ОФИЦИАЛЕН ПРЕВОДАЧ
TEZA
OFFICIAL TRANSLATION

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

ЛИРЕКС БГ ООД
СОФИЯ

Вярно с оригинала

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

cisco Partner

Cisco Channel Partner Program

Gold Certified Partner

Awarded to

LIREX BG LTD

SOUTH EAST EUROPE

valid until October 29, 2020

cisco Gold Partner

Validate this certificate at:
cisco.com/go/partnerlocator

Cisco Partner Ecosystem Programs
Global Partner Organization

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

Вярно с оригинала

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

ТЕЗА ООД
ЦЕНТЪР ЗА ПРЕВОДИ
София 1784, Младост-1.54А
факс: +359 2 9 691 599
тел.: +359 2 9 691 598
office@teza.bg; www.teza.bg
TEZA

Превод от английски език

Лого на Cisco

ОТОРИЗАЦИОННО ПИСМО ОТ ПРОИЗВОДИТЕЛ

Дата: **26 Септември 2019**

До: **Министерство на труда и социалната политика**

Предмет: **„Поддръжка на локална информационна инфраструктура на МТСП и Единната комуникационна инфраструктура на Министерството на труда и социалната политика и структурните звена“**

Сиско Интернешънъл Лимитед [Cisco International Limited], регистрирана в Англия и Уелс (фирмен номер 06640658), имаща основно място на дейност 9-11 Ню Скуаре Парк, Бедфонд Лайкс, Фелтам, Англия TW14 8XA, ОК [9-11 New Square Park, Bedfont Lakes, Feltham, England TW14 8HA, United Kingdom] ("Сиско"), който е доставчик на цялостни мрежови продукти и услуги, с настоящото потвърждава, че считано от датата на настоящото писмо, ЛИРЕКС БГ ООД ("Дистрибутор") желае да участва в търга или проекта, посочен по-горе и е сключило Партньорски договор за непряк канал [Indirect Channel Partner Agreement], съгласно който Дистрибуторът има право на следното:

(1) препродава и/или разпространява Cisco продукти и/или услуги в БЪЛГАРИЯ на крайните потребители в рамките на тази територия;

(2) предлага, преговаря и сключва договор с вас за гореизброените продукти/услуги, произведени или предоставени от Сиско. Дистрибуторът е независим изпълнител и няма правомощия да ангажира и/или обвързва Cisco или нейните филиали по никакъв начин.

Сиско, в рамките на обхвата на договора със своите оторизирани канали, ще осигурява поддръжка и гаранционни услуги за продуктите на Сиско, които са закупени през оторизираните дистрибутори на Сиско.

Настоящата оторизация влиза в сила от датата, посочена по-горе в писмото и е за шест (6) седмици, считано от тази дата.

Ако имате нужда от допълнителна информация, моля, не се колебайте да се свържете с Пламен Жечев на тел. +359 899 [redacted]. За повече информация за партньорската програма на Сиско, моля посетете уеб-страница: http://www.cisco.com/web/partners/index.html.

Надлежно упълномощен да подпише тази оторизация за и от името на **Сиско Интернешънъл Лимитед [Cisco International Limited]**

Подпис */не се чете/*
Джеймс Гленистър
Директор МГМТ-Финанси
Сиско Интернешънъл Лимитид [Cisco International Limited]
9-11 Ню Скуаре Парк, Бедфонд Лайкс, Фелтам, Мидълсекс, TW14 8XA, Англия

Удостоверявам верността на извършения от мен превод от английски на български език, на приложения документ/ Оторизационно писмо 26.09.2019/. Преводът се състои от 1 стр.

Преводач: Мая Танева ***подпис: /печат/***

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

ЛИРЕКС БГ ООД София

Вярно с оригинала

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

CISCO

MANUFACTURER'S AUTHORIZATION FORM

Date: **26 September 2019**

To: **Ministry of labor and social policy**

Subject: **Maintenance of MLSP Local Information Infrastructure and the Unified Communication Infrastructure of the Ministry of Labor and Social Policy and Structural Units**

Cisco International Limited, registered in England and Wales (Company Number 06640658), having a principal place of business at 9-11 New Square Park, Bedfont Lakes, Feltham, England TW14 8HA, United Kingdom ("**Cisco**"), who is a provider of networking products and services, hereby confirms that, as of the date of this letter, LIREX BG LTD ("**Reseller**") wishes to participate in the Bid or Project stated above and has entered into an Indirect Channel Partner Agreement which entitles Reseller to do the following:

(1) resell and/or distribute Cisco products and/or services in BULGARIA to end users within that territory;

(2) bid, negotiate and conclude a contract with you for the above products/services manufactured or supplied by Cisco. The Reseller is an independent contractor and has no authority to commit and/or bind Cisco or its affiliates in any way.

Cisco will, within the scope of its agreement with its authorized channels, provide support and product warranty services for Cisco products obtained through its authorized channels.

This Authorization shall be accurate as of the date appearing at the top of this letter and for six (6) weeks from such date.

If you need any additional information, please do not hesitate to contact Plamen Zhechev at +359 899 [redacted]. For more information about Cisco's channel partner program, please visit the following URL: http://www.cisco.com/web/partners/index.html.

Duly authorized to sign this authorization for and on behalf of: **Cisco International Limited**

James Glenister
DIRECTOR.MGMT-FINANCE

CISCO
Cisco International Limited
9-11 New Square Park
Bedfont Lakes, Feltham
Middlesex, TW14 8HA
United Kingdom

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

ЛИРЕКС БГ ООД
София

Вярно с оригинала

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

ТЕЗА ООД
ЦЕНТЪР ЗА ПРЕВОДИ

София 1784, Младост-1,54А
факс: +359 2 9 691 599
тел.: +359 2 9 691 598
office@teza.bg; www.teza.bg

TEZA

Превод от английски език

Лого на Cisco

ПИСМО ЗА ПАРТНЬОРСТВО /ПОКУПКА ЧРЕЗ КАНАЛ/

Дата: **26 Септември 2019**

До: **Министерство на труда и социалната политика**

Номер на офертата или име на проект: **„Поддръжка на локална информационна инфраструктура на МТСП и Единната комуникационна инфраструктура на Министерството на труда и социалната политика и структурните звена“**

Сиско Интернешънъл Лимитид [Cisco International Limited], регистрирана в Англия и Уелс (фирмен номер 06640658), имаща основно място на дейност 9-11 Ню Скуеър Парк, Бедфонд Лайкс, Фелтам, Англия TW14 8XA, Обединено Кралство [9-11 New Square Park, Bedfont Lakes, Feltham, England TW14 8HA, United Kingdom] ("Сиско") потвърждава, че към датата на настоящото писмо, ЛИРЕКС БГ ООД е Златен сертифициран партньор на Сиско и Сиско и ЛИРЕКС БГ ООД са сключили договор за покупка и препродажба на Сиско продукти и/или услуги („Договор").

Това означава, че ЛИРЕКС БГ ООД е изпълнило всички условия по процедурата по сертифициране на Сиско и е надлежно упълномощено да закупува и препродава продукти на Сиско в БЪЛГАРИЯ, както и да преговаря за условията и реда за поддръжка и обслужване на продуктите на Сиско, включително гаранционните условия, в съответствие с условията и реда за подобен Договор.

Освен това, ЛИРЕКС БГ ООД е специализирано в следните технологии на Сиско:

- Архитектурна специализация на Център за данни за напреднали [Advanced Data Center Architecture Specialization];
- Архитектурна специализация за сигурност за напреднали [Advanced Security Architecture Specialization];
- Архитектурна специализация за корпоративна мрежа за напреднали [Advanced Enterprise Networks Architecture Specialization] и
- Архитектурна специализация за съвместна работа за напреднали [Advanced Collaboration Architecture Specialization].

Моля да имате предвид, че настоящото потвърждение няма безсрочен характер, а статусът на упълномощената партньорска програма на Сиско е предмет на редовно преразглеждане. Тази информация е актуална към датата, посочена в горната част на този сертификат, и е валидна за период от 6 /шест/ седмици, считано от тази дата.

Ако имате нужда от допълнителна информация, моля, не се колебайте да се свържете с Пламен Жечев на тел. +359 899

Подпис */не се чете/*
Джеймс Гленистър
Директор МГМТ-Финанси
Сиско Интернешънъл Лимитид [Cisco International Limited]
9-11 Ню Скуаре Парк, Бедфонд Лайкс, Фелтам, Мидълсекс, TW14 8XA, Англия

Удостоверявам верността на извършения от мен превод от английски на български език, на приложения документ /Писмо за партньорство - покупка чрез канал от 26.09.2019/ Преводът се състои от 1 стр.

Преводач: Мая Танева ***подпис: /чете се/ печат/***

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

Вярно с оригинала

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

CISCO

LETTER FOR CHANNEL PURCHASING

Date:	**26 September 2019**
To:	**Ministry of labor and social policy**
Bid Number or Project Name:	**Maintenance of MLSP Local Information Infrastructure and the Unified Communication Infrastructure of the Ministry of Labor and Social Policy and Structural Units**

Cisco International Limited, registered in England and Wales (Company Number 06640658), having a principal place of business at 9-11 New Square Park, Bedfont Lakes, Feltham, England TW14 8HA, United Kingdom ("**Cisco**") hereby confirms that, as of the date of this letter, LIREX BG LTD is a Gold certified Cisco channel partner and that Cisco and LIREX BG LTD have entered into an agreement for the purchase and resale of Cisco Products and/or Services (the "**Agreement**").

This means that LIREX BG LTD has complied with the Cisco certification procedure and is duly authorized to purchase and resell Cisco products in BULGARIA as well as negotiate the terms and conditions of support and maintenance services on Cisco products, including warranties, in accordance with the terms and conditions of such Agreement.

Furthermore, LIREX BG LTD is specialized in the following Cisco technologies:

- Advanced Data Center Architecture Specialization ;
- Advanced Security Architecture Specialization ;
- Advanced Enterprise Networks Architecture Specialization ; and
- Advanced Collaboration Architecture Specialization

Please note that the present confirmation is not permanent, and that the status of Cisco's authorized channel is reviewed on a regular basis. This information is accurate as of the date appearing at the top of this certificate and shall be valid for six (6) weeks from such date.

If you need any additional information, please do not hesitate to contact Plamen Zhechev at +359 899 !

CISCO
Cisco International Limited
9-11 New Square Park
Bedfont Lakes, Feltham
Middlesex, TW14 8HA
United Kingdom

James Glenister
DIRECTOR.MGMT-FINANCE

Cisco International Limited

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

ЛИРЕКС БГ ООД София

Вярно с оригинала

Lloyd's Register

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

Сертификат за одобрение

Настоящият сертификат се издава, за да удостовери, че Системата за управление на:

Лирекс БГ ООД

ж.к. Младост 3, бл. 306, 1712 София, България

е одобрена от Lloyd's Register Quality Assurance в съответствие със следните стандарти:

ISO/IEC 27001:2013

Gilles Bessiere - Area Technical Manager

Издаден от: Lloyd's Register EMEA Branch

за и от името на: Lloyd's Register Quality Assurance Limited

Този сертификат е валиден само заедно с приложението към него, което носи същия номер и на което са изброени всички обекти, включени в това одобрение.

Дата на издаване: 14 Март 2019
Дата на валидност: 25 Март 2021
Сертификат номер: 10178798

Първоначално одобрение:
ISO/IEC 27001 – 3 Юни 2009

Номер на одобрение: ISO/IEC 27001 – 0039379

Обхватът на одобрението е приложим за:

Системна интеграция на ИТ проекти – консултации, системен анализ, проектиране, разработка, внедряване, поддържане и управление на ИТ проекти. Мрежова интеграция – консултации, системен анализ, проектиране, разработка, внедряване, поддържане и управление на мрежови проекти. Проектиране, разработване, внедряване и поддръжка на приложни програмни продукти. Одит на информационни системи. Аутсорсинг на ИТ бизнес процеси. Проектиране, строителство, ремонт и реконструкция на административни, обществени, промишлени обекти и инфраструктурни проекти. Търговия с ИТ и мрежови продукти, офис консумативи и копирна хартия. Технически сервиз на ИТ продукти и мрежови комуникационни системи. Предоставяне на Интернет услуги и комуникационни услуги (Интернет доставчик). Провеждане на обучения. Разпространение, инсталация и поддръжка на програмни продукти. Разработване, внедряване и поддръжка на системи за управление на качеството, ИТ услуги, информационната сигурност и защита на личните данни (GDPR).
Декларация за приложимост вер. 5, 12/03/2015.

UKAS MANAGEMENT SYSTEMS
001

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

ЛИРЕКС БГ ООД СОФИЯ

Lloyd's Register Group Limited, its affiliates and subsidiaries, including Lloyd's Register Quality Assurance Limited (LRQA) and their respective officers, employees or agents are, individually and collectively, referred to in this clause as 'Lloyd's Register'. Lloyd's Register assumes no responsibility and shall not be liable to any person for any loss, damage or expense caused by reliance on the information or advice in this document or how it has been provided, unless that person has signed a contract with the relevant Lloyd's Register entity for the provision of this information or advice and in that case any responsibility or liability is exclusively on the terms and conditions set out in that contract.
Издаден от Lloyd's Register EMEA Branch 81A Bulgaria Blvd., Floor 8, Offices 9 & 10 1404 Sofia Bulgaria за и от името на Lloyd's Register Quality Assurance Limited 1 Trinity Park Bickenhill Lane Birmingham B37 7ES United Kingdom

Вярно с оригинала

Lloyd's Register

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

Приложение към сертификат

Сертификат номер: 10178798

Обекти	Дейности
Лирекс БГ ООД ж.к. Младост 3, бл. 306 1712 София	ISO/IEC 27001:2013 Системна интеграция на ИТ проекти – консултации, системен анализ, проектиране, разработка, внедряване, поддържане и управление на ИТ проекти. Мрежова интеграция – консултации, системен анализ, проектиране, разработка, внедряване, поддържане и управление на мрежови проекти. Проектиране, разработване, внедряване и поддръжка на приложни програмни продукти. Одит на информационни системи. Аутсорсинг на ИТ бизнес процеси. Проектиране, строителство, ремонт и реконструкция на административни, обществени, промишлени обекти и инфраструктурни проекти. Търговия с ИТ и мрежови продукти, офис консумативи и копирна хартия. Технически сервиз на ИТ продукти и мрежови комуникационни системи. Предоставяне на Интернет услуги и комуникационни услуги (Интернет доставчик). Провеждане на обучения. Разпространение, инсталация и поддръжка на програмни продукти. Разработване, внедряване и поддръжка на системи за управление на качеството, ИТ услуги, информационната сигурност и защита на личните данни (GDPR).
Теза ООД ж.к. Младост, бл. 54А, вх. 1 1784 София	ISO/IEC 27001:2013 Провеждане на обучения. Разпространение, инсталация и поддръжка на програмни продукти. Извършване на писмени преводи, включително легализацията им. Извършване на устни преводи, превод на субтитри, видео, аудио и аудио дублажи на български и чужди езици.

UKAS MANAGEMENT SYSTEMS
001

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

Lloyd's Register Group Limited, its affiliates and subsidiaries, including Lloyd's Register Quality Assurance Limited (LRQA), and their respective officers, employees or agents are, individually and collectively, referred to in this clause as 'Lloyd's Register'. Lloyd's Register assumes no responsibility and shall not be liable to any person for any loss, damage or expense caused by reliance on the information or advice in this document or howsoever provided, unless that person has signed a contract with the relevant Lloyd's Register entity for the provision of this information or advice and in that case any responsibility or liability is exclusively on the terms and conditions set out in that contract.
Издаден от Lloyd's Register EMEA Branch, 81A Bulgaria Blvd, Floor 8, Offices 9 & 10 1404 Sofia Bulgaria за и от името на Lloyd's Register Quality Assurance Limited, 1 Trinity Park, Bickenhill Lane, Birmingham, B37 7ES, United Kingdom

ЛИРЕКС БГ ООД
Офис

Вярно с оригинала.

Lloyd's Register

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

Приложение към сертификат

Сертификат номер: 10178798

Обекти	Дейности
Лирекс БС АД ж.к. Младост 3, бл. 306 1712 София	ISO/IEC 27001:2013 Системна интеграция на ИТ проекти – консултации, системен анализ, проектиране, разработка, внедряване, поддържане и управление на ИТ продукти. Мрежова интеграция – консултации, системен анализ, проектиране, разработка, внедряване, поддържане и управление на мрежови проекти. Проектиране, внедряване и поддръжка на приложни програмни продукти и ИТ системи. Одит на информационни системи. Аутсорсинг на ИТ и бизнес процеси. Предоставяне на виртуални сървъри, десктоп и приложения като услуга.
Лирекс Хай Тех АД ж.к. Младост 3, бл. 302 1712 София	ISO/IEC 27001:2013 Технически сервиз на ИТ продукти и мрежови комуникационни системи.
Лирекс Хай Тех АД ж.к. Младост 3, бл. 306 1712 София	ISO/IEC 27001:2013 Технически сервиз на ИТ продукти и мрежови комуникационни системи. Търговия с ИТ продукти.
Лирекс БС АД ул. Ян Хуняди 6 9000 Варна	ISO/IEC 27001:2013 Системна интеграция на ИТ проекти – консултации, системен анализ, проектиране, разработка, внедряване, поддържане и управление на ИТ продукти. Мрежова интеграция – консултации, системен анализ, проектиране, разработка, внедряване, поддържане и управление на мрежови проекти. Проектиране, внедряване и поддръжка на приложни програмни продукти и ИТ системи. Одит на информационни системи. Аутсорсинг на ИТ и бизнес процеси. Предоставяне на виртуални сървъри, десктоп и приложения като услуга.

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

UKAS MANAGEMENT SYSTEMS
001

ЛИРЕКС БГ ООД

Lloyd's Register Group Limited, its affiliates and subsidiaries, including Lloyd's Register Quality Assurance Limited (LRQA), and their respective officers, employees or agents are, individually and collectively, referred to in this clause as 'Lloyd's Register'. Lloyd's Register assumes no responsibility and shall not be liable to any person for any loss, damage or expense caused by reliance on the information or advice in this document or howsoever provided, unless that person has signed a contract with the relevant Lloyd's Register entity for the provision of this information or advice and in that case any responsibility or liability is exclusively on the terms and conditions set out in that contract.
Издаден от: Lloyd's Register EMEA Branch, 81A Bulgaria Blvd., Floor 8, Offices 9 & 10 1404 Sofia Bulgaria за и от името на: Lloyd's Register Quality Assurance Limited, 1 Trinity Park, Bickenhill Lane, Birmingham B37 7ES, United Kingdom

Вярно с оригинала

Lloyd's Register

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

Приложение към сертификат

Сертификат номер: 10178798

Обекти	Дейности
Лирекс БГ ООД ул. Любен Каравелов 26 9000 Варна	ISO/IEC 27001:2013 Системна интеграция на ИТ проекти – консултации, системен анализ, проектиране, разработка, внедряване, поддържане и управление на ИТ проекти. Мрежова интеграция – консултации, системен анализ, проектиране, разработка, внедряване, поддържане и управление на мрежови проекти. Проектиране, разработване, внедряване и поддръжка на приложни програмни продукти. Одит на информационни системи. Аутсорсинг на ИТ и бизнес процеси. Проектиране, строителство, ремонт и реконструкция на административни, обществени, промишлени обекти и инфраструктурни проекти. Търговия с ИТ и мрежови продукти, офис консумативи и копирна хартия. Технически сервиз на ИТ продукти и мрежови комуникационни системи. Предоставяне на Интернет услуги и комуникационни услуги (Интернет доставчик). Провеждане на обучения. Разпространение, инсталация и поддръжка на програмни продукти. Предоставяне на виртуални сървъри, десктоп и приложения като услуга. Разработване, внедряване и поддръжка на системи за управление на качеството, ИТ услуги, информационната сигурност и защита на личните данни (GDPR).
Лирекс БГ ООД ул. Беласица 28 5800 Плевен	ISO/IEC 27001:2013 Технически сервиз на ИТ продукти и мрежови комуникационни системи.

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

UKAS MANAGEMENT SYSTEMS
001

Lloyd's Register Group Limited, its affiliates and subsidiaries, including Lloyd's Register Quality Assurance Limited (LRQA), and their respective officers, employees or agents are, individually and collectively, referred to in this clause as 'Lloyd's Register'. Lloyd's Register assumes no responsibility and shall not be liable to any person for any loss, damage or expense caused by reliance on the information or advice in this document or howsoever provided, unless that person has signed a contract with the relevant Lloyd's Register entity for the provision of this information or advice and in that case any responsibility or liability is exclusively on the terms and conditions set out in that contract.
Издаден от Lloyd's Register EMEA Branch, 81A Bulgaria Blvd. Floor 8, Offices 9 & 10 1404 София Bulgaria за и от името на Lloyd's Register Quality Assurance Limited, 1 Trinity Park, Bickenhill Lane, Birmingham B37 7ES, United Kingdom.

ЛИРЕКС БГ ООД

Вярно с оригинала

Lloyd's Register

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

Приложение към сертификат

Сертификат номер: 10178798

Обекти	Дейности
Лирекс БС АД ул. Емануил Манолов 13 5300 Габрово	ISO/IEC 27001:2013 Системна интеграция на ИТ проекти – консултации, системен анализ, проектиране, разработка, внедряване, поддържане и управление на ИТ продукти. Мрежова интеграция – консултации, системен анализ, проектиране, разработка, внедряване, поддържане и управление на мрежови проекти. Проектиране, внедряване и поддръжка на приложни програмни продукти и ИТ системи. Одит на информационни системи. Аутсорсинг на ИТ и бизнес процеси. Предоставяне на виртуални сървъри, десктоп и приложения като услуга.
Лирекс Скопие ДООЕЛ ул. Октомври 23 11, вх. 2, ет. 4, ап. 7 1000 Скопие	ISO/IEC 27001:2013 Търговия с ИТ продукти.

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

UKAS MANAGEMENT SYSTEMS

001

Lloyd's Register Group Limited, its affiliates and subsidiaries, including Lloyd's Register Quality Assurance Limited (LRQA), and their respective officers, employees or agents are, individually and collectively, referred to in this clause as 'Lloyd's Register'. Lloyd's Register assumes no responsibility and shall not be liable to any person for any loss, damage or expense caused by reliance on the information or advice in this document or howsoever provided, unless that person has signed a contract with the relevant Lloyd's Register entity for the provision of this information or advice and in that case any responsibility or liability is exclusively on the terms and conditions set out in that contract.
Издаден от: Lloyd's Register EMEA Branch, 81A Bulgaria Blvd., Floor 8, Offices 9 & 10 1404 Sofia Bulgaria за и от името на: Lloyd's Register Quality Assurance Limited, 1 Trinity Park, Bickenhill Lane, Birmingham

ЛИРЕКС БГ ООД

Вярно с оригинала



чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

CERTIFICATE

No. 3591318

LL-C Certification

Този сертификат се издава да удостовери, че IT Service Management на

ЛИРЕКС БГ ООД

ж.к. Младост 3, бл. 306, вх. 2
1712 гр. София
България

е оценена и е установено, че съответства на изискванията на стандарта

ISO/IEC 20000-1:2011

за обхват на сертификация

Поддържане и управление на ИТ и мрежови комуникационни системи. Аутсорсинг на ИТ бизнес процеси. Технически сервиз на ИТ продукти и мрежови комуникационни системи. Предоставяне на Интернет услуги и продукти (Интернет доставчик). Разпространение, инсталация и поддръжка на програмни продукти.

Този сертификат е издаден под номер **3591318** и е валиден от
19. Април 2019 до 18. Април 2022.

Approved by

Printed by

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

S 3137

validity code: **89533E43-477**
код за валидност на сертификата на www.ll-c.info

Вярно с оригинала

ЛИРЕКС БГ ООД
СОФИЯ

LL-C (Certification) Czech Republic a.s. | Pobřežní 620/3, 186 00 Praha 8

www.ll-c.net

Лирекс БГ ООД
1712 София, ж.к. Младост 3, бл. 306
Телефон: 02/ 9 691 691, Факс: 02/ 9 691 692
www.lirex.bg

ЕИК: 121057952
Банка: Алианц Банк България АД
IBAN: BG46BUIN95611010007719

ЛИРЕКС БГ

Приложение № 2

към Техническо предложение

ОПИСАНИЕ НА УСЛУГИТЕ (ДЕЙНОСТИТЕ),

СЪГЛАСНО ТЕХНИЧЕСКА СПЕЦИФИКАЦИЯ НА ВЪЗЛОЖИТЕЛЯ

за участие в открита процедура за възлагане на обществена поръчка с предмет:

„Поддръжка на локална информационна инфраструктура на МТСП и Единната комуникационна инфраструктура на Министерството на труда и социалната политика и структурните звена“

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

СЪДЪРЖАНИЕ

1. Обща информация 3

1.1. Организация на поддръжката в Лирекс БГ 3

2. Обхват на услугите. Ниво на обслужване 5

2.1. Услуги по поддръжката 5
2.1.1. Услуги по отношение на сървърите 6
2.1.2. Инфраструктурни услуги 8
2.1.3. Услуги по отношение на специализирания приложен софтуер 9
2.1.4. Услуги по отношение на базата от данни 10
2.1.5. Услуги по отношение на поддръжката на потребителски компютри в ИТ инфраструктурата на МТСП 10
2.1.6. Дейности по отношение на сигурността на информацията 10
2.1.7. Услуги по отношение на комуникационното оборудване 11
2.1.8. Услуги по поддръжка и администриране и специализирани връзки 11
2.1.9. Консултантска помощ 11
2.2. Поддръжка на регистри 11
2.3. Отчети 12
2.4. Еднократни дейности 12

3. Параметри на услугата по поддръжка и техническите изисквания по отношение на сроковете за реакция и отстраняване на проблеми: 13

3.1. Дейности по поддръжката 15
3.2. HelpDesk звено 17
3.2.1. Канали за комуникация с потребителите на услугата HelpDesk 17

4. Спецификация на техническите устройства и софтуер предмет на поръчката 17

4.1. Списък на сървърното (хардуерно) оборудване разположено в сградата на МТСП на адрес: гр.София, ул. „Триадица" № 2. 17
4.2. Описание на програмна среда в информационната инфраструктура на МТСП 18
4.3. Списък на комуникационното оборудване разположено в сградата на МТСП на адрес: гр.София, ул. „Триадица" № 2 18
4.4. Описание на хардуерно оборудване и софтуер за единната комуникационна инфраструктура. 18
4.5. Място за изпълнение 20
4.5.1. Списък на адресите и вида на комуникационното оборудване за единната комуникационна инфраструктура на МТСП и структурните звена. 20

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

1. Обща информация

Стратегията на Лирекс БГ за обслужване очертава различни нива на поддръжка и процедури за ескалация на проблемите по време на периода на предоставяне на услуги.

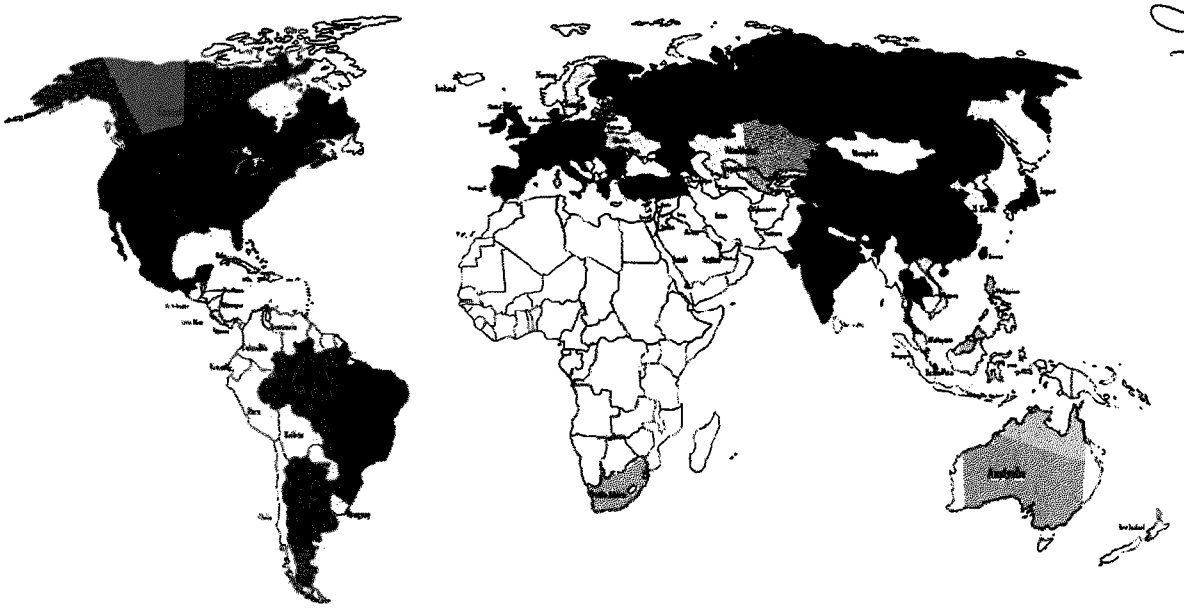
Водещите принципи на стратегията за поддръжка са:

- Насърчаване на „собствеността" и разширяване на знанията на служителите за продуктите.
- Предаване на знания и развитие на поддържащия персонал, като по този начин служителите могат да осигурят висококачествена поддръжка на други групи в организацията на клиента.
- Оптимизиране на ефективността на поддръжката чрез развитие на ключови потребители и консултанти, като се разчита на доставчика само при възникване на сложни проблеми.

1.1. Организация на поддръжката в Лирекс БГ

Лирекс БГ ООД е водещ в областта на управлението на проекти, консултиране, технически и външни услуги. Дружеството се ангажира да доставя знания и иновации на бизнес и правителствени органи, да им помага да трансформират знания и технологии в стойност, като по този начин им помага да се развиват от регионален до глобален мащаб. Чрез задълбочено изследване на индустриални и бизнес процеси, използване на широко приложими ресурси и доказани проследяващи записи, компаниите мобилизират точните хора, умения и технологии, за да помогне на клиентите да увеличат производителността си.

От гледна точка на сервизното обслужване, Лирекс БГ е доказал лидерството си на пазара, обслужвайки клиенти на световно ниво.



	Several types of services
	One type of service
	Limited service

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

Като опитен доставчик на решения за обслужване и поддръжка, дружеството е доказало на своите клиенти, че:

- Знае, обучава и управлява компетенции – знания и умения – типични за поддържане на клиенти от световно ниво и държавни организации (например – разбира и прилага световни политики и стандарти);
- Планира обучението на служителите в познати от клиента стандарти, като част от предварителен процес на делегация на отговорности за поддръжка;
- Във всекидневната работа класифицира проблемите и гарантира решенията им в съответствие с предварително дефинирани приоритети, реакции и времена за ескалация;
- Управлява оперативния риск чрез прилагане на доказани решения;
- Гарантира, че решенията на повтарящите се проблеми не се преоткриват всеки път и не изискват нови ресурси.

Водещ принцип на екипа за поддръжка на дружеството е да осигури висококачествено и ефикасно обслужване на клиентите чрез:

- Бързи отговори и решения на възникналите проблеми.
- Улесняване на дейностите и по-малко бизнес загуби.
- Ефикасна и ефективна поддръжка.
- Сервизно обслужване от край до край.
- Отлични постижения при извършването на сервизно обслужване.

Използвайки ITIL като основно ръководство за управление на ИТ услугите, дружеството дефинира следните процеси по време на организацията на поддръжката:

- Управление на инцидентите – представено описание в Приложение № 4, т. 8.1.
- Управление на конфигурацията – представено описание в Приложение № 4, т. 7.
- Управление на промените - представено описание в Приложение № 4, т. 5.
- Управление на нивото на обслужване.

Процесът на управление на нивото на обслужване контролира качеството на доставените услуги в съответствие с писмени споразумения с клиента, наречени съгласувани нива на обслужване (SLAs).

Основна цел на управлението на нивата на обслужване е да поддържа и постепенно да подобрява качеството чрез постоянен процес, който включва наблюдение, отчитане и преглеждане на постигнатото и премахване на неприемливите нива на обслужване.

Внедряването на процес на управление на нивата на обслужване следва тези стъпки:

- Създаване на каталог на обслужване.
- Разработване на съгласувани нива на обслужване.
- Наблюдение и отчитане.
- Извършване на редовни прегледи на нивото на обслужване.

Отговорности:

- Уточнява изискванията и очакванията на клиента относно обслужването.
- Измерване и отчитане на:
  - Нивото на обслужване, което в действителност е постигнато спрямо целта;
  - Необходимите ресурси;
  - Разходите за обезпечаване на обслужването;
- Непрекъснатото подобряване на нивата на обслужване заедно с бизнес процесите и с програмата за подобрение на обслужването.
- Координира другите управления на услугите и функции за поддръжка включително и доставчици от трета страна.
- Преглежда съгласуваните нива на обслужване, за да посрещне променящите се бизнес нужди или разрешаването на важни проблеми.

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

- Изработва, преглежда и поддържа каталог на услугите.

2. Обхват на услугите. Ниво на обслужване.

В настоящето техническо предложение по процедура за възлагане на обществена поръчка се включва осигуряване на комплексна услуга за професионални услуги за мониторинг, управление, администриране и Поддръжка на локална информационна инфраструктура на МТСП и Единната комуникационна инфраструктура на Министерството на труда и социалната политика и структурните звена – дейности по поддръжка на системен софтуер, хардуер, комуникационно оборудване, мрежови услуги на LAN и WAN информационна и комуникационна инфраструктура на МТСП и териториалните структури описани в **т.4 Спецификация на техническите устройства и софтуер предмет на поръчката** на предложението, включително експертна и системна помощ.

Услугата включва обслужване на следните елементи на информационно-комуникационната инфраструктурата:

- Системен и общ приложен софтуер;
- Специализиран приложен софтуер;
- Бази от данни;
- Хардуер (сървърна, компютърна и офис техника);
- Комуникационно оборудване;

Услугите по поддръжка, предмет на поръчката, ще се извършват само от технически компетентни лица /технически експерти/, които са преминали съответните курсове на обучение и покриват поставените минимални изисквания към експертния екип.

Дружеството разполага с капацитет да осигури необходимите решения за:

- Отдалечено наблюдение на статуса на устройствата;
- Мониторинг на основните системи и програми;
- Портал/уеб-базирано приложение за обработка на инциденти с достъп чрез парола, което позволява на МТСП да регистрира проблеми и следи изпълнението на нивото на услугата;
- Възможност за подаване на заявки 24 часа в денонощието, 365 дни в годината;
- Осигуряване на 4 канала за достъп - мобилен телефон, стационарен телефон, факс, e-mail за връзка в работно време по въпроси, свързани с изпълнението на услугата;

Заявка за инцидент/проблем се подава от представител на Възложителя до Изпълнителя в web-базирана система на адрес https://portal.lirex.com (подробно описание за работа със системата е дадено в Приложение№ 1.1). Заявката съдържа серийния номер на повреденото оборудване, местонахождението на техниката, часа и датата на подаване на заявката, вероятния характер на повредата и идентифицираните последствия от повредата.

Време за реакция - времето от заявяване на проблема от Възложителя в web-базирана HELP-DESK система на дружеството до започване на дейности по отстраняването на неизправността.

Време за отстраняване на проблема - времето от започване на дейности по отстраняването на неизправността до възстановяване на пълната функционалност.

2.1. Услуги по поддръжката

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

Лирекс БГ ще осигури следните дейности и услуги по поддръжката:

- Приемане и регистриране на инцидент / съобщение за повреда;
- Вземане на решение за приоритет на изпълнение на съответната заявка, в случай че са постъпили едновременно няколко заявки;
- Консултации по телефона;
- Посещение на място или отдалечена диагностика;
- Диагностика на повреденото устройство;
- Попълване на констативен протокол;
- Транспорт от и до съответната структура на МТСП.

Услугата по поддръжката е регулярна и се изпълнява непрекъснато през годината, без задължение за, но с право за подаване на заявки от Възложителя.

Лирекс БГ ще осъществява контакт и съдейства на външни компании при инсталация на приложен софтуер, хардуер или информационна система за нуждите на Възложителя при необходимост.

2.1.1. Услуги по отношение на сървърите

Лирекс БГ ще осигури следните дейности и услуги по отношение на сървърите:

- Мониторинг на Windows базирани системи:
  - Наблюдение на наличността и работоспособността на операционната система;
  - Наблюдение на състоянието на основните услуги на операционната система (services);
  - Наблюдение на натоварването на процесорите;
  - Наблюдение на количеството заета оперативна памет;
  - Наблюдение на заетото (свободно) дисково пространство;
  - Наблюдение на натовареността на дисковата подсистема;
  - Наблюдение на натоварването на мрежовите интерфейси;
  - Анализ на получената информация;
- Мониторинг на Unix/Linux базирани системи:
  - Наблюдение на наличността и работоспособността на операционната система;
  - Наблюдение на състоянието на основните услуги на операционната система (daemons);
  - Наблюдение на натоварването на процесорите;
  - Наблюдение на количеството заето оперативна памет;
  - Наблюдение на количеството заета swap памет;
  - Наблюдение на заетото (свободно) дисково пространство;
  - Наблюдение на натовареността на дисковата подсистема;
  - Наблюдение на натоварването на мрежовите интерфейси;
  - Анализ на получената информация;
- Наблюдение на системните съобщения за грешки:
  - Наблюдение за грешки и предупреждения в Event Logs на Windows базирани сървъри;
  - Наблюдение за предупреждения и грешки в syslog, messages и deamon за Unix/Linux базирани сървъри;
  - Наблюдение за предупреждения и грешки в логовете на устройствата от мрежовата инфраструктура;
  - Анализ на получената информация;
- Наблюдение на състоянието на архивите:
  - Наблюдение на състоянието на архивите на операционните системи;
  - Наблюдение на състоянието на архивите на 3rd party приложенията в ИТ инфраструктурата;
  - Наблюдение на състоянието на архивите на СУБД;
  - Анализ на получената информация;

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

- Наблюдение на състоянието на планираните задачи:
  - Наблюдение на състоянието на Scheduled tasks;
  - Наблюдение на състоянието на Crontab jobs;
  - Анализ на получената информация;
- Наблюдение на състоянието на хардуера:
  - Наблюдение на състоянието на хардуера чрез специализиран централизиран софтуер на всички устройства, които позволяват това;
  - Наблюдение на състоянието на хардуера чрез специализиран софтуер предоставен от производителя на хардуера;
  - Анализ на получената информация;
- Администриране на Windows базирани системи:
  - Администриране на MS Windows операционни системи;
  - Инсталиране на нови закупени/наети MS Windows базирани сървъри;
  - Конфигуриране на основни услуги предлагани от операционната система;
  - Конфигуриране на хардуер на нови закупени/наети сървъри;
  - Конфигуриране на планирани задачи (Scheduled tasks);
  - Оказване на съдействие при инсталиране на 3rd party софтуер;
  - Оказване на съдействие при конфигуриране на 3rd party софтуер;
  - Анализ на получената информация;
- Администриране на Unix/Linux операционни системи:
  - Администриране на Unix/Linux операционни системи;
  - Инсталиране на нови закупени/наети Unix/Linux базирани сървъри;
  - Конфигуриране на основи услуги предлагани от операционните системи;
  - Конфигуриране на хардуер на нови закупени/наети сървъри;
  - Конфигуриране на планирани задачи (Crontab jobs);
  - Оказване на съдействие при инсталиране на 3rd party софтуер;
  - Оказване на съдействие при конфигуриране на 3rd party софтуер;
  - Анализ на получената информация;
- Администриране на виртуална инфраструктура:
  - Администриране на виртуалната инфраструктура и всички прилежащи към нея компоненти;
  - Администриране на виртуалните машини. Създаване, изтриване и администриране на ресурсите на виртуалните машини;
  - Анализ на получената информация;
- Администриране на архивите:
  - Архивиране на данни по предварително изготвена архивна схема спрямо нуждите на сървърните приложения;
  - Създаване на нови архивни задачи чрез специализиран софтуер (при наличие);
  - Конфигуриране и промяна в конфигурацията при необходимост на архивните задачи;
  - Конфигуриране и промяна в конфигурацията при необходимост на архивните задачи за архивиране на СУБД;
  - Отстраняване на възникнали проблеми с архивите;
  - Оказване на съдействие при конфигурирането на архивите на 3rd party софтуер чрез специализирани за него инструменти;
  - Поддръжка на специализиран софтуер за архивиране (при наличие);
  - Възстановяване на информация от архив при необходимост;
  - Управление на смяната на архивни ленти и други носители (при наличие);
  - Тестово възстановяване от архив в случай на срив на системите.
  - Администриране на DPM (Администриране на архиви)
  - Анализ на получената информация;
- Администриране на кръпки по сигурността (Security Patches Management):

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

- Тестване на кръпки по сигурността за различните видове приложения и операционни системи;
- Инсталиране на одобрените кръпки за различните видове приложения и операционни системи;
- Оказване на съдействие при необходимост от инсталация на кръпки/обновяване на версии на 3rd party приложения;
- Анализ на получената информация;

- Възстановяване на работоспособността на различните ОС в случай на срив;
- Възстановяване на работоспособността на СУБД в случай на срив.
- Възстановяване на комуникационната свързаност в случай на срив.

2.1.2. Инфраструктурни услуги

Лирекс БГ ще осигури следните дейности по отношение на инфраструктурните услуги:

- Наблюдение на инфраструктурни услуги:
  - Мониторинг на Active Directory услугата;
  - Мониторинг на репликацията между домейн контролери;
  - Мониторинг на състоянието на DNS услугата;
  - Мониторинг на състоянието на репликацията между DNS сървърите;
  - Мониторинг на състоянието на DHCP услугата;
  - Мониторинг на състоянието на базата с опашките от писма на MS Exchange Server;
  - Анализ на получената информация;
- Администриране на MS Active Directory:
  - Създаване, конфигуриране и управление на Group Policy Objects (GPOs);
  - Създаване, конфигуриране и поддръжка на структурата на Organizational Units (OU);
  - Създаване, конфигуриране и поддръжка на Security Groups (SG);
  - Създаване и администриране на потребителски акаунти;
  - Инсталиране на нови Domain Controllers (DC);
  - Управление на AD Site Topology;
  - Управление на домейни;
  - Управление на Operations Masters ролите;
  - Управление на схемата на MS Active Direcroty;
  - Архивиране и възстановяване на услугата MS Active Directory;
  - Анализ на получената информация;
- Администриране на DNS услугата:
  - Поддръжка на DNS сървъри за вътрешни и външни DNS зони;
  - Създаване, конфигуриране и поддръжка на вътрешни и външни DNS зони;
  - Управление на DNS запис в създадените зони;
  - Следене на репликацията между DNS сървърите;
  - Архивиране и възстановяване от архив на DNS зони;
  - Анализ на получената информация;
- Администриране на DHCP услугата:
  - Поддръжка на DHCP сървъри;
  - Създаване, конфигуриране и поддръжка на DHCP scopes;
  - Управление на записите;
  - Архивиране и възстановяване от архив на DHCP услугата;
  - Анализ на получената информация;
- Администриране на файлови сървъри:
  - Поддръжка на Windows File Sharing файлови сървъри;
  - Поддръжка на SAMBA File Sharing файлови сървъри;
  - Администриране на структурата на папките със споделени файлове;

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

- Администриране на правата за достъп до папките със споделени файлове;
- Архивиране и възстановяване от архив на информацията в папките със споделени файлове;
- Анализ на получената информация;

2.1.3. Услуги по отношение на специализирания приложен софтуер

Лирекс БГ ще осигури следните дейности и услуги по отношение на специализирания приложен софтуер:

- Инсталиране на специализиран приложен софтуер (на сървърите) при закупуване или подмяна на технически и програмни средства, след предоставяне на дизайн и инструкции от Възложителя;
- Обновяване на инсталирания специализиран приложен софтуер, след предоставяне на дизайн и инструкции от Възложителя;
- Периодично наблюдение и осигуряване на нормално функциониране на специализираните приложни системи;
- Администриране на приложен софтуер - поддържане на актуални потребители и други административни функции;
- Оказване на системна помощ на потребителите на специализираните приложни системи;
- Управление на MS Exchange Server, осигуряване на достъп до MS Exchange сървър чрез клиентски програми от компютри и мобилни устройства в МТСП и отдалечено по гарантиран на информационната и комуникационна сигурност начин. Също така:
  - Мониторинг на състоянието на пощенската услуга;
  - Мониторинг на състоянието на пощенските сървъри;
  - Мониторинг на състоянието на базите;
  - Мониторинг на състоянието на базите с опашки от писма;
  - Инсталиране, конфигуриране и поддръжка на пощенски сървъри и сървъри, които са необходими за нормалното функциониране на пощенската услуга;
  - Администриране на конфигурацията на пощенската услуга;
  - Администриране на пощенските клъстери;
  - Администриране на базите с пощенските кутии и публични папки (Public Folders) на потребителите;
  - Администриране на базите с опашки от писма;
  - Конфигуриране и администриране на Anti-Spam защитата на пощенската услуга;
  - Провеждане на тестове в тестова среда преди промяна в конфигурацията на пощенската услуга;
  - Архивиране и възстановяване на конфигурацията на пощенската услуга;
  - Ежедневно архивиране на базите с потребителски пощенски кутии и публични папки (Public Folders).
- Достъп на потребителите от МТСП до Интранет и Интернет – както локален достъп чрез кабелна или безжична връзка (WiFi), така и отдалечен достъп на упълномощени потребители на МТСП до вътрешни за МТСП ресурси на информационната инфраструктура съгласно изискванията за информационна и комуникационна сигурност;

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

Забележка: Цялата необходима документация, както и дистрибутивите на софтуера за инсталиране и преинсталиране на наличните специализирани приложни системи и дефиниране на информационни структури и номенклатури в тях се предоставя от Възложителя.

2.1.4. Услуги по отношение на базата от данни

Лирекс БГ ще осигури следните дейности и услуги по отношение на базата от данни:

- Архивиране на базите данни на МТСП;
- Администриране на наличните бази от данни по установени еталони и модели;
- Ежедневно архивиране на статистическите файлове;
- Промяна на системни настройки - след съгласуване с ВЪЗЛОЖИТЕЛЯ;
- Отстраняване на възникнали проблеми, като в случай на необходимост действията се съгласуват с външни организации;

2.1.5. Услуги по отношение на поддръжката на потребителски компютри в ИТ инфраструктурата на МТСП

Лирекс БГ ще подсигури следните дейности и услуги по отношение на поддръжката на потребителски компютри в ИТ инфраструктурата на МТСП:

- Поддръжка в изправност на операционни системи и приложно програмно осигуряване;
- Възстановяване на операционни системи и приложно програмно осигуряване;
- Първоначална диагностика на потребителско оборудване при наличие на проблем;
- Обновяване на версиите на операционните системи и приложния софтуер;
- Инсталиране на кръпки по сигурността (Security Updates);
- Инсталиране на нов приложен софтуер;
- Инсталиране на нов системен софтуер;
- Конфигуриране на хардуер на нови закупени/наети работни станции и мобилни компютри.

2.1.6. Дейности по отношение на сигурността на информацията

Лирекс БГ ще извърши следните дейности и услуги за да осигури сигурност на информацията:

- Ще изпълни всички дейности по договора в съответствие с изискванията на Закона за електронно управление и Закона за киберсигурност и подзаконовите нормативни актове свързани с тяхното прилагане.
- Ще прилага приложимите за предмета на договора изисквания за мрежова и информационна сигурност разписани в „Наредба за минималните изисквания за мрежова и информационна сигурност".
- Ще прилага Политиката и процедурите за информационна сигурност на информационните системи на МТСП;
- Ще осигурява контрол и незабавно известяване на ВЪЗЛОЖИТЕЛЯ по отношение на:
  - Осъществяване на пробив или опит за пробив в системата, хакерски атаки и проникване на вируси;
  - Неоторизирано протичане или копиране на информацията, опит за кражба на потребителски имена, пароли, лични данни и друга поверителна информация;
  - Неоторизирано записване на данни и информация или унищожаване на такава в системата;
- Ще впише възникнали инциденти в „Регистър на събития и инциденти свързани с информационната сигурност", съгласно внедрената система за информационна сигурност в МТСП;

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

- Ще извърши тестване на сигурността на различни приложения, част от операционните системи на Възложителя.
- Ще гарантира конфиденциалност (включително защита на личните данни) на извършваните дейности по поддръжка и няма да разкрива такава информация пред трети лица.

2.1.7. Услуги по отношение на комуникационното оборудване

Лирекс БГ ще осигури следните дейности и услуги по отношение на комуникационното оборудване:

- Конфигурация и преконфигурация на комуникационното оборудване и преносната среда. Сваляне и запазване на конфигурациите на активното мрежово оборудване. Поддържане на база от данни за текущите и миналите конфигурации на активното оборудване;
- Конфигуриране на ново закупено/нает комуникационно оборудване;
- Допълнително преконфигуриране на ИТ инфраструктурата, ако е необходимо;
- Наблюдение и анализ на функционирането на комуникационното оборудване. Измерване и анализ на параметрите на трафика и предложения за оптимизации на комуникационното оборудване;
- Мониторинг и управление на комуникационната инфраструктура;
- Консултации по телефон и e-mail;
- Поддържане на актуална база данни относно видовете активно оборудване, комуникационни връзки и др;
- Системна администрация и наблюдение на интегриран с активната директория уеб филтър и защитна стена.

2.1.8. Услуги по поддръжка и администриране и специализирани връзки

Лирекс БГ ще осигури поддръжка и администриране и на следните специализирани връзки:

- Всички връзки с външни доставчици на интернет и свързаност;
- Проверка на изградената двупосочна комуникационната свързаност на сървърния център на МТСП със сървърните центрове на второстепенните разпоредители, за ползване на споделени услуги (вътрешен сайт, Конто 66, СИМЕВ и други.).

2.1.9. Консултантска помощ

При възникване на необходимост и заявка от Възложителя, Лирекс БГ ще осигури предоставянето на консултантска помощ, експертна подкрепа и съдействие на Възложителя за сметка на Лирекс БГ по специфични: технически, комуникационни, хардуерни, софтуерни, фърмуерни, лицензионни, монтажни, охладителни и т.н. проблеми за оборудването или цялата изградена мрежовата среда, включително дейности свързани с повишаване нивото на информационна и комуникационна сигурност при необходимостта от технологично осъвременяване, обновяване, оптимизиране, развитие, разширение, увеличаване капацитета на оборудването, преконфигуриране на информационната и комуникационна инфраструктура и/или интегриране на допълнителни нови продукти независимо от техния Производител.

2.2. Поддръжка на регистри

За периода на договора дружеството ще води и поддържа в актуално състояние следните регистри в електронен вид и ще предоставя достъп до тях на упълномощен служител от МТСП:

а) **Регистър „Устройства”** – съдържа име на устройството, място на инсталация, производител, модел, инсталирана операционна система, конфигурация,

контакти за поддръжка на съответното устройство – както в рамките на структурите на министерството, така и на външни доставчици, налични договори за поддръжка с външни доставчици. Регистърът на устройствата включва всички потребителски устройства с мрежови достъп – компютри, сървъри, преносими компютри, мобилни устройства, мрежови принтери, многофункционални устройства и други;

b) **Регистър на адресите** – съдържа политиката за раздаване на IPv4 адреси и адресната схема, използвана в МТСП;
c) **Регистър на Услугите** – услуги използвани от клиенти, в това число инфраструктурни (DNS, DHCP, File Share. Print Server);
d) **Регистър на потребителите** – клиенти, права за достъп, кои услуги ползват, кои устройства ползват, този регистър може да се поддържа и като част от наличната в МТСП Active Directory инфраструктура;
e) **Регистър на инцидентите** – съдържа класификация на инцидента, времето на постъпване на оплакването, подател на оплакването, същност на инцидента, кога е разрешен, както и отговорен за разрешаването служител от страна на Изпълнителя;

След приключване на договора всички регистри ще бъдат предадени на упълномощен служител на МТСП.

2.3. Отчети

За извършваните дейности дружеството ще представя на Възложителя месечен отчет, съдържащ следното:

- анализ на получената информация от извършвания мониторинг на сървърната инфраструктура и мрежовото оборудване;
- изпълнени дейности и разрешени проблеми;
- неразрешени инциденти и проблеми;
- наличност на архивите;
- планирани дейности за следващия период;
- препоръки.

2.4. Еднократни дейности

За периода на предоставяне на услугата ще извършим еднократно следните дейности:

- първоначална профилактика на сървърната, сторидж, виртуална и комуникационна инфраструктура базирана на преглед на системни логове с цел установяване на текущото състояние на информационната и комуникационна инфраструктура на МТСП;
- анализ на състоянието и нуждите от архивиране на информационната и комуникационна инфраструктура на МТСП и изготвяне на схема за архивиране;
- разписване на процедура за създаване на годишен архив и еднократно архивиране на информацията от всички информационни и комуникационни системи в МТСП на външен носител, който ще предоставим на Възложителя за съхранение извън сървърните помещения;
- анализ на състоянието и представяне на препоръки за оптимизация на информационната и комуникационна инфраструктура на МТСП;
- анализ на състоянието на информационната сигурност в информационната и комуникационна инфраструктурата на МТСП и предоставяне на доклад на МТСП с препоръки за подобряването ѝ. Ще се извърши от специалист със съответната квалификация;
- анализ на входящия и изходящия интернет трафик в МТСП по предварително утвърден план и предоставяне на доклад включващ

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

информация за количеството на нелегитимния трафик. Лирекс БГ ще предостави необходимите инструменти за извършване на анализа.

Лирекс БГ детайлно ще документира всички предприети дейности през периода на поддръжка.

Описаните еднократни дейности ще бъдат реализирани в срок от 1 (един) месец от сключването на договорът. Лирекс БГ ще осигури всички необходими условия и ще извърши всички подготвителни и организационни дейности за редовното и ефективно предоставяне на услугата.

3. Параметри на услугата по поддръжка и техническите изисквания по отношение на сроковете за реакция и отстраняване на проблеми:

Лирекс БГ разполага с електронна система за регистриране и обработка на инциденти (https://portal.lirex.com), достъпа до системата е чрез парола, което позволява на МТСП да:

- Регистрира проблеми и следи изпълнението на нивото на услугата.
- Възможност за подаване на заявки 24 часа в денонощието, 365 дни в годината.

През времето на договора ще бъдат осигурени 4 канала за комуникация - мобилен телефон, стационарен телефон и e-mail за връзка в работно време по въпроси, свързани с изпълнението на услугата, електронна система за регистриране на инциденти;

Заявка за инцидент/проблем се подава от представител на Възложителя до Лирекс БГ по един от 4-те канала за комуникация. Заявката съдържа серийния номер на повреденото оборудване, местонахождението на техниката, часа и датата на подаване на заявката, вероятния характер на повредата и идентифицираните последствия от повредата.

Време за реакция - времето от заявяване на проблема от Възложителя по един от 4-те канала за комуникация към Изпълнителя до започване на дейности по отстраняването на неизправността.

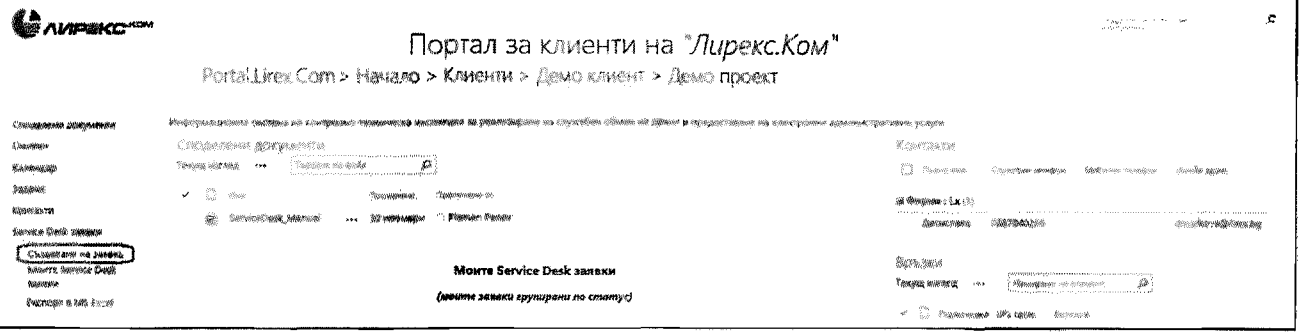
Време за отстраняване на проблема - времето от започване на дейности по отстраняването на неизправността до възстановяване на пълната функционалност.

Времето за реакция се определя от спецификата на проблема, както следва:

- Приоритетите и срокът за решаването на проблемите се определят от Възложителя в зависимост от влиянието им върху работата на администрацията.
- Редът на отстраняване на проблемите се определя в зависимост от техния приоритет.

№	Параметър	Тип изискване	Описание / Изискване	Предложено	Съответствие
1.	Обслужване и достъпност на каналите за заявяване на поддръжка (24 часа в денонощието, 7 дни в седмицата, 365 дни в годината)	Точно	Задължително	Обслужване и достъп на каналите за заявяване на поддръжка 24 часа в денонощието, 7 дни в седмицата, 365 дни в годината	Съответства
2.	Време за реакция при критичен инцидент, застрашаващ работата на цялата система в рамките	Максимум	30 минути	30 минути	Съответства

№	Параметър	Тип изискване	Описание / Изискване	Предложено	Съответствие
	на работното време на Възложителя				
3.	Време за реакция при инцидент, застрашаващ работата на сегмент/част от системата в рамките на работното време на Възложителя	Максимум	2 часа	2 часа	Съответства
4.	Време за реакция при инцидент, застрашаващ работата на отделни елементи на системата, с некритичен статус в рамките на работното време на Възложителя	Максимум	4 часа	4 часа	Съответства
5.	Време за отстраняване на критичен инцидент, застрашаващ работата на цялата системата в рамките на работното време на Възложителя	Максимум	4 часа	4 часа	Съответства
6.	Време за отстраняване на инцидент, застрашаващ работата на сегмент от системата в рамките на работното време на Възложителя	Максимум	12 часа	12 часа	Съответства
7.	Време за отстраняване на инцидент, застрашаващ работата на отделни елементи на системата, с некритичен статус в рамките на работното време на Възложителя	Максимум	24 часа	24 часа	Съответства
8.	Осигуряване на минимум двама души, които ежедневно в рамките на работното време на Възложителя от 09:00 до 17:30 да се ангажират на място	Точно	Задължително	Осигуряване на двама души, които ежедневно в рамките на работното време на МТСП от 09:00 до 17:30 да се ангажират на място с поддръжката.	Съответства

№	Параметър	Тип изискване	Описание / Изискване	Предложено	Съответствие
	в сградата на МТСП с поддръжка.				
9.	Осигуряване на поддръжка, в извън работното време на Възложителя и през празничните дни – при необходимост.	Точно	Задължително	Осигуряване на поддръжка в извън работно време на Възложителя и през празничните дни – при необходимост.	Съответства
10.	Възможност за приемане на заявки за поддръжка по телефон или други гласови канали	Точно	Задължително	Осигурена е възможност за приемане на заявки за поддръжка по телефон или други гласови канали.	Съответства
11.	Възможност за приемане на заявки за поддръжка по e-mail.	Точно	Задължително	Осигурена е възможност за приемане на заявки за поддръжка по e-mail LirexSS@lirex.com.	Съответства
12.	Възможност за нотификация по e-mail при развитие на всеки „инцидент"	Точно	Задължително	Осигурена е възможност за изпращане на нотификация по e-mail при развитие на всеки „инцидент".	Съответства
13.	Отчетност и статистика за постигнатите параметри на поддръжка (времена за реакция, времена за затваряне на „инцидента" и пр.)	Точно	Задължително	Осигурена е възможност за отчетност и статистика за постигнатите параметри на поддръжка (времена за реакция, времена за затваряне на „инцидента" и пр.) чрез електронна система за регистриране на инциденти https://portal.lirex.com. Описание на работата със системата е дадено в Приложение№ 1.1.	Съответства
14.	Линк: https://portal.lirex.com 				

3.1. Дейности по поддръжката

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

Дейностите по поддръжка ще бъдат своевременно планирани и извършвани за осигуряване на необходимото ниво на сигурност и надеждност на информацията и ще са съобразени с изискванията на информационна сигурност и РЕГЛАМЕНТ (ЕС) 2016/679, като включват изпълнение на следното:

- Поддръжка, актуализация и отстраняване на проблеми, свързани със сървърни операционни системи. Там, където е необходимо ще се инсталират операционни системи на нови машини, запазвайки данните и прехвърлянето им в работещ вид.
- Извършване на мониторинг на активни мрежови устройства.

- Извършване на мониторинг на софтуер за антивирусна защита. При необходимост ще се обновяват лицензите.
- Конфигуриране и поддръжка на мрежовите пасивни и активни устройства за да се гарантира безпроблемното функциониране на мрежата и връзката й от и към интернет.
- Извършване на бърза диагностика и пристъпване към решаването на възникнали проблеми.
- Извършване на съгласувана профилактика и тестване на информационните системи на МТСП.
- Установяване на хардуерни проблеми със съответното предписание и максимално бързо пристъпване към отстраняването им, като за целта се изготвят констативни протоколи, които се предават на Възложителя.
- Конфигурация и преконфигурация на комуникационното оборудване и преносната среда. Сваляне и запазване на конфигурациите на активното мрежово оборудване. Поддържане на база от данни за текущите и миналите конфигурации на активното оборудване.
- Допълнително преконфигуриране на ИТ инфраструктурата при необходимост.
- Наблюдение и анализ на функционирането информационната и комуникационната инфраструктура и при необходимост от предприемане на действия се уведомява писмено Възложителя.
- При необходимост съдействие на доставчиците при конфигуриране на новопридобити хардуерни системи и сървъри или софтуер.
- При необходимост съдействие при осъществяване на връзка с външни компании за отстраняване на възникнали проблеми.
- При установяване на възникнали проблеми, свързани с външни организации, ще подпомага действията на Възложителя за решаването им.
- Наблюдение на защитна стена и при необходимост конфигуриране и преконфигуриране след съгласуване с Възложителя.
- В случай на невъзможност за ремонтиране на устройство, модул, повредена част или единица от оборудването удостоверено с констативен протокол в рамките на 24 часа от страна на Възложителя, Лирекс БГ ще предостави временно - оборотно оборудване за срока на ремонта, гарантирайки същата функционалност като тази на оборудването, което се ремонтира.
- Предоставянето на услугите ще се осъществява при прилагане на система за управление на информационната сигурност по стандарт ISO 27001:2013, с цел гарантиране в максимална степен поверителността, сигурността на данните и информацията, както и по стандарт ISO 20000-1:2011 за управление на информационни услуги.
    - Сертификацията на Лирекс БГ по стандарт ISO 27001:2013 за управление на сигурността на информацията, обхваща предмета на настоящата обществена поръчка (дейности, свързани с интеграция и/или разработване и/или внедряване и/или поддръжка на приложни и/или системни програмни продукти и/или интеграция и/или разработване и/или внедряване и/или поддръжка на информационни и/или комуникационни системи).
    - Сертификацията на Лирекс БГ по стандарт ISO 20000-1:2011 за управление на информационни услуги с обхват на сертификация, обхваща предмета на настоящата обществена поръчка (дейности, свързани с интеграция и/или разработване и/или внедряване и/или поддръжка на информационни и/или комуникационни системи и/или

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

интеграция и/или разработване и/или инсталация и/или внедряване и/или поддръжка на програмни продукти).

3.2. HelpDesk звено

За предоставянето и управлението на ИТ услуги „Лирекс БГ" ООД ще осигури присъствие (на място на адрес гр. София, ул. "Триадица" № 2) на 2 техническа лица в рамките на работното време на МТСП, които да извършват консултации от типа HelpDesk и да подпомагат министерството при възникнали проблеми с информационната и комуникационна инфраструктура на МТСП.

Helpdesk звеното ще приема и обслужва заявки, както и ще предоставя квалифицирана помощ на потребителите в рамките на стандартното работно време (5 работни дни по 8 часа), от 09:00 часа до 17:30 часа.

Лирекс БГ гарантира параметрите на предоставената услуга до изтичането на срока на договора.

3.2.1. Канали за комуникация с потребителите на услугата HelpDesk

HelpDesk звеното ще приема заявки за обслужване чрез следните комуникационни канали:

1. Телефон – приемане на заявки за обслужване чрез телефонно обаждане.
2. E-Mail – за входящи запитвания с цел осигуряване на единна входяща точка за изпращани електронни съобщения.
3. Интернет – попълване на WEB форма в системата за обслужване на HelpDesk.
4. Приемане на заявки на хартиен носител (писма) – заявки за услуги могат да постъпят по традиционните за държавната администрация канали, а именно на хартиен носител през съответните деловодства. Тези заявки се регистрират ръчно в системата за обслужване, като след приключване на заявката ще се изготви и изпрати писмен отговор на заявителя. Всички входящи и изходящи хартиени писма се одобряват и подписват от Възложителя.

Всички заявки ще бъдат регистрирани, класифицирани и проследявани от екипа на Лирекс БГ.

Подробно описание на Help Desk системата на „Лирекс БГ" ООД е описано в Приложение 1 и Приложение 1.1 за работа със системата на техническото предложение.

4. Спецификация на техническите устройства и софтуер предмет на поръчката

Видът и броят на подлежащите на поддържане технически устройства и софтуер са както следва:

4.1. Списък на сървърното (хардуерно) оборудване разположено в сградата на МТСП на адрес: гр.София, ул. „Триадица" № 2.

Таблица 1.

Наименование	Брой	Гаранция / до
HPE ProLiant DL 360	2	3г / 17.01.2021
HPE 3PAR 8400	1	3г / 17.01.2021
Huawei OceanStor 5500v3	1	5г / 16.10.2020
Lenovo IBM System x 3550 M5	7	5г / 16.10.2020
Lenovo IBM System n 3630 M4	1	5г / 16.10.2020
HP DL320eG8	1	
HP DL380G5	1	
Cisco UCSC-BSE-SFF-C200	2	
HP ProLiant BL460cE5450 2G	7	
HP Blade System C7000 Enclosure	1	

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

Наименование	Брой	Гаранция / до
Лентово устройство за архивиране HP StorEver 1/8 G2	1	
HP ProLiant ML 350 G5	1	
HP EVA 4400	1	
HP ProLiant ML150 G6	1	

4.2. Описание на програмна среда в информационната инфраструктура на МТСП

Таблица 2.

Приложение	**Брой**
Виртуална среда VMWare ESXi	2
Виртуална среда Microsoft Hyper-V	5
Microsoft Exchange 2010 Server	1
Web Server	5
Microsoft WSUS Server	1
Database Server	9
Виртуални машини	16
Други	9
Сървърни операционни системи	**Брой**
Microsoft Windows 2000/2003/2008/2012	30
Linux/Unix	8

От 350 до 390 работни места(всяко работно място е с персонален компютър, свързан с принтер и/или скенер).

4.3. Списък на комуникационното оборудване разположено в сградата на МТСП на адрес: гр.София, ул. „Триадица“ № 2

Таблица 3.

Наименование	Брой	Гаранция / До
HPE SN 3000B	1	3г / 17.01.2021
Cisco Catalyst 6800	4	3г / 05.01.2021
Cisco Catalyst 6880	1	3г / 05.01.2021
Lenovo Brocade 6505 FC SAN Switch	2	
Cisco Catalyst 6800	7	
Cisco Catalyst 6880	1	
Cisco Catalyst WS-C2960S-24PS-L	2	
Cisco Catalyst WS-C2960-24TT-L	10	
Cisco C2911-VSEC/K9	1	

4.4. Описание на хардуерно оборудване и софтуер за единната комуникационна инфраструктура.

Таблица 4.

№	**Опорен VPN Концентратор, Защитна стена и Маршрутизатор – 2 бр.**
1.	Cisco ASR1004 Chassis Dual P/S
2.	Cisco ASR1000 Route Processor 14GB DRAM

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

3.	Cisco ASR1000 RP1 4GB DRAM
4.	Cisco ASR1000 RP1 40GB HDD
5.	Cisco ASR 1000 Series RP1 ADVANCED ENTERPRISE SERVICES
6.	Cisco ASR1000 SPA Interface Processor 10
7.	Cisco 5-Port Gigabit Ethernet Shared Port Adapter
8.	2x 1000BASE-LX/LH SFP transceiver module MMF/SMF 1310nm DOM
9.	2x 1000BASE-T SFP (NEBS 3 ESD)
10.	SPA for ASR1000; No Physical Part; For Tracking Only
11.	2x Cisco ASR1004 AC Power Supply
12.	2x 10A AC Pwr Cord left-angle (Europe) (bundle option)
13.	Flex. Pack Insp. Right-To-Use Feat LicASR1000 Series
14.	Firewall Right-To-Use Feature Lic for ASR1000 Series
15.	Firewall/NAT Stateful Inter-Chassis Redundancy License
16.	SW Redundancy Right-To-Use Feat Lic for ASR1000 Series
17.	Encryption Right-To-Use Feature Lic for ASR1000 Series
18.	Cisco ASR1000 Embedded Services Processor 10G
	Агрегационен VPN Концентратор, Защитна стена и Маршрутизатор – 13 бр.
1.	Cisco 3925 Security Bundle w/SEC license PAK
2.	Cisco 3925-3945 IOS UNIVERSAL
3.	U.S. Export Restriction Compliance license for 3900 series
4.	Cisco 3925/3945 AC Power Supply
5.	Cisco 3925/3945 AC Power Supply (Secondary PS)
6.	2x AC Power Cord (Europe) C13 CEE 7 1.5M
7.	Cisco Services Performance Engine 100 for Cisco 3925 ISR
8.	Insert Packout - PI-MSE
9.	IP Base License for Cisco 3925/3945
10.	Cisco 3925/3945 Fan Assembly (Bezel included)
11.	4x Blank faceplate for HWIC slot on Cisco ISR
12.	Cisco Config Pro Express on Router Flash
13.	1GB DRAM (512MB+512MB) for Cisco 3925/3945 ISR (Default)
14.	256MB Compact Flash for Cisco 1900 2900 3900 ISR
15.	Security License for Cisco 3900 Series
16.	Blank faceplate for DW slot on Cisco 2951 and 3925
17.	2x Removable faceplate for SM slot on Cisco 290039004400 ISR
18.	Integrated Management Controller Express for 3925 and 3945

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

	Защитна стена, Маршрутизатор и VPN устройство за крайните точки на присъствие на МТСП – 6 бр.
1.	Cisco 2901 Security Bundle w/SEC license PAK
2.	Cisco 2901-2921 IOS UNIVERSAL
3.	Cisco 2901 AC Power Supply
4.	AC Power Cord (Europe) C13 CEE 7 1.5M
5.	Insert Packout - PI-MSE
6.	IP Base License for Cisco 2901-2951
7.	4x Blank faceplate for HWIC slot on Cisco ISR
8.	Cisco Config Pro Express on Router Flash
9.	512MB DRAM for Cisco 2901-2921 ISR (Default)
10.	256MB Compact Flash for Cisco 1900 2900 3900 ISR
11.	Security License for Cisco 2901-2951
	Защитна стена и VPN устройство за малки крайни точки на присъствие на МТСП – 25 бр.
1.	ASA 5505 Appliance with SW 10 Users 8 ports 3DES/AES
2.	ASA 9.0 software image for 5505
3.	AC Power Cord Type C5 Europe
4.	ASA 5500 Strong Encryption License (3DES/AES)
5.	ASA 5505 AC Power Supply Adapter
6.	ASA 5505 10 User software license
7.	ASA 5500 AnyConnect Client + Cisco Security Desktop Software
8.	ASA 5505 SSC Blank Slot Cover
	Персонални VPN Софтуерни клиенти – 300 бр. Cisco VPN Client Software, осигуряваща право за неограничено инсталиране на клиентските устройства и неограничено изтегляне от сайта на производителя на избрана или последна версия на софтуера.

4.5. Място за изпълнение

МТСП, гр.София, ул. „Триадица“ № 2

4.5.1. Списък на адресите и вида на комуникационното оборудване за единната комуникационна инфраструктура на МТСП и структурните звена.

Таблица 5.

НОМЕР ПО РЕД	ОБЕКТ (Организационна структура във ведомството)	НАСЕЛЕНО МЯСТО	АДМИНИСТРАТИВЕН АДРЕС	ТИП УСТРОЙСТВО (Продуктов номер)
1.	Министерство на труда и социалната политика	София	ул. "Триадица" 2	Cisco ASR1004

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

НОМЕР ПО РЕД	ОБЕКТ (Организационна структура във ведомството)	НАСЕЛЕНО МЯСТО	АДМИНИСТРАТИВЕН АДРЕС	ТИП УСТРОЙСТВО (Продуктов номер)
2.	Министерство на труда и социалната политика	София	ул. "Триадица" 2	Cisco ASR1004
3.	Министерство на труда и социалната политика	София	ул. "Триадица" 2	Cisco 3925-SEC/K9
4.	Министерство на труда и социалната политика	София	ул. "Триадица" 2	Cisco 3925-SEC/K9
5.	Агенция за социално подпомагане	София	ул. "Триадица" 2	ASA5505-BUN-K9
6.	0532 Агенция за социално подпомагане Стара Загора; 0533 Агенция за социално подпомагане Стара Загора РДСП-Стара Загора; 0535 Агенция по заетостта Стара Загора ДБТ; 0536 Главна дирекция Европейски фондове, международни програми и проекти Стара Загора РУП - Югоизточен; 0537 Изпълнителна Агенция "Главна инспекция по труда" Стара Загора; 0538 Проект „Красива България" Стара Загора Регионално звено за изпълнение на Проект "Красива България"; 0687 Агенция за хората с увреждания Стара Загора	Стара Загора	ул. "Стефан Караджа" 8	Cisco 3925-SEC/K9
7.	0053 Агенция за социално подпомагане Раковски ; 0054 Агенция по заетостта Раковски ДБТ	Раковски	бул. Георги С.Раковски №108а	ASA5505-BUN-K9
8.	Дирекция социално подпомагане Ръковски – изнесено работно място Брезово	Гр. Брезово	Ул. Марин Домусчийски № 3	ASA5505-BUN-K9
9.	Дирекция социално подпомагане Долни Дъбник	Гр. Долни Дъбник	Ул. Генерал Ганецки №2	ASA5505-BUN-K9
10.	Дирекция социално подпомагане Долна Митрополия	Гр. Долна Митрополия	Ул. Цоньо Митев №5	ASA5505-BUN-K9
11.	Дирекция социално подпомагане Бяла Слатина	Гр. Бяла Слатина	Ул. Хан Крум №75	ASA5505-BUN-K9
12.	0609 Агенция по заетостта Харманли ДБТ	Харманли	бул. "България" 4 ет.4	ASA5505-BUN-K9
13.	0499 Агенция по заетостта Ардино ДБТ	Ардино	ул. "Републиканска" 3	ASA5505-BUN-K9
14.	0267 Агенция по заетостта Брезово Филиал	Брезово	ул. "Димитър Благоев" № 3	ASA5505-BUN-K9
15.	0172 Агенция по заетостта Болярово Филиал	гр. Болярово	ул. "9-ти септември" 37	ASA5505-BUN-K9

НОМЕР ПО РЕД	ОБЕКТ (Организационна структура във ведомството)	НАСЕЛЕНО МЯСТО	АДМИНИСТРАТИВЕН АДРЕС	ТИП УСТРОЙСТВО (Продуктов номер)
16.	0291 Агенция по заетостта Котел ДБТ	гр. Котел	ул. "Г.С. Раковски" 34	ASA5505-BUN-K9
17.	0490 Агенция по заетостта с. Руен ДБТ	с. Руен	ул. "Първи май" 11	ASA5505-BUN-K9
18.	0684 Агенция за хората с увреждания София – централно управление	София	ул. "Софроний Врачански" № 104-106	Cisco 2901-SEC/K9
19.	0676 Агенция за хората с увреждания	Пловдив	бул. "Санкт Петербург" № 1	ASA5505-BUN-K9
20.	0150 Агенция за хората с увреждания	Варна	ж.к. "Чайка", бл.191, партер, офис № 2	ASA5505-BUN-K9
21.	Изпълнителна агенция "Главна инспекция по труда" (ИА ГИТ)	София	бул. „княз Александър Дондуков" 3	Cisco 2901-SEC/K9
22.	Изпълнителна агенция "Главна инспекция по труда" (ИА ГИТ)	София	бул. „княз Александър Дондуков" 3	ASA5505-BUN-K9
23.	Национален институт за помирение и арбитраж(НИПА)	София	кв. „Овча купел", ул. "Боряна" 59, бл. 215 А, ет. 1, ап. 1	Cisco 2901-SEC/K9
24.	Център за развитие на човешките ресурси и регионални инициативи (ЦРЧРРИ)	София	кв. „Кремиковци" 1849	Cisco 2901-SEC/K9
25.	Главна дирекция Европейски фондове, международни програми и проекти Бургас РУП - Югоизточен	Бургас	ул. Цар Петър №5б ет.13 ст.7, НАП	CISCO2901-SEC/K9
26.	Главна дирекция Европейски фондове, международни програми и проекти Ямбол РУП - Югоизточен;	Ямбол	Ул. „Търговска" № 2, ет.1, офис 6	CISCO3925-SEC/K9
27.	Главна дирекция Европейски фондове, международни програми и проекти Сливен РУП - Югоизточен	Сливен	ул. "Ген.Скобелев" № 6, ет.3, стая 22	ASA5505-BUN-K9
28.	Главна дирекция Европейски фондове, международни програми и проекти Кърджали РУП - Южен централен	Кърджали	Бул. "България" №49, ет.3, офис №4	ASA5505-BUN-K9
29.	Главна дирекция Европейски фондове, международни програми и проекти Смолян РУП - Южен централен	Смолян	Бул."България" №14, ет.4, офис 407	CISCO3925-SEC/K9
30.	Главна дирекция Европейски фондове, международни програми и проекти Хасково РУП - Южен централен;	Хасково	Ул. "Патриарх Евтимий" №2, ет.2, стая №148 и №149	CISCO3925-SEC/K9
31.	Главна дирекция Европейски фондове, международни програми и	Пловдив	пл. "Н. Мушанов" 1, стая 131 и 132	ASA5505-BUN-K9

НОМЕР ПО РЕД	ОБЕКТ (Организационна структура във ведомството)	НАСЕЛЕНО МЯСТО	АДМИНИСТРАТИВЕН АДРЕС	ТИП УСТРОЙСТВО (Продуктов номер)
	проекти Пловдив РУП - Южен централен;			
32.	Главна дирекция Европейски фондове, международни програми и проекти Пазарджик РУП - Южен централен	Пазарджик	Ул. Екз. Йосиф" №15А, ет.4, стая №8	CISCO3925-SEC/K9
33.	Главна дирекция Европейски фондове, международни програми и проекти Перник РУП - Югозападен	Перник	пл. Св. "Ив. Рилски" № 1 Б ет.14 ст.10 и 11	ASA5505-BUN-K9
34.	Главна дирекция Европейски фондове, международни програми и проекти Кюстендил РУП - Югозападен	Кюстендил	ул. "Демокрация" №44, ет.7, стая 4	CISCO3925-SEC/K9
35.	Главна дирекция Европейски фондове, международни програми и проекти Благоевград РУП - Югозападен	Благоевград	ул."Ив. Михайлов" № 58, ет 3	CISCO3925-SEC/K9
36.	Главна дирекция Европейски фондове, международни програми и проекти Видин РУП - Северозападен	Видин	пл. „Бдинци" № 3, ет. 3, ст. 43 А, Сградата на Бюрото по труда	CISCO2901-SEC/K9
37.	Главна дирекция Европейски фондове, международни програми и проекти Враца РУП - Северозападен;	Враца	Ул. „Ст. Заимов" № 2 ет. 4 офис 11-13	CISCO3925-SEC/K9
38.	Главна дирекция Европейски фондове, международни програми и проекти Монтана РУП - Северозападен	Монтана	Пл. „Жеравица" № 5, ет. 3, стая 309 Инспекция по труда	CISCO3925-SEC/K9
39.	Главна дирекция Европейски фондове, международни програми и проекти Ловеч РУП - Северозападен	Ловеч	Ул. „Търговска" 24, ет. 3, офис 310	ASA5505-BUN-K9
40.	Главна дирекция Европейски фондове, международни програми и проекти Велико Търново РУП - Северен централен	Велико Търново	пл. "Център" - 2, ет.5, стая 524	ASA5505-BUN-K9
41.	Главна дирекция Европейски фондове, международни програми и проекти Габрово РУП - Северен централен	Габрово	Ул. „Ц. Дюстабанов" № 24, стая 18	ASA5505-BUN-K9
42.	Главна дирекция Европейски фондове, международни програми и проекти Русе РУП - Северен централен	Русе	бул. Скобелев № 45, ет. 3, офиси 4 и 5.	ASA5505-BUN-K9
43.	Главна дирекция Европейски фондове,	Силистра	Бул. „Македония" № 167, до ДБТ	CISCO3925-SEC/K9

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

НОМЕР ПО РЕД	ОБЕКТ (Организационна структура във ведомството)	НАСЕЛЕНО МЯСТО	АДМИНИСТРАТИВЕН АДРЕС	ТИП УСТРОЙСТВО (Продуктов номер)
	международни програми и проекти Силистра РУП - Северен централен			
44.	Главна дирекция Европейски фондове, международни програми и проекти Варна РУП - Североизточен	Варна	ул. „Шипка" № 10, ет. 5, ст. 509	CISCO3925-SEC/K9
45.	Главна дирекция Европейски фондове, международни програми и проекти Шумен РУП - Североизточен	Шумен	Ул. „Цар Ив. Александър" № 108, ет.2, стая 204	ASA5505-BUN-K9
46.	Главна дирекция Европейски фондове, международни програми и проекти Добрич РУП - Североизточен	Добрич	Ул. „България" № 16, ет. 7, стая 706 А	ASA5505-BUN-K9

Дата: 27.09.2019 г.

Подпис, печат: .....

Гр. София

Място и дата на издаване

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

Манол Илиев

(*име, длъжност*)

Изготвил:В.Димитрова
Съгласувал: В.Стоев

Лирекс БГ ООД
1712 София, ж.к. Младост 3, бл. 306
Телефон: 02/ 9 691 691, Факс: 02/ 9 691 692
www.lirex.bg

ЕИК: 121057952
Банка: Алианц Банк България АД
IBAN: BG46BUIN95611010007719

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

Приложение№ 3
към Техническо предложение

ПРЕДЛОЖЕНИЕ ЗА УПРАВЛЕНИЕ ИЗПЪЛНЕНИЕТО НА ПОРЪЧКАТА

за участие в открита процедура за възлагане на обществена поръчка с предмет:

„Поддръжка на локалната информационна инфраструктура на МТСП и Единната комуникационна инфраструктура на Министерството на труда и социалната политика и структурните звена“

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

Съдържание

1. Методология за административно управление на дейностите 3
2. Фази, през които минава управлението на проекта 8
2.1. Управление на интеграцията 9
2.2. Управление на обхвата 10
2.3. Управление на времевата рамка 10
2.4. Управление на качеството 11
2.5. Управление на конфигурациите/промените 11
2.5.1. Контролни точки в процеса на промяна 12
2.5.2. Процедурата за контрол на промените 12
2.5.3. Методика за диагностициране и превантивни дейности 13
2.6. Управление на човешките ресурси 13
2.7. Управление на риска 13
2.8. Управление на комуникациите 13
2.9. Процедури и документи от СУКИС на Изпълнителя 14
3. Разпределение на ролите и ресурсите при изпълнение на предмета на поръчката 15
3.1. Екип за изпълнение на поръчката 15
3.2. Организация, структура и отговорности на екипа 23
3.2.1. Общи изисквания и ангажимент на Изпълнителя по време на изпълнение на договора 28
4. Описание на стандартизирани процедури и документи за управление 28
4.1. Основни принципи на комуникация 28
4.2. Видове доклади и документи 29
4.3. Начин на взаимодействие и механизми на контрол и отчетност 30
5. Механизми за управление и контрол на качеството 31

1. Методология за административно управление на дейностите

„Лирекс БГ" ООД е сертифициран по международно признати стандарти като ISO 9001:2008, ISO 20000-1:2011, ISO 27001:2013.

Тези световно познати сертификати покриват управлението, контролирането и непрекъснатото усъвършенстване на разнообразието от продукти и професионални услуги. Използването на основни принципи от стандартите за управление на качеството гарантират, че дейностите в рамките на проекта се извършват по критерии, които напълно съответстват на тези на водещи световни системни интегратори.

Методологиите за управление на проекти, които ще бъдат използвани и следвани във всички дейности за успешно реализиране на проекта са PMI и PRINCE2.

За изпълнението на проекта е предложена методология, която следва принципите, определени от най-добрите практики на PMI и PRINCE2. Приетите подходи за управление на проект са описани с подробности в документите за системата за управление на качеството.

Лирекс БГ използва ITIL като най-добри практики за доставка на ИТ базирани интелигентни системи, услуги и поддръжка на клиенти. Част от тях са също сертифицирани партньори на Microsoft, осигуряващи високотехнологични услуги на базата на продукти и методологии, разработени от Microsoft.

За анализиране на текущите услуги и фази на проекта, в методологията са включени понятия от бизнес анализа. Всяка методология, която няма правилна поддръжка на знанията и инструментите не е успешна, по тази причина екипът на дружеството ще използва следните инструменти за автоматизиране и контролиране на процесите: Microsoft Office Project, ARIS, Microsoft Visio.

Управлението на проект е дисциплина за организиране и управление на ресурсите по такъв начин, че цялата необходима работа по проекта да се извърши и той да приключи в рамките на обхвата, качеството и ограничението за време и разход. Проектът е временно и единично усилие, което има за цел да създаде уникален продукт или услуга, която довежда до изгодна промяна или добавена стойност. Свойствата „временност" и „единично усилие" са противоположни с процесите и дейностите, които са постоянни или полупостоянни за създаване отново и отново на един продукт или услуга. Управлението на тези две системи много често е различно и изисква разнообразни технически и философски умения, необходими за развитието на управлението на проекти.

Управлението на проекта ще е съобразено с най-добрите практики. Екипът, който ще работи по проекта ще прилага гъвкав подход и едновременно водещ опит, за да осигури качество и контрол за всяка фаза от работата по проекта. Ръководенето на проекта ще следва препоръките и методиката на PRINCE2 съобразени с изискванията на Документацията вкл. техническото задание на Възложителя.

PRINCE2

PRINCE2 (PRojects IN Controlled Environments) е структуриран метод за ефективно управление на проекти, уникален по рода си, общ, структуриран метод за управление на проекти, който е:

- Повторяем;
- Напълно достъпен;
- Построен на базата на опита;
- Гарантиращ, че екипът знае какво, къде, как и кога да очаква;
- Рано предупреждаващ за проблеми;
- Метод, който е проактивен, а не реактивен, но имащ възможност да се приспособи към внезапни, неочаквани събития;
- Проектите могат да съществуват сами, да бъдат във връзка с други проекти или да бъдат част от по-голяма програма.

При всички такива случаи партньорите в дружеството прилагат метода PRINCE2. Този метод осигурява на Изпълнителя и Възложителя:

- Контролирано управление на промените, от гледна точка на инвестициите и възвръщането им;
- Активно включване по време на проекта на потребители и заинтересовани лица, това гарантира, че реализирания продукт ще посрещне всички изисквания (функционални, на бизнеса и средата, изисквания относно услугите и управлението).

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

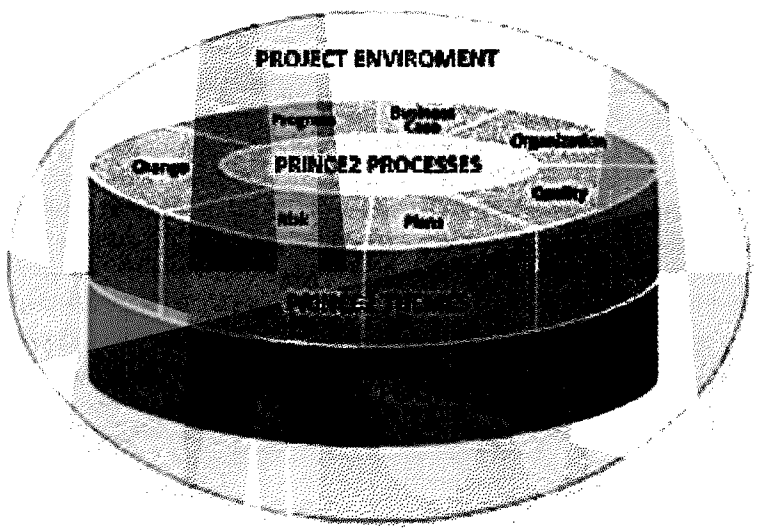
- Подход, който прави разлика между управление на проект и разработване на продукт(и), по този начин подходът на управление е еднакъв независимо дали проекта е за построяване на кораб или за внедряване на нови работни практики.

Предимствата и ползите от прилагане на този метод се свеждат до многото успешни проекти, прилагали PRINCE2. Той балансира трите основни интереса от проекта – на бизнеса, на потребителите и на разработчика. Това е един повтарящ се, гъвкав и скалируем метод за управление. Той е разработван и усъвършенстван в продължение на години и съчетава в себе си опита на стотици ръководители на проекти, които са в основата на разработката му. Първата версия на PRINCE2 е разработена през 1989г. и е усъвършенствана до днес. Тя въплъщава утвърдена и доказана практика при управление на проекти и е широко позната и разбираемо средство, осигуряващо общ език за описание за всички участници в проекта.

PRINCE2 насърчава формално разпознаване на отговорностите в един проект и се фокусира върху това какво трябва да предостави проектът, защо, кога и за кого. Когато мениджърите на проектите използват PRINCE2, те могат да установят правилни инструкции, да използват определена структура за делегация, права и комуникации, както и да разделят проекта на лесни за управление части, които могат да се планират точно.

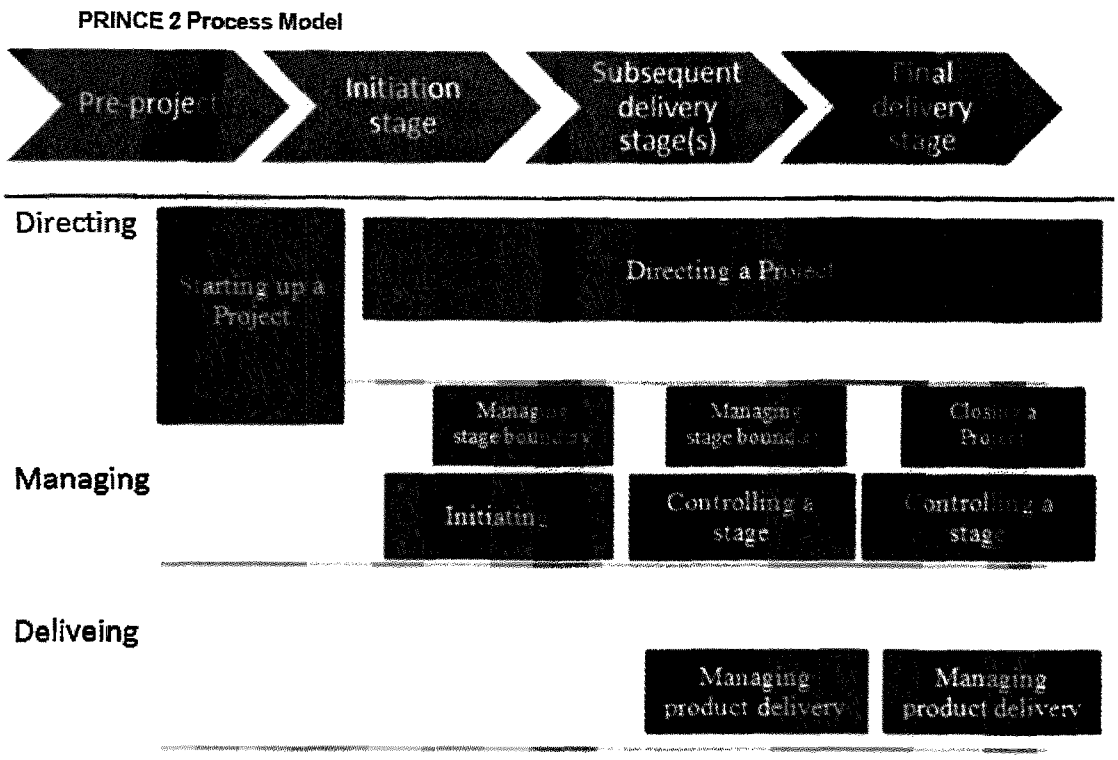
Методологията PRINCE2 прилага процесно-ориентиран подход. Процесите определят съответните управленски действия по време на изпълнение на проекта. Допълнително, PRINCE2 описва определен брой компоненти, които са приложими в подходящите дейности.

Структурна схема на методологията PRINCE2 е дадена по-долу на фиг.1.



Фиг. 1 Структурна схема на методологията PRINCE2

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679



Фиг. 2 Процесен модел на PRINCE2

Мениджърите на проектите могат да се сдобият с ресурсно задължение като част от процеса за одобрение на проекта, но могат и да предоставят редовни, но кратки управленски доклади, по този начин срещите с ръководството и вложителите се свеждат до минимум – макар че се налагат при главните точки от развитието на проекта. PRINCE2 се използва по целия свят.

PMI – PMBOK (Project Management Body of Knowledge)

Най-широко разпространен в целия свят стандарт за управление на проекти, който дава ценни професионални насоки за управление на отделните проекти и програми и представлява богат набор от концепции за управление на отделните направления и фази на жизнения цикъл на проектите. Стандартът представлява формален документ, който описва норми, методи, процеси и практики в управлението на проекти. Развил се е във времето от ползването на добри практики от професионалисти в сферата на управление на проекти до професионален стандарт, следващ етичен код и професионални норми. Използването на този стандарт при управлението на проекти е доказателство за висока степен на професионализъм на екипа и е гаранция за високо качество не само на резултата, но и на начина на постигането му.

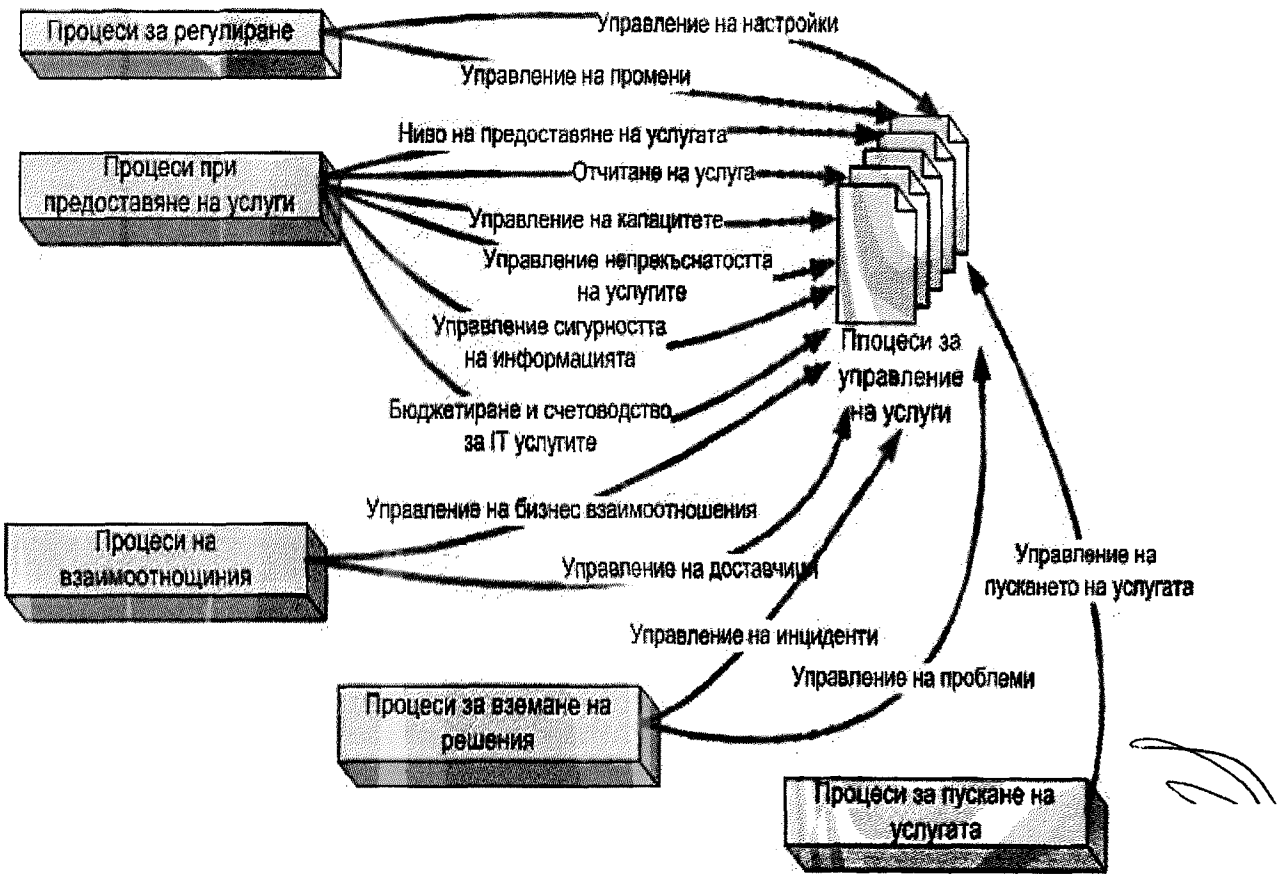
В основата на стандарта стоят пет процесни групи: Иницииране, Планиране, Изпълнение, Наблюдение и контрол и Затваряне и 47 процеса, които се изпълняват многократно в рамките на жизнения цикъл на проекта и използват съответно специфични входни данни, изходни резултати, техники и инструменти.

Важно е да се отбележи, че стандартът дава важни насоки за балансиране на основните ограничения в управлението на проекти: Обхват, Качество, Време (График), Бюджет, Ресурси, Рискове, тъй като тези ограничения са пряко свързани помежду си и всяка промяна в параметрите на някое от тези ограничения води до промяна на параметрите на поне още едно. Именно затова в управлението на проектите стриктно се наблюдават и контролират тези ограничения.

Методологията на ISO 20000 за цялостното управление на услугата.

□□□□□□□□□а управление на услуга

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679



Фиг. 3 Процеси за управление на услуга

Както се вижда от фигурата, ISO/IEC 20000 посочва съвкупност от тясно свързани процеси за управление на предоставянето на услуги – в конкретния случай – Поддръжка на локалната информационна инфраструктура на МТСП и Единната комуникационна инфраструктура на Министерството на труда и социалната политика и структурните звена.

Методологията е система от процеси и сфери на знание, широко приети като най-добра практика в дисциплината „Управление на проекти". Този международно признат стандарт е основата на управлението на проекти. Според него съществуват 5 основни групи процеси (пускане на услугата, предоставяне, регулиране, взаимоотношения, вземане на решения) и 7 сфери на знание (управление на интеграцията на проекта, на обхвата, на времето, на качеството, на човешките ресурси, на комуникациите, на риска и на трети лица). Във всеки проект или фаза процесите се застъпват и си взаимодействат. Те се описват от гледна точка на вход (документи, планове, проекти), инструменти и техники (механизми, прилагани върху входящите данни) и изход (документи, продукти, резултати).

Основните цели на методологията са:

- Контролиране на обхвата, графика, разходите и качеството,
- Намаляване и управляване на риска,
- Управление на ресурсите,
- Идентифициране на дейностите по проекта,
- Координиране на комуникациите между заинтересованите страни,
- Съобразяване на работата с бизнес целите на Възложителя.

За постигане на горните цели методологията е съсредоточена върху следните 9 сфери на знание:

- Управление на интеграцията,
- Управление на обхвата,

- Управление на времето,
- Управление на разходите,
- Управление на качеството,
- Управление на човешките ресурси,
- Управление на комуникациите,
- Управление на риска,
- Управление на доставките.

Съвместимост с други стандарти

Международната Асоциация по Управлението на Проекти (International Project Management Aassociation) е установила международно приет стандарт с Международни стандарти за сертифициране по управление на проекти, който е преведен на одобрените езици от националните сдружения на IPMA. Това е основата за четири степенната сертификационна програма на IPMA, която се използва по целия свят. PRINCE2 е съвместим с този стандарт.

PRINCE2 е главна ръководна методология, целяща да предостави механизъм за изграждането на структура, в която да протича проекта, както и неговото приключване с предаването му на оперативните отдели.

Има голяма съвместимост между PRINCE2 и PMBOK въпреки някои разлики в използваната терминология. Едната гледна точка е, че приемането на PRINCE2 ще подобри прилагането на стандартите на PMBOK като предоставя голяма дълбочина и структура на изграждането на обстановката на проекта, и предлага по-строг подход към изграждането, провеждането и приключването на индивидуалните проекти.

За областите, които не се покриват от PRINCE2 ще се прилагат съответните стандарти и ръководни принципи на PMBOK.

EVMS

Earned Value Management System (EVMS) е разработена от US DoD през 60-те години на 20-ти век като инструмент за финансов анализ, но с развитието си се е превърнала в основен раздел от управлението на проекти и проследяване на разходите. Основното преимущество в използването й е възможността да се оцени обективно хода на проекта. EVMS има уникалното свойство да комбинира обхвата, времето и разходите на проекта в единна измервателна система. При правилно използване, EVMS дава ранни предупреждения за проблеми в изпълнението на проекта. В добавка, EVMS помага за уточняването на обхвата на проекта, избягването на „scope creep", подобряването на комуникацията между заинтересованите лица и фокусирането на проектния екип върху постигането на прогрес в проекта.

ITIL

Библиотеката за инфраструктура на информационните технологии Information Technology Infrastructure Library (ITIL®) е набор от най-добри практики, които имат за цел да улеснят доставянето на висококачествени ИТ услуги. ITIL е набор от процедури за управление, които подпомагат бизнеса за достигане на качество и стойност в ИТ дейностите. Тези процедури се доставят независимо и осигуряват ръководство в целия обхват на ИТ инфраструктурата.

MSF

Microsoft® Solutions Framework (MSF) е приспособим подход за по-бързо успешно доставяне на технологични решения, с участието на по-малко хора и с по-нисък риск, като в същото време дава резултати с високо качество.

Екипът за помощ на MSF открива най-честите причини за техническия провал на проекта, подобрява степента на успех, качеството на решението и влиянието върху бизнеса. Освен това MSF:

- Подрежда техническите и бизнес целите
- Определя ясни цели за проекта, роли и отговорности
- Внедрява итеративен, milestone-driven процес
- Проактивно управление на риска
- Отговаря за въвеждане на ефективни промени

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

MOF

Целта на Microsoft Operations Framework (MOF) е да помогне на ИТ организациите да постигнат висока надеждност, достъпност, поддръжка, и управляемост в критични зони на системите.

Чрез прилагане на принципите на ITIL към технологичната платформа на Microsoft, MOF помага на ИТ организациите да посрещнат предизвикателствата описани по-горе и да следват целта за непрекъснато усъвършенстване.

MOF е набор от най-добри практики, принципи и модели, които представляват ръководство за управление на ИТ услугите в ИТ организациите.

Построен на базата на ITIL от британската правителствена агенция (Office of Government Commerce) в Обединеното Кралство, MOF е основа за управление на дейностите и поддържане на ИТ системите. Методът е приспособим към променящите се бизнес нужди и оптимизира процесите за по-голяма ефективност.

Microsoft Project

Microsoft Project (или MSP) е софтуерна програма за управление на проекти, разработена и продавана от Microsoft, която е проектирана да помага на ръководителя на проекта в разработването на планове, назначаване на задачи на ресурсите, проследяване на прогреса, управление на бюджета и анализиране на работната натовареност. Приложението създава план на критичния път. Графиците могат да бъдат изравнени по ресурси и веригите се визуализират в диаграма на Гант. Microsoft Office Project предлага инструменти за управление на проекта с подходяща комбинация от използваемост, мощност и гъвкавост, така че процесите да се управляват по-ефективно. По този начин ръководителя на проекта е информиран и контролира работата по проекта, графиците и финансите, поддържа екипа на проекта синхронизиран и е по-продуктивен при интегрирането с проекти, има възможност за множество отчети, планиране и не на последно място гъвкави средства за обработка.

Microsoft Visio

Microsoft Office Visio улеснява визуализирането, разучаването и предаването на сложна информация от ИТ и бизнес специалисти. За разлика от сложните текстове и таблици, които са трудни за разбиране диаграмите на Visio, предават необходимата информацията от пръв поглед. Вместо статистически рисунки се създават диаграми със свързани данни на Visio, които лесно се актуализират и по този начин се увеличава продуктивността. Голямото разнообразие от диаграми в Office Visio позволява да се представи различна информация относно организацията, ресурсите и процесите в дадена компания.

Предлаганата проектна методология се базира на световно утвърдени стандарти и добри практики и включва подробно описание на:

- Проектните дейности и оценка на сроковете (детайлизиран План за изпълнение);
- Организационната структура на партньорите в дружеството и връзки за взаимодействие с Възложителя;
- Фазите/етапите, през които преминава управлението на проекта и изпълнението на софтуерната разработка;
- Описание на ролите и отговорните на ключовите експерти в екипа на Изпълнителя;
- Проектна комуникация и доклади – методики/канали на комуникация, периодичност и съдържание на докладите.

2. Фази, през които минава управлението на проекта

Управлението на проект е прилагане на знания, умения, инструменти и техники към дейностите по проекта, за да се удовлетворят изискванията и да се постигнат целите на проекта.

В методологиите за управление на проекти няма предписание за точен брой фази, през които да премине изпълнението.

Рамката, която ще се използва от Изпълнителя при управлението на проекта е базирана на пет основни групи процеси, през които ще мине изпълнението на проекта:

- Иницииране – процесът, отбелязващ началото на проекта.
- Планиране – процесът за създаване на плановете, които ще ръководят изпълнението.
- Изпълнение – процесът за изпълнение на плановете и изработване на резултата.

- Наблюдение и контрол – процесът, който сравнява резултатите с плановете и прави корекции, необходими за бъдещата работа.
- Приключване – процесът, с който се завършва фаза на изпълнение или целият проект, създават се записи и архивна информация за изпълненото.

Като основни опорни точки в управлението на проекта ще служат и десетте основни области на познанието, които екипът на Изпълнителя познава в детайли и прилага богатия си опит при изпълнение на проекти:

- Управление на интеграцията – фокусиране върху всички елементи на проекта на по-високо ниво, за да се гарантира отлична координация и изпълнение на проекта.
- Управление на обхвата – контрол на обхвата чрез управление на изискванията, детайлите и процесите. Промените в обхвата се управляват чрез структурирани процедури и контролирано.
- Управление на времевата рамка – отнася се основно за ресурсите, дейностите, графика и управлението на графика.
- Управление на разходите – постоянно наблюдение и контрол на разходите спрямо времето, обхвата, качеството и риска, за да бъде сигурно, че изпълнението на проекта остава реалистично и с ясно дефинирани резултати.
- Управление на качеството – постоянно наблюдение и контрол на качеството, базирано на факта, че поправянето на грешка в процеса на изпълнение на проекта струва много повече, отколкото усилията да бъде предотвратена.
- Управление на персонала – важно е да бъде ясно дефинирана всяка роля и отговорностите на всеки участник в проекта.
- Управление на комуникациите – важно е да се знае кои са заинтересованите лица в проекта и какво им е необходимо да знаят. Управление на докладването и отчетността по време на изпълнението на проекта е важен фактор за неговия успех.
- Управление на риска – анализът на риска и начините за намаляване на влиянието на рисковете е изключително важна област на познанието при управлението на проекта и в настоящото предложение има отделна точка.
- Управление на доставките – поръчката и доставката на оборудване и лицензи също е част от управлението на проекта и от това зависи успешното и навременно внедряване на системата при Възложителя.
- Управление на заинтересованите лица – управление на очакванията, които водят до удовлетвореност на заинтересованите лица. Може още да бъде дефинирано като „създаване и поддръжка на отношения с цел да се задоволят нужди". Заинтересованите лица в проекта имат очаквания и нужди, които първо трябва да бъдат идентифицирани и разбрани, преди да бъде направен план за управлението им.

2.1. Управление на интеграцията

Процесите по управление на интеграцията гарантират правилната координация на различните елементи на проекта. Те включват балансиране на целите и алтернативите с оглед на нуждите и очакванията на заинтересованите страни. Описаните в тази точка процеси са предимно интегративни.

- Разработване на план на проекта / план за управление на услугата
  При разработването на плана на проекта / план за управление на услугата се използват резултатите от други планиращи процеси, включително стратегическо планиране, за да се създаде един ясен и последователен документ, който да насочва и изпълнението, и контрола на проекта. Този процес минава през няколко итерации. Сборът от всички интегрирани планове за управленски контрол съставлява обхвата на проекта.
- Изпълнение на плана на проекта / плана за управление на услугата
  Изпълнението на плана на проекта / плана за управление на услугата е основен процес при осъществяването на плана – преобладаваща част от бюджета и усилията по проекта се изразходват при извършването на този процес. Чрез него ръководителят на проекта и

неговия екип координират и насочват техническите и организационните интерфейси. В рамките на този процес фактически се предоставя услугата, предмет на проекта. Изпълнението постоянно се сравнява с основния план на проекта, за да се вземат своевременни коригиращи мерки. В подкрепа на анализа се правят периодични прогнози за окончателните разходи и резултати.

- Интегриран контрол на промените
  Интегрираният контрол на промените се занимава с факторите, които влияят върху пораждането на промени, грижи се за съгласуването на промените, констатира наличието на промени и ги управлява, когато възникнат.

Първоначално дефинираният обхват и интегрираният основен план на проекта се поддържат чрез постоянно управление на възникналите промени чрез приемане или отхвърляне на промените и включването им в актуализираната версия на основния план. Интегрираният контрол на промените предоставя:

- Поддържане интегритета на базовите измерители на изпълнението.
- Отразяване на промените в обхвата на продукта във вече дефинирания обхват.
- Координиране на промените във всички сфери на знание.

2.2. Управление на обхвата

Управлението на обхвата на проекта включва процесите, които гарантират, че проектът включва цялата необходима работа и само необходимата работа за успешното осъществяване на проекта. То се занимава най-вече с определянето и контролирането на това какво е включено и какво не е включено в проекта.

- **Стартирането** е процесът на официалното възлагане на нов проект. Официалното възлагане на този проект е подписването на договор, което свързва проекта с работата на изпълнителя.
- **Планирането** на обхвата е процесът на детайлизиране и документиране на работата по проекта (обхвата на проекта), чийто резултат е описание на предоставяните услуги по проекта. Описанието на услугите обхваща изискванията, които отразяват съгласуваните нужди на клиента, и план, който отговаря на тези изисквания. Резултатите от планирането на обхвата са Дефиниция на обхвата и План за управление на обхвата. Дефиницията на обхвата е основата за постигане на споразумение между Възложителя и Изпълнителя, чрез идентифициране на целите и резултатите по проекта. След стартирането на проекта екипа разработва множество дефиниции на обхвата, в съответствие с нивото на детайлизиране на работата (напр. системен анализ, подробен график и др.).
- **Определянето** на обхвата включва разбиването на основните резултати, посочени в Дефиницията на обхвата, на по-малки, по-управляеми елементи. Целта е:
  - Подобряване на прогнозите за разходи, продължителност и ресурси;
  - Определяне на основни параметри за измерване на изпълнението и контрол;
  - Ясно разпределяне на отговорностите.
- **Потвърждаването** на обхвата е процесът по официално приемане на обхвата на проекта от заинтересованите страни. Той изисква преглед на резултатите от работата и потвърждение, че всичко е свършено както трябва.
- **Контролът** на промените в обхвата се занимава с факторите, които влияят върху пораждането на промени, грижи се за съгласуването на промените, констатира наличието на промени и ги управлява, когато възникнат.

2.3. Управление на времевата рамка

Управлението на времето по проекта включва следните процеси, необходими за навременното приключване на проекта:

- Определяне на дейностите – идентифициране и документиране на конкретните дейности, необходими за постигане на набелязаните резултати и подрезултати. Определянето на

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

дейностите се съгласува с Дефиницията на обхвата и включва детайлизиране, предположения и ограничения.

- Последователност на дейностите - идентифициране и документиране на логическите взаимозависимости. Дейностите трябва да бъдат в правилна последователност, за да спомогнат за разработването на реалистичен и постижим график. Последователността може да следва критичната пътека. В резултат се определя график със съответните контролни точки и зависимости.
- Продължителност на дейностите – определя се въз основа на информацията за обхвата на проекта и ресурсите. Предварителната оценка ще се детайлизира в хода на работата, предвид наличието и качеството на входящите данни. Оценката се прави по методологията на критичната пътека.
- Определяне на график – задава се началната и крайната дата на дейностите по проекта. Процесът преминава през няколко итерации преди окончателното определяне на графика на проекта.
- Контрол на графика – занимава се с факторите, които влияят върху пораждането на промени, грижи се за съгласуването на промените, констатира наличието на промени и ги управлява, когато възникнат.

2.4. Управление на качеството

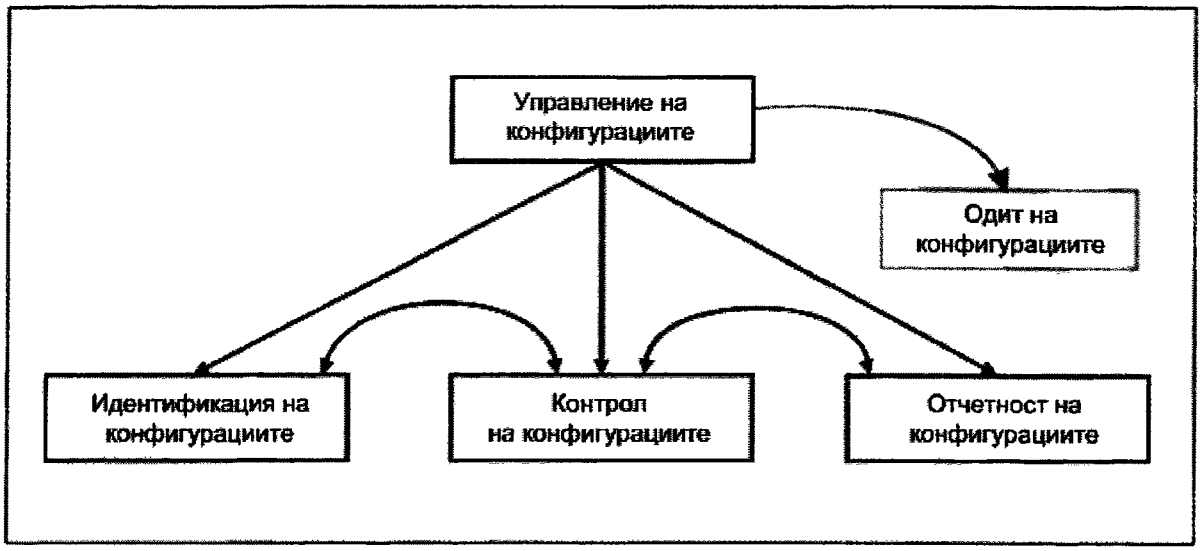
Целта на процесите по управление на качеството е да бъдат задоволени нуждите, заради които е предприет проектът. Тези процеси включват всички дейности от цялостното управление на проекта, които определят политиката, целите и отговорностите по качеството и ги осъществяват чрез планиране на качеството, гарантиране на качеството, качествен контрол и подобряване на качеството в рамките на системата за качество.

- Задачи и цели по качеството, периоди и жизнения цикъл на системата
- Планиране на качеството – идентифициране на стандартите за качество за конкретния проект и начините за спазването им. Това е един от ключовите процеси при планиране на качеството и ще се извършва редовно, успоредно с останалите процеси по планиране на проекта.
- Гарантиране на качеството – всички планирани и систематични действия в рамките на системата за качество, които дават увереност, че проектът отговаря на съответните стандарти. Извършва се в хода на целия проект от вътрешни Специалисти по качеството.
- Качествен контрол – проследяване на конкретни резултати, за да се определи дали отговарят на зададените стандарти и да се набележат начини за отстраняване на причините за незадоволителните резултати. Извършва се в хода на целия проект. Резултатите включват както доставката на конкретен резултат, така и резултати от управлението на проекта (изпълнение на графика). Необходимо е да се разграничават:
  - Предотвратяване (недопускане на грешки в процеса) и проверка (недопускане на грешки от страна на клиента);
  - Изпробване на атрибути (резултатът отговаря или не отговаря) и изпробване на променливи (резултатите се измерват по прогресивна скала за степен на съответствие);
  - Специални причини (необичайни събития) и случайни причини (нормално отклонение от процеса);
  - Допустимост (резултатът е приемлив, ако попада в посочения обхват на допустимост) и контролни граници (процесът е под контрол, ако резултатът е в рамките на контролните граници).

2.5. Управление на конфигурациите/промените

Управлението на промените е тясно свързано с управление на конфигурациите.

Управлението на конфигурациите има за цел да се поддържа контрол над конфигурационните елементи в хода на изпълнение на проекта. То се състои от три основни елемента: идентификация на конфигурациите, контрол над конфигурациите, и отчетност на конфигурациите.



Идентификация на конфигурация е именуване на документация, на всеки компонент (документ единица, модул, подсистема, и система за), така че във всеки даден момент, определен компонент може да бъде еднозначно идентифициран.

Контролът на конфигурацията е дейност, която не позволява въвеждането на не-упълномощени промени на конфигурационен елемент. Всяка промяна се проверява за необходимост и коректност, преди да бъде одобрена и въведена, така се упражнява и контрол.

Чрез отчетност на конфигурациите се следи състоянието на всеки компонент. Предоставя се най-новата версия при актуализация на всеки компонент. По този начин, при необходимост от промени или други дейности по отношение на компонент, правилната версия на компонента е винаги на разположение. С цел проследимост, се съхраняват и предишните версии на компонентите. Предоставя се визуален интерфейс за сравняване на промените между една или няколко версии.

Управлението на промените става чрез процедура за промяна, която е тясно свързана с процедурите по управление на конфигурациите и управление на качеството.

Класификацията на промените е показана в следващата таблица:

Тип промяна	Описание
Адаптивни	Необходими промени, на системата, в резултат на променящата се среда
Коригиращи	Фиксиране на дефекти
Подобрения	Подобрения изискуеми от възложителя
Други	Друг тип на промяна изискваща процеса на промяна. Естеството на промяната трябва да бъде отразена
Промяна на данни	Коригиране на грешни данни

2.5.1. Контролни точки в процеса на промяна

- Преглед и одобряване на оценка на въздействието, включително решението да се премине към реализация на промяната
- Одобрение за промяна
- Одобрение за завършване на процеса на промяната

2.5.2. Процедурата за контрол на промените

- Процедурата за контрол на промените ще гарантира, че предложените промени в системата са оценени и приложими:
- Подаване на Искане на промяна;
- Анализ на Искането за промяна;
- Оценка на цената (време, усилия, средства) на Искането за промяна;
- Прилагане на Искането за промяна;

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

- Поддържане на история / проследимост на Исканията за промяна.

2.5.3. Методика за диагностициране и превантивни дейности

- За диагностицирането на проблеми и потенциални уязвимости се използват всички стандартни средства, налични в системата:
- Преглед на съдържанието на журнални файлове с цел идентификация на причините за възникване на инцидента;
- Анализ на последиците с използване на програмните средства за диагностика, налични в системния софтуер (операционна система, Application Server, конзоли за управление (iLO) и други);
- Специализирани софтуерни решения за наблюдения на мрежови трафик;
- Анализ на базата на сравнение със събрани статистики за натоварване на системите от предишни период;

2.6. Управление на човешките ресурси

Управлението на човешките ресурси включва процесите, които осигуряват най-ефективното използване на хората, участващи в проекта. То обхваща всички заинтересовани страни – клиенти, партньори, индивидуални изпълнители и др. Състои се от:

- Организационно планиране — идентифициране, документиране и определяне на роли, отговорности и канали за отчитане;
- Набиране на персонал — осигуряване на необходимите човешки ресурси и включването им в работата по проекта;
- Развитие на екипа — развиване на индивидуални и групови умения, с цел подобряване на изпълнението.

2.7. Управление на риска

Управлението на риска е систематичният процес по идентифициране, анализиране и реагиране на рисковете по проекта. То включва максимизиране на вероятността и последствията от благоприятни събития и минимизиране на вероятността и последствията от нежелателни за проекта събития. Проектният риск е несигурно събитие или състояние, което, ако се случи, има положително или отрицателно влияние върху целите на проекта. Рискът има причина и, ако се материализира, последствие.

Предложението за управлението на риска при изпълнението на настоящата поръчка е описано в Приложение 4 – приложен към техническото предложение документ.

2.8. Управление на комуникациите

Процесите по управление на комуникациите осигуряват навременното и адекватно генериране, събиране, разпространение, съхранение и унищожаване на информацията по проекта. Те осъществяват критичната за успеха връзка между хора, идеи и данни. Всеки участник в проекта трябва да е готов да изпраща и приема комуникации и трябва да разбира как каналът на комуникация, в която участва, се отразява на целия проект.

- Планиране на комуникациите – определяне на нуждите на заинтересованите страни от информация и комуникации: кой от каква информация се нуждае, как ще я получи и от кого. Нуждата от предоставяне на информация за проекта е общовалидна, но информационните нужди и методите на разпространение са различни за всеки проект. Идентифицирането на нуждата от информация и разпространяването ѝ по подходящ начин е важен фактор за успех на проекта;
- Разпространение на информацията – своевременното достигане на информацията до заинтересованите страни. Включва прилагането на Плана за комуникация и откликването на неочаквани искания на информация;
- Отчитане на изпълнението – събиране и разпространение на данни за изпълнението, показателни за използването на ресурсите за постигане на целите на проекта. Този процес включва:

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

- Отчитане на състоянието — описва докъде е стигнал проектът в дадения момент;
- Отчитане на напредъка — описва какво е постигнал екипът по проекта;
- Прогнозиране — предполага бъдещото състояние и напредък по проекта;
- Отчитане на изпълнението – данни за обхвата, графика, разходите и качеството.

- Административно приключване: след постигане на целите или след прекратяване по други причини, проектът или фазата трябва да приключи. Административното приключване се състои от документиране на резултатите, с цел официалното приемане на продукта от страна на клиента. То включва събиране на проектната документация, която отразява окончателните спецификации, анализ на успеха и ефективността на проекта и на извлечените поуки, и архивиране на тази информация за бъдещо ползване. Дейностите по административното приключване не се отлагат до приключването на проекта. Всяка фаза трябва да бъде надлежно приключена, за да не бъде загубена тази важна и полезна информация.

2.9. Процедури и документи от СУКИС на Изпълнителя

По време на изпълнение на дейностите по предмета на поръчката, ще бъдат прилагани следните процедури, част от Системата за Управление на Качеството и Информационната Сигурност (СУКИС) на Изпълнителя:

LPP002 – Идентификация и проследимост на продукти и услуги;
LPP003 – Работа с продукти на клиент;
LPP004 – Манипулиране, съхранение, опаковане и доставка на продукти;
LPP007 – Управление на конфигурациите;
LPP009 – Управление на outsourcing процеси;
LPP012 – Управление на промените;
LPP013 – Управление на външни ИТ услуги;
LPP301 - Организация и управление на мрежово сервизно обслужване (Support)
LAP001 - Измерване степента на удовлетвореност на клиентите
LAP004 – Работа с продукти, несъответстващи на определените изисквания;
LSP001 – Управление на информационната сигурност;
LSP200 – Управление на риска;
LSP900 – Непрекъсваемост на бизнес процесите
LSP702 – Управление на капацитета;
LPI301 - Сервизно поддържане на мрежови решения (Support)
LPN002 – План за управление на външна услуга.

Процесите, описани в процедурите по-горе ще бъдат интегрирани в плана за управление на услугите. Съгласно изискванията на стандарта ISO 20000-1:2011 и процедурите в СУКИС, Изпълнителят изготвя план за управление за всяка услуга при различните клиенти. Освен регулярните одити по стандарта, дейностите на Изпълнителя и плановете за управление на предоставяните услуги са били одитирани ежегодно от водещи доставчици на ИТ продукти (напр. CISCO, HP и др.), както и от наши клиенти, включително и фармацевтични компании известни с високите стандарти и строгия контрол в сектора. След проведени одити фармацевтичните компании приемат Изпълнителя за доверен партньор и доставчик.

Изпълнителят предоставя услугите точно и с грижата на добър търговец, като ползва в максимална степен експертните познания на доказалия се екип от професионалисти, за осигуряването и използването на най-ефективни способи за предоставянето на услугите.

Изпълнителят ще предоставя услугите съгласно изискванията посочени в Техническата спецификация, а когато те не са подробно описани, по начин, съгласуван с Възложителя. Изпълнителят спазва и предприема необходимото, така че нашите служители да спазват точно изискванията на приложимото право и вътрешната Система за Управление на Качеството и Информационната Сигурност (СУКИС) по повод на здравословните и безопасни условия на труд и изискванията на Възложителя за безопасност при работа. Изискванията са част от СУКИС и са дефинирани във вътрешна процедура LRP004 и инструкция LRI004.

Изпълнителят предоставя на Възложителя документи и сертификати, които доказват качеството на продуктите и услугите, които предоставяме, съгласно изискванията в тръжната документация.

3. Разпределение на ролите и ресурсите при изпълнение на предмета на поръчката

3.1. Екип за изпълнение на поръчката

- Екип на Възложителя – предварителна оценка за основните отговорности

Във връзка с успешното изпълнение на проекта и необходимостта от осигуряване на съдействие, Изпълнителят очаква информация за обособен екип за управление на проекта от страна на Възложителя.

Предварителна оценка на основни отговорности:

- Контрол и наблюдение на изпълнението;
- Участие в работни срещи и срещи за статуса на изпълнение на проекта;
- Съдействие за осигуряване на информация, свързана с изпълнение на задълженията по проекта и уточняване на въпроси;
- Приемане, съгласуване и утвърждаване на документи, свързани с изпълнението на проекта – технически и административни;
- Предоставяне на работно помещение за двама специалисти на Изпълнителя;
- Разписване на приемо-предавателни протоколи;
- Оказват организационно-техническа помощ за успешното осигуряване на изпълнението на задачите в частта им от компетентността на Възложителя;
- Координират и своевременно осигурят необходимата информация;
- Решават възникнали проблеми в процеса на ескалация, които са от тяхната компетенция.

- Екип на Изпълнителя

Всички експерти, които играят основна роля в изпълнението на настоящата поръчка, се наричат Ключови експерти.

За изпълнението на проекта дружеството формира екип за изпълнение на проекта от ключови експерти, както следва:
Ключов експерт № 1 – Ръководител на екипа (проекта)– Николина Петрова
Ключов експерт № 2 – Експерт поддръжка на сървърни операционни системи – Светослав Манев
Ключов експерт № 3 – Експерт електронна пощенска услуга – Христо Христов
Ключов експерт № 4 – Експерт мрежова инфраструктура – Данчо Митев
Ключов експерт № 5 – Експерт мрежова сигурност – Петър Петров
Ключов експерт № 6 – Експерт поддръжка на софтуерни телефонни централи – Здравко Ножаров
Ключов експерт № 7 – Експерт информационна сигурност - Боян Янчев

Подробна информация за тях е дадена в приложен Списък с експертите, попълнен по образец и приложен към техническото предложение.

Матрица на отговорностите е представена в следващата таблица:

№	Описание на дейности при изпълнение на договора	Ключов експерт №1 – Ръководител на екипа	Ключов експерт № 2 – Поддръжка на сървърни операционни системи	Ключов експерт № 3 – Електронна пощенска услуга	Ключов експерт № 4 – Мрежова инфраструктура	Ключов експерт № 5 – Мрежова сигурност	Ключов експерт № 6 – Поддръжка на софтуерни телефонни централи	Ключов експерт № 7 – Информационна сигурност	Хелпдеск специалисти	Ръководител по качество	Експерт по оценка на риска	Експерт логистика	Администратор на проекта
	Услуги по отношение на сървърите												
1.	Мониторинг на Windows/Unix/Linux базирани системи		X						X				
2.	Наблюдение на системните съобщения за грешки		X						X				
3.	Наблюдение на състоянието на архивите		X						X				
4.	Наблюдение на състоянието на планираните задачи		X						X				
5.	Наблюдение на състоянието на хардуера		X						X				
6.	Администриране на Windows/Unix/Linux базирани системи		X						X				
7.	Администриране на виртуална инфраструктура		X						X				
8.	Администриране на архивите		X						X				
9.	Администриране на кръпки по сигурността (Security Patches Management)		X						X				
10.	Възстановяване на работоспособността на ОС / СУБД, комуникационната свързаност в случай на срив		X		X				X				
	Инфраструктурни услуги												
11.	Наблюдение на инфраструктурни услуги		X						X				
12.	Администриране на MS Active Directory, DNS, DHCP, файлови		X						X				

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

№	Описание на дейности при изпълнение на договора	Ключов експерт №1 – Ръково-дител на екипа	Ключов експерт № 2 – Поддръжка на сървърни операционни системи	Ключов експерт № 3 – Електронна пощенска услуга	Ключов експерт № 4 – Мрежова инфра-структура	Ключов експерт № 5 – Мрежова сигурност	Ключов експерт № 6 – Поддръжка на софтуерни телефонни централи	Ключов експерт № 7 – Инфор-мационна сигурност	Хелпдеск специа-листи	Ръково-дител по качество	Експерт по оценка на риска	Експерт логис-тика	Администр-атор на проекта
	сървъри												
	Услуги по отношение на специализирания приложен софтуер												
13.	Инсталиране на специализиран приложен софтуер (на сървърите) при закупуване или подмяна на технически и програмни средства		X						X				
14.	Обновяване на инсталирания специализиран приложен софтуер		X					X	X				
15.	Периодично наблюдение и осигуряване на нормално функциониране на специализираните приложни системи		X					X	X				
16.	Администриране на приложен софтуер - поддържане на актуални потребители и други административни функции		X					X	X				
17.	Оказване на системна помощ на потребителите на специализираните приложни системи		X	X					X				
18.	Управление на MS Exchange 2010, осигуряване на достъп до MS Exchange сървър чрез клиентски програми от компютри и мобилни устройства в МТСП и отдалечено по гарантиран		X	X					X				

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

№	Описание на дейности при изпълнение на договора	Ключов експерт №1 – Ръково-дител на екипа	Ключов експерт № 2 – Поддръжка на сървърни операционни системи	Ключов експерт № 3 – Електронна пощенска услуга	Ключов експерт № 4 – Мрежова инфра-структура	Ключов експерт № 5 – Мрежова сигурност	Ключов експерт № 6 – Поддръжка на софтуерни телефонни централи	Ключов експерт № 7 – Инфор-мационна сигурност	Хелпдеск специа-листи	Ръково-дител по качество	Експерт по оценка на риска	Експерт логис-тика	Администр-атор на проекта
	сигурността												
19.	Достъп на потребителите от МТСП до Интранет и Интернет		X						X		X		
	Услуги по отношение на базата от данни												
20.	Архивиране на базите данни на МТСП		X										
21.	Администриране на наличните бази от данни по установени еталони и модели		X										
22.	Ежедневно архивиране на статистическите файлове		X										
23.	Промяна на системни настройки на БД- след съгласуване с ВЪЗЛОЖИТЕЛЯ		X										
24.	Отстраняване на възникнали проблеми в БД, като в случай на необходимост действията се съгласуват с външни организации		X										
	Услуги по отношение на поддръжката на потребителски компютри в ИТ инфраструктурата на МТСП												
25.	Поддръжка в изправност на операционни системи и приложно програмно осигуряване		X						X				
26.	Възстановяване на операционни системи и приложно програмно осигуряване		X						X				

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

№	Описание на дейности при изпълнение на договора	Ключов експерт №1 – Ръково-дител на екипа	Ключов експерт № 2 – Поддръжка на сървърни операционни системи	Ключов експерт № 3 – Електронна пощенска услуга	Ключов експерт № 4 – Мрежова инфра-структура	Ключов експерт № 5 – Мрежова сигурност	Ключов експерт № 6 – Поддръжка на софтуерни телефонни централи	Ключов експерт № 7 – Инфор-мационна сигурност	Хелпдеск специа-листи	Ръково-дител по качество	Експерт по оценка на риска	Експерт логис-тика	Администр-атор на проекта
27.	Първоначална диагностика на потребителско оборудване при наличие на проблем								X				
28.	Обновяване на версиите на операционните системи и приложния софтуер		X				X		X				
29.	Инсталиране на кръпки по сигурността (Security Updates)		X					X	X				
30.	Инсталиране на нов приложен софтуер		X						X				
31.	Инсталиране на нов системен софтуер		X						X				
32.	Конфигуриране на хардуер на нови закупени/наети работни станции и мобилни компютри								X				
	Услуги по отношение на комуникационното оборудване												
33.	Конфигурация и преконфигурация на комуникационното оборудване и преносната среда. Сваляне и запазване на конфигурациите на активното мрежово оборудване. Поддържане на база от данни за текущите и миналите конфигурации на активното оборудване				X	X	X		X				
34.	Конфигуриране на ново закупено/наето комуникационно оборудване				X	X	X		X				

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

№	Описание на дейности при изпълнение на договора	Ключов експерт №1 – Ръководител на екипа	Ключов експерт № 2 – Поддръжка на сървърни операционни системи	Ключов експерт № 3 – Електронна пощенска услуга	Ключов експерт № 4 – Мрежова инфраструктура	Ключов експерт № 5 – Мрежова сигурност	Ключов експерт № 6 – Поддръжка на софтуерни телефонни централи	Ключов експерт № 7 – Информационна сигурност	Хелпдеск специалисти	Ръководител по качество	Експерт по оценка на риска	Експерт логистика	Администратор на проекта
35.	Допълнително преконфигуриране на ИТ инфраструктурата, при необходимост				X	X	X		X				
36.	Наблюдение и анализ на функционирането на комуникационното оборудване. Измерване и анализ на параметрите на трафика и предложения за оптимизации на комуникационното оборудване				X	X	X		X				
37.	Мониторинг и управление на комуникационната инфраструктура				X	X	X		X				
38.	Консултации по телефон и e-mail				X	X	X		X				
39.	Поддържане на актуална база данни относно видовете активно оборудване, комуникационни връзки и др				X		X	X		X			
40.	Системна администрация и наблюдение на интегриран с активната директория уеб филтър и защитна стена		X		X	X		X					
41.	Оказване на техническа помощ и консултации		X		X		X	X		X	X		
42.	Конфигуриране и настройка на оборудването при необходимост		X		X		X						
43.	Поддържане, обновяване и		X	X	X			X		X			

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

№	Описание на дейности при изпълнение на договора	Ключов експерт №1 – Ръководител на екипа	Ключов експерт № 2 – Поддръжка на сървърни операционни системи	Ключов експерт № 3 – Електронна пощенска услуга	Ключов експерт № 4 – Мрежова инфраструктура	Ключов експерт № 5 – Мрежова сигурност	Ключов експерт № 6 – Поддръжка на софтуерни телефонни централи	Ключов експерт № 7 – Информационна сигурност	Хелпдеск специалисти	Ръководител по качество	Експерт по оценка на риска	Експерт логистика	Администратор на проекта
	конфигуриране на системата за мониторинг и управление на мрежата												
44.	Хардуерна и софтуерна поддръжка на описаното в договора оборудване от производителя или от негов оторизиран представител		X	X	X		X	X		X			
45.	Поддържане, конфигуриране, настройка и обновяване на софтуера на описаното в договора оборудване		X		X								
46.	Поддържане на детайлно техническо описание на мрежата и на техническите и програмни средства				X								
47.	Поддържане на актуална регистрация на описаните в договора устройства в системата за мониторинг и управление на мрежата		X	X	X				X				
48.	Ремонт на всички установени повреди (хардуер и софтуер) на оборудването, предмет на договора, компоненти към него, включително подмяна на повредени модули с нови такива		X	X	X				X				
49.	Отстраняване на възникнали неизправности,		X	X	X				X				

№	Описание на дейности при изпълнение на договора	Ключов експерт №1 – Ръководител на екипа	Ключов експерт № 2 – Поддръжка на сървърни операционни системи	Ключов експерт № 3 – Електронна пощенска услуга	Ключов експерт № 4 – Мрежова инфраструктура	Ключов експерт № 5 – Мрежова сигурност	Ключов експерт № 6 – Поддръжка на софтуерни телефонни централи	Ключов експерт № 7 – Информационна сигурност	Хелпдеск специалисти	Ръководител по качество	Експерт по оценка на риска	Експерт логистика	Администратор на проекта
	дефекти и функционални откази												
50.	Оказване на техническа помощ и консултации		X	X	X	X							
51.	Изготвяне и предаване на месечни отчети	X	X	X	X			X		X	X		X
	Общи административни задачи и управление на услугите												
52.	Планиране на работата и организация на екипа	X											
53.	Комуникация и кореспонденция с Възложителя	X											
54.	Управление на риска при изпълнение на договора: оценка, анализ, противодействие на риска	X									X		X
55.	Управление на качеството при изпълнение на договора	X						X		X	X		
56.	Приемане на заявки за проблеми и участие в ежедневната поддръжка								X				
57.	Управление и наблюдение на спазването на политиката за сигурност на информацията при изпълнение на договора							X					
58.	Организира и следи за ресурсното осигуряване при изпълнение на договора											X	X

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

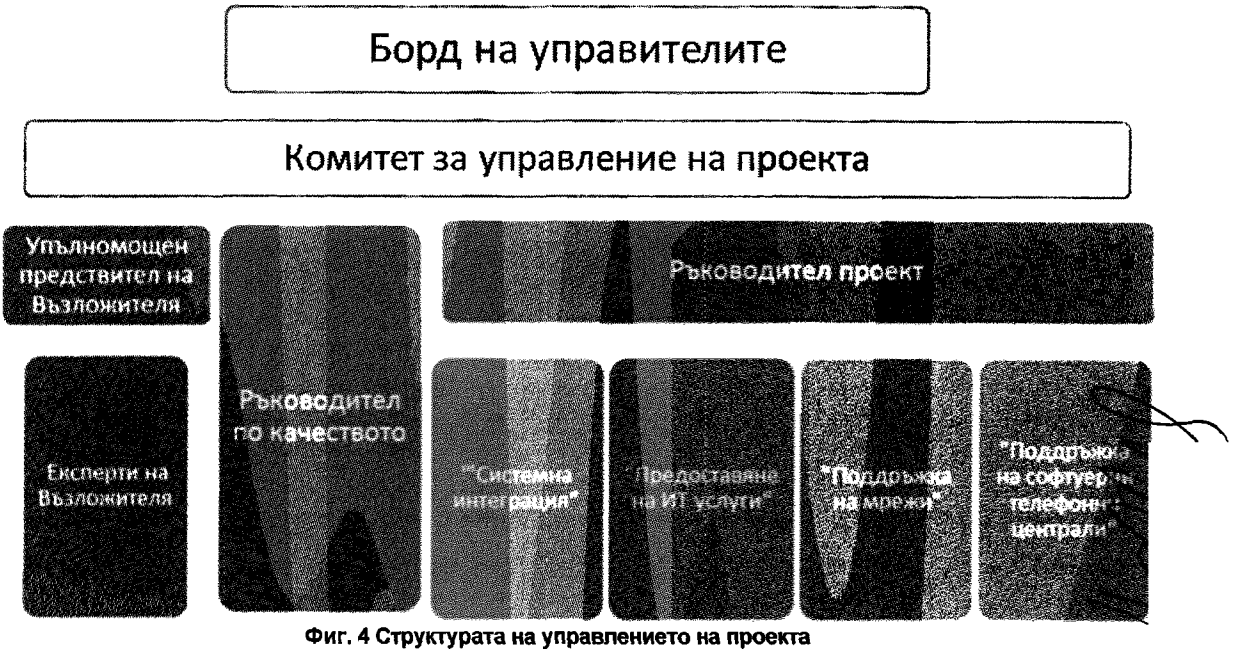
3.2. Организация, структура и отговорности на екипа

- ***Управление на проекта***

Организацията на проекта се базира на методология, използвана от екипа на Изпълнителя. Тази методология е доказана по време на изпълнението на многобройни и сложни проекти.

Успешното реализиране на този проект изисква създаването и използването на овластен персонал на управленско ниво от Възложителя и Изпълнителя.

Предложена е следната структура на управление на проекта:



Фиг. 4 Структурата на управлението на проекта

Структурата на управлението на проекта, показана на фиг. 4, се състои от ролите и отговорностите, които способстват за поставянето на една маса на различните интереси и уменията на екипите, по този начин осигурявайки изпълнението на комплексните изисквания на проекта.

За да бъде един проект успешен е важно долуспоменатите роли да се дефинират още в началото му и съответните лица да бъдат запознати с техните права и отговорности в рамките на текущия проект.

Структурата на екипа за управлението на проекта е специално избрана да управлява проекта до неговото успешно приключване и да посрещне изискванията от заданието. Изготвената структура взема под внимание комуникационните схеми и се базира на описание на работата, която определя точно отговорностите, целите, ограниченията на правомощията, връзките, уменията, познанията и опита необходим за всички роли в организацията на проекта.

Бордът на управителите е най-високото ескалационно ниво, членовете на което имат пълномощията да вземат управленски и стратегически решения при необходимост.

На ръководителите на проекта и на екипа са дадени правомощия да ръководят ежедневната работа по проекта от името на Комитета за управление на проекта в рамките на ограниченията наложени от Борда на управителите.

Ръководителят на екипа контролира и следи изпълнението на задачите на високо ниво спрямо представения и утвърден план. Експертите на Възложителя в различните области подпомагат за технически становища и решения.

Ръководителят на проекта организира, координира и отчита от страна на Изпълнителя изпълнението на всички дейности по договора, включени в предмета на обществената поръчка, да отговаря за организацията и оперативната работа на Изпълнителя по договора, за останалите експерти и персонал на Изпълнителя, ангажирани в изпълнението, включително ако има подизпълнител/и, да поддържа контакти с Ръководителя проект на Възложителя и да подписва от страна на Изпълнителя протоколи, уведомления и др., да изпълнява и други правомощия, посочени от Изпълнителя в неговото пълномощно или предвидени в Договора за изпълнение, съгласува

предадените документи и продукти с екипа на Възложителя, отговаря за управлението на риска, решаване на затруднения, проблеми и ескалация при необходимост.

Ръководителят по качеството следи за спазване на утвърдените стандарти и политики по качеството при изпълнение на услугите.

- ***Модел на комуникация***

Моделът на комуникация и управление се базира на организационната структура показана на фигурата по-долу:



Фиг. 5 Комуникация в рамките на проекта

- ***Борд на управителите на проекта***

Бордът на управителите на проекта (Project Steering Board) представлява неформална единица на отговорните лица от страна на Изпълнителя и на Възложителя, които лично или чрез упълномощени лица полагат подписа си под договора, който представлява формалното споразумение за започване на изпълнението на проекта и определят основните рамки и стратегическите цели на проекта като цяло.

Ролята на Борда на управителите на проекта е да:

- Осигури управленските насоки на екипа на проекта;
- Гарантира, че всички резултати на проекта са в съответствие с договора;
- Решава проблеми, които не могат да се решат от Комитета за управление на проекта.
- Служи за крайна ескалационна точка.

- ***Комитет за управление на проекта***

Комитетът за управление на проекта отговаря за следните дейности:

- Одобрява плана за изпълнение на проекта;
- Преглежда прогреса, достигнат в предишния период, спрямо графика на проекта;
- Преглежда и одобрява план за следващия период;
- Одобрява двустранни документи и протоколи от собствената си компетенция;
- Решава проблеми, които не могат да се решат от ръководителя на проекта;
- Преглежда и решава проблеми или ги ескалира с препоръки до Борда на управителите на проекта;
- Определя приоритетите и съгласува подробните планове за действия.

- ***Ръководител на проекта***

Ръководителят на проекта изпълнява следните дейности:

- Контролира прогреса, достигнат в предишния период, спрямо графика на проекта;
- Контролира и одобрява план за следващия период;
- Контролира и одобрява двустранни документи и протоколи за приключване на етапи;
- Контролира решаването проблеми или ги отнася с препоръки до Комитета за управление на проекта;
- Провежда политиките на проекта заложени в договора;
- Контролира и отчита изпълнението на дейностите спрямо подробните планове и график;
- Контролира спазването на приоритетите и предлага подробните планове за действия;
- Планиране на изпълнението на задачите;
- Контрол и наблюдение на изпълнението на задачите;
- Контрол на качеството – заедно с Ръководителя по качеството;
- Комуникация с Възложителя
- Комуникация и координация на работата на екипите чрез Ръководителите на отделите екипи;
- Следене на промените;
- Управление на ниво Ръководители на отделните екипи;
- Статус на изпълнението;
- Отчитане и докладване;
- Управление на риска и ескалациите.

- ***Упълномощен представител от страна на Възложителя***

Като представител на Възложителя, ежедневните отговорности и ролята на ръководителя на екипа са свързани с комуникация с Ръководителя на проекта от страна на Изпълнителя и координиране на изпълнение на задачите, свързани със съдействие от страна на Възложителя.

В допълнение на чисто методологичните функции на структурата за управление на проекта, в контекста на изпълнението на поръчката, предложените от дружеството ключови експерти ще имат следните основни отговорности и задачи:

- Ключов експерт №1 Ръководител на екипа:
  - Организира и ръководи изпълнението на проекта/екипа, в съответствие с утвърдените обхват на дейностите и график за изпълнението им, както и изготвя планираните отчети;
  - Ръководи цялостното изпълнение на предмета на поръчката;
  - Подпомага и информира заинтересованите страни в проекта;
  - Организира и контролира поддържането на досие на проекта (в електронен и документален вид);
  - Съвместно с упълномощения представител на Възложителя и експерта по управление на качеството определя критериите за качество на услугите;
  - Съвместно с експерта по управление на качеството организира проучването на причините за несъответствията и предлагане на решения и коригиращи действия за отстраняването им;
  - Осъществява комуникацията с Възложителя;
  - Осъществява управление на риска по проекта в съответствие с плана за управление на риска;

- Ключов експерт № 2 – Поддръжка на сървърни операционни системи:
  - Участва в оперативните срещи в периода на предоставяне на услугите;
  - Координира и контролира процеса на предоставяне на услугите при Възложителя;
  - Участва в наблюдение на предоставяните услуги;
  - Инсталира, администрира и поддържа системния, общия и приложен софтуер
  - Участва в поддръжката и отстраняването на проблеми със сървърните устройства

- Ръководи работата на техническите екипи;
- Познава в дълбочина технологиите предмет на договора;
- Предлага оптимални решения за предоставяне на услугите;
- Докладва на ръководителя на проекта и експерта по управление на качеството за хода на изпълнение на задачите;
- Преглежда техническите документи необходими при изпълнение на услугите;

- Ключов експерт № 3 - Електронна пощенска услуга
  - Участва в оперативните срещи в периода на предоставяне на услугите;
  - Координира и контролира процеса на предоставяне на пощенските услуги при Възложителя;
  - Участва в наблюдение и превантивно обновяване на пощенската услуга;
  - Консултира Хелпдеск специалистите в ежедневната им работа по потребителските настройки на услугата
  - Инсталира, администрира и поддържа системния и приложен софтуер, свързан с пощенската услуга.
  - Участва в поддръжката и отстраняването на проблеми със непрекъсваемостта на услугата

- Ключов експерт № 4 – Мрежова инфраструктура:
  - Участва в оперативните срещи по изпълнението на проекта;
  - Участва в организирането на наблюдение (Monitoring) на мрежовите устройства от вътрешната мрежа и тези, които осигуряват свързаност с интернет;
  - Участва в конфигурирането на мрежови устройства от вътрешната мрежа и тези, които осигуряват свързаност с интернет;
  - Участва в поддръжката и отстраняването на проблеми с мрежовите устройства от вътрешната мрежа и тези, които осигуряват свързаност с интернет;
  - Участва в изготвянето и прилагането на процедури за поддръжка на актуален архив на конфигурацията на мрежовите устройства;

- Ключов експерт № 5 – Мрежова сигурност:
  - Участват в оперативните срещи по изпълнение на проекта;
  - Участва в процеса на изпълнение на услугите;
  - Координира технически работата на екипите и участва в разпределение на задачите;
  - Участва в процеса на изготвяне на методика за оценка на риска за сигурността на информацията;
  - Участват в идентифицирането на заплахите за информационните активи;
  - Участват в идентифицирането на уязвимостите, които могат да бъдат използвани от заплахите;

- Ключов експерт № 6 – Поддръжка на софтуерни телефонни централи
  - Участва в оперативните срещи по изпълнението на проекта;
  - Участва в организирането на наблюдение на работата на софтуерната телефонна централа;
  - Отговаря за отстраняване на проблеми със софтуерната телефонна централа;

- Ключов експерт № 7 Информационна сигурност:
  - Следва и контролира процеса на предоставяне на услугите;
  - Гарантира, че изискванията за сигурност за всички дейности и стандарти са планирани, документирани и изпълнение през целия период на предоставяне на услугите;
  - При необходимост извършва одити и осигурява коригиращо действие както е дефинирано в плана за предоставяне на услугите;

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

- Контролира важните събития и оценки на прегледа на изпълнението;
- Ескалира нерешените проблеми относно сигурността до висшето ръководство;
- Участват в идентифицирането на въздействието, което загубата на поверителност, цялостност и наличност може да окаже върху активите;

Други неключови експерти:

- Хелпдеск специалисти
  - участват в оперативните срещи по изпълнение на проекта;
  - приемат заявки за проблеми в ИТ инфраструктурата на изпълнителя (компютри, периферни устройства, сървъри, мрежа и т.н.);
  - участват в ежедневната поддръжка на персоналните компютри и периферните устройства на служителите;
  - извършват ежедневно наблюдение (Monitoring) на компонентите от ИТ инфраструктурата на изпълнителя;
  - поддържат в актуално състояние всички налични електронни регистри;
  - оказват съдействие при проблем с кабелната инфраструктура;
  - съдействат при първоначална диагностика на проблеми.

- Ръководител по качество:
  - Отговаря за управлението на качеството при изпълнение на услугите.;
  - Контролира прилагането на политиката по качество;
  - Разработва плана по качеството;
  - Разработва плана за тестване и профилактики;
  - Методически ръководи развитието и допълнението на процедурите от СУК за приложимост в проекта.;
  - Организира и ръководи приемането на междинните и крайните резултати по проекта;
  - Познава стандартите за управление на качество ISO 9001:2008, ISO 27001:2013 и ITIL (ISO 20000-1:2011);

- Експерт по оценка на риска:
  - Отговорност за разработването на план за управление на риска като част от Плана за управление на услугите;
  - Разработва и поддържа в актуално състояние на Регистъра на рисковете;
  - Осигурява успех на проекта чрез минимизиране на риска през периода на предоставяне на услугите;
  - Извършва оценка на вредата от въздействието;
  - Извършва оценка на вероятността за пробив в сигурността;
  - Извършва оценка на нивата на рисковете;
  - Извършва идентификация на възможните рискове и избор на подходи за третиране на риска;
  - Идентифицира рисковите фактори на всички стадии (фази) за реализация и предприемат своевременни и ефективни действия за намаляване влиянието им за постигане целите на проекта;
  - Извършва оценка на риска в съответствие с утвърдена методология;
  - Ескалира нерешени рискове и проблеми към висшето ръководство;

- Експерт логистика:
  - Подпомага работата на Ръководителя проект в частта за доставка на резервни части и компоненти;
  - Отговаря за ресурсното осигуряване за изпълнението на услугите;
  - При необходимост организира транспорта на екипа специалисти;

- Администратор на проекта:

- Подпомага работата на Ръководителя проект;
- Изготвя документи, свързани с управлението на проекта;
- Грижи се за ресурсното осигуряване за изпълнение на услугите;

3.2.1. Общи изисквания и ангажимент на Изпълнителя по време на изпълнение на договора

- Изпълнението на поръчката ще се осъществява в съответствие с изискванията на Възложителя, настоящата документация, Плана за управление на услугите и съгласно приложимото действащо законодателство.
- При изпълнение на дейностите служителите на Изпълнителя ще се задължават:
  - да опазват и да не разгласяват пред трети лица съдържанието на документацията, която е станала известна при изпълнението на тази поръчка, без писменото съгласие на Възложителя, с изключение на случаите, когато са задължени по закон за това;
  - да опазват и да не разгласяват пред трети лица съдържанието на данъчна и осигурителна информация, лични данни и друга защитена информация, която е станала известна при изпълнението на тази поръчка;
  - да спазват вътрешните правила за достъп до сградите и режим на работа на обектите на Възложителя.

4. Описание на стандартизирани процедури и документи за управление

4.1. Основни принципи на комуникация

Създаването и развиването на ясна, ефективна комуникация е ключово за успеха на един проект. Важно е да бъдат описани мерките за координация на дейностите от страна на участващите страни, стъпките, които се предприемат при възникване на проблеми, докладване на напредъка на работите и отчетност при изпълнение на проекта.

Създаването на ефективна комуникация, въвежда и поддържа добри работни взаимоотношения, базиращи се на навременна и точна споделена информация. Това помага да се намалят неразбиранията посредством трети страни, служители на Възложителя или други от екипа.

ията включва всички елементи според описанията в техническата спецификация. Осигурява, че комуникация в екипа и обмяна на информация между екипа на Възложителя и екипа на Изпълнителя, позволявайки на двата екипа да наблюдават изпълнението на услугите.

Създадените ключови индикатори за изпълнение, позволят на Възложителя и Изпълнителя да дадат една обективна оценка за изпълнението на услугите

- Комуникацията се извършва писмено и на работни срещи;
- Провеждат се работни срещи за отчитане на изпълнението;
- На оперативно ниво се провеждат срещи за отчитане на статуса на изпълнение на задачите, като тези срещи е възможно да са неприсъствени;
- Оперативният екип по управление на проекта, в това число Ръководителят на екипа, Ръководителите на отделните екипи провеждат кратка оперативна среща с цел дискутиране на предстоящите задачи, възникналите проблеми и необходимостта някои от тях да бъдат докладвани на Комитета за управление на проекта;
- Писмената комуникация се извършва посредством хартиени писма и/или факс. Оперативната комуникация може да се осъществява и посредством електронна поща и по телефон;
- Кореспонденцията се води на български език;
- Кореспонденцията се адресира до всички страни по договора;
- Комитетът за управление на проекта и Ръководителят на екипа на Изпълнителя провеждат периодични срещи. На срещите се дискутират предстоящите задачи, възникналите проблеми и методите и механизмите за отстраняване на проблемите;
- Възложителят определя конкретни ангажименти за всеки член от работната група по повод изпълнението на договора;
- За всяка среща се води протокол от среща;

- При възникването на значим проблем, чието решаване изисква намеса от страна на Възложителя или от трета страна, за проблема и с предложение за мерките по неговото отстраняване Ръководителят на проекта уведомява писмено Комитета за управление на проекта;
- При възникване на специални ситуации Комитетът за управление на проекта се среща задължително и следва схемата за ескалация на проблем;
- С цел осъществяване на добра координация между Изпълнителя и Възложителя, Изпълнителят ще осигури екип за административно и експертно взаимодействие, както и нарочен технически сътрудник на проекта, който се грижи за цялостното документиране на преписките и документите в процеса на комуникация между страните.

4.2. Видове доклади и документи

- ***Месечни доклади***

Съгласно изискванията на Възложителя за отчитане на дейностите при изпълнение на услугата Изпълнителят изготвя и представя ежемесечен отчет за извършените дейности по договора всеки месец до десето число на месеца, следващ отчетния. Отчетът съдържа следните основни точки:

- Анализ на получената информация от извършвания мониторинг на сървърната и комуникационна инфраструктура и мрежовото оборудване;
- Изпълнени дейности и разрешени проблеми;
- Неразрешени инциденти и проблеми;
- Наличност на архивите;
- Планирани дейности за следващия период;
- Препоръки.

- ***Извънредни доклади до Възложителя при възникване на обстоятелства, застрашаващи или възпрепятстващи планираното изпълнение на проекта, и/или договора***

При възникване на обстоятелства, застрашаващи или възпрепятстващи планираното изпълнение на проекта и/или договора Изпълнителят представя на Възложителя Извънреден доклад в срок до 3 (три) дни от датата на възникването му. Докладът съдържа:

- Информация за възникналото събитие;
- Информация за неговото въздействие върху изпълнението на договора;
- Информация за причините за неговото настъпване и за отговорността на отделните участници в него;
- Препоръки към Възложителя за преодоляване на обстоятелствата.

- ***Доклади за контрол и осигуряване на качеството (изготвяне при необходимост)***
  - Общи резултати в управлението на качеството
  - Натрупани до съответния момент отклонения от изискванията за качеството;
  - Коригиращи действия, които трябва да се предприемат за отстраняване на отклоненията;
  - Превантивни действия, които трябва да се предприемат за отстраняване предпоставките за отклонения в качеството;
  - Други въпроси и потенциални проблеми, които Изпълнителят предвижда, че могат да окажат влияние върху напредъка на проекта и/или неговата ефективност.

Изпълнението на проекта се съпровожда с подготовката и предоставянето на Възложителя на следните допълнителни документи:

- ***Протоколи от срещи***

Протоколите от срещи включват информация за присъстващите на работната среща представители на Изпълнителя и Възложителя. Описват обсъжданите по време на работните срещи въпроси, взетите решения, поставените задачи, отговорниците и сроковете за изпълнение.

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

- ***Протоколи за ремонти***

След извършването на сервизни дейности се изготвят протоколи за ремонт, които се подписват от упълномощени от МТСП лица и от съответния сервизен инженер и съдържат: имената на специалистите, извършили ремонта; причината за повреда; вложените резервни части и материали.

- ***План за управление на услугите***

Актуализиран план за управление на услугите се изготвя и представя след подписване на договора.

- ***План за управление на риска***

Актуализиран План за управление на рисковете се представя на Възложителя при започване на изпълнение на договора като част от Плана за управление на услугите. В този план ще бъдат обхванати всички възможни рискове и противодействието на Изпълнителя срещу тях за успешното изпълнение на договора.

- ***Документи за приемане на изпълнението***
  - За изпълнението на услугите, предмет на настоящия договор, Изпълнителят представя Доклади с пълно описание на дейностите.
  - Докладите се разглежда и приема от Възложителя.
  - Приемането на съответния тип услуга, предоставена по договора се осъществява с подписването на Приемателно-предавателен протокол.
  - ване на недостатъци в предоставената услуга, това се отразява в Приемо-предавателния протокол, като се указва и срок, в който Изпълнителят трябва да ги отстрани.
  - След отстраняване на недостатъците, двете страни подписват протокол удостоверяващ това.

4.3. Начин на взаимодействие и механизми на контрол и отчетност

Като част от процеса за управление на проекти, работните срещи се придържат основно към разглеждане на напредъка на проекта и разрешаването на възникнали въпроси.

Оперативни работни срещи - За събиране на информация, преглед на документи, уточняване на въпроси, свързани с работата по проекта. Възможно е да се разглеждат задачите, които трябва да напреднат текущо, съгласно графика за изпълнение на дейностите.

При необходимост: **Ежемесечни координационни срещи** за отчитане на изпълнението.

Изпълнителят предлага адекватен механизъм за управление на комуникацията, който да бъде интегрална част от предлаганата цялостна методология.

Подходът на Изпълнителя за управление на проектната комуникация и за съгласуване на дейностите по проекта с Възложителя и взаимодействие с него, включва:

- Планиране на съгласувателните действия и отразяване в Плана за управление на услугата от Ръководителя на проекта;
- Координирането на съгласувателните действия се извършва от Ръководителя на проекта;
- При необходимост от извършване на съгласувателни действия изпращане на писмо за уведомяване за необходимостта от съгласуване с Възложителя;
- Обикновено за съгласуване на дадена дейност се провежда работна среща с Възложителя, а ако това е невъзможно се изпраща или изисква на съгласувателна документация;
- Ако се проведе съгласувателна среща на нея се води протокол, който завършва с конкретни предложения, решения и срокове, като той се комуникира с всички заинтересовани страни;
- При съгласувателен обмен на техническа документация, инсталационни копия и др. винаги се уведомява Възложителя, като и за него се предвижда и изпраща съгласувателно копие на технически носител;
- При провеждане на съгласувателна процедура от страна на Възложителя се уведомява максимално бързо Изпълнителя при настъпили промени;
- При наличие на затруднения и проблеми при извършването на съгласувателни действия, проблемът се ескалира от Ръководителя на проекта до Ръководителите на дружеството на

Изпълнителя, които от своя страна уведомяват писмено Ръководството на Възложителя и при необходимост свикват заседание на Борда на управителите на проекта.

5. Механизми за управление и контрол на качеството

Качеството е характеристика, която се изразява в способността за задоволяване установени или скрити нужди. Управлението на качеството включва изисквания и процеси, които осигуряват успешното изпълнение на проекта. Всички дейности по управлението на проекта и крайният резултат се включват в мероприятията по осигуряване на качеството. Такива са политиката по качество, обстоятелствата, отговорностите и тяхното прилагане чрез планиране на качеството (quality planning QP), контрол по качеството (quality control QC) и осигуряване на качеството (quality assurance QA).

- **Планиране (Quality Planning)** – определя кои стандарти по качеството са приложими за проекта и как те да бъдат постигнати;
- **Осигуряване на качеството (Quality Assurance)** – цялостна оценка на изпълнението на задачите по проекта, извършвана периодично и даваща сигурност, че са постигнати съответните стандарти за качество;
- **Контрол на качеството (Quality Control)** – наблюдение на специфични резултати в хода на изпълнение на проекта и определяне дали те съответстват на съответните стандарти за качество, както и намиране на пътища за елиминиране на причините за незадоволително изпълнение.

Коригиращи действия ще бъдат прилагани в съответствие със същността и степента на отклоненията от стандартите. Къде те да бъдат насочени и какви мерки ще се предприемат. ще бъде предмет на процедурата по контрол на промените.

По време на изпълнението на проекта, Ръководителят за осигуряване на качеството и Ръководителят на проекта ще провеждат вътрешен контрол по изпълнение на задачите свързани с доставката, монтажа на техническото обезпечение, разработката, тестовете, въвеждането в експлоатация на системата. Ръководителят за осигуряване на качеството ще упражнява вътрешен контрол за определяне ефективността от прилагане на Системата за осигуряване на качеството.

Партньорите в дружеството са е сертифицирани по системата за управление на качеството ISO 9001:2008 и ще прилагат нея при работата по проекта.

Гарантирането на качеството е ключов компонент при изпълнението на всеки проект на екипа на изпълнителя.

Гарантирането на качеството в проекта се управлява чрез План за осигуряване на качество на проекта (ПКП). Този план се добавя към Плана на проекта.

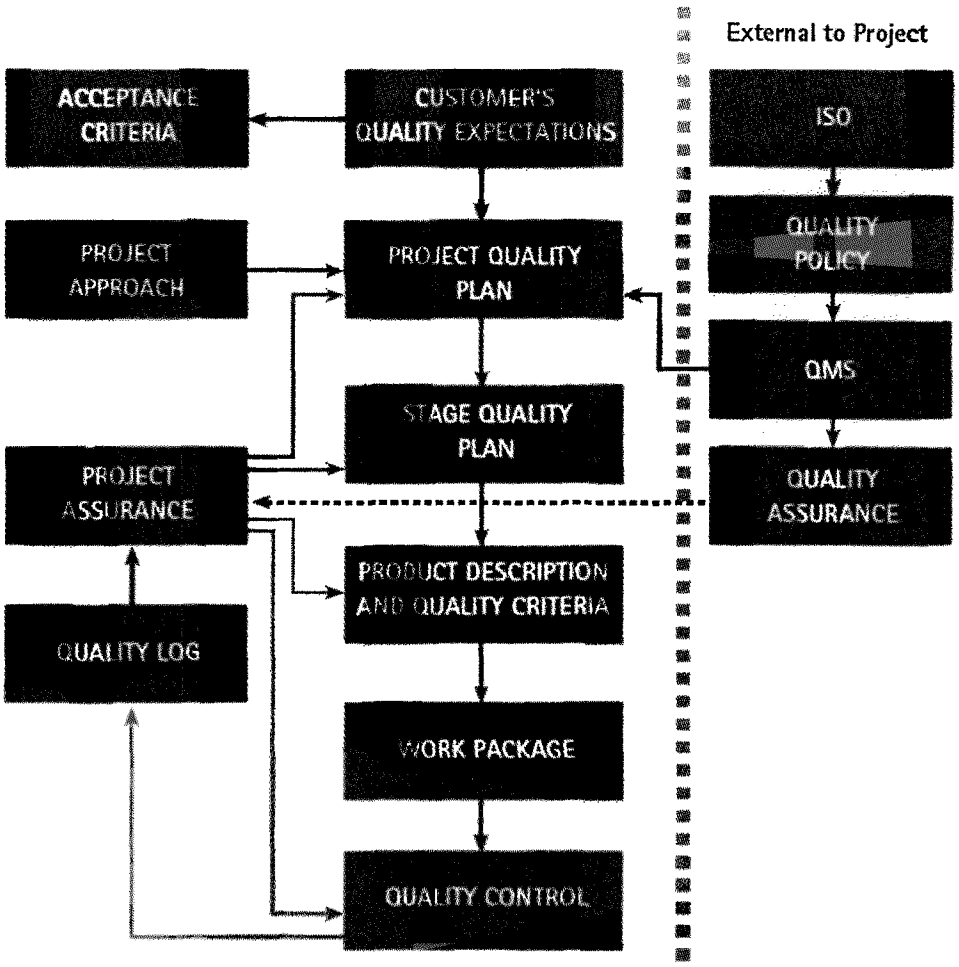
Планът за качеството определя:

- Въведената организация относно качеството, която осигурява вземането под внимание на всички договорени изисквания на проекта и правилното им изпълнение;
- Свързаните отговорности;
- Предприетите дейности за контрол и утвърждаване (прегледи, тестове и т.н.);
- Всеки нов вариант на системата за осигуряване на качество е свързан с обновяване на плана за качество на проекта. Извършването на обновяването е отговорност на отговорника по качеството. Изпълнителят информира относно развитието на плана за качество на проекта;
- Ръководителят за осигуряване на качеството на проекта има отговорността да осигури дефинирането, документирането и изпълнението на специфичните за проекта стандарти за качество. Всеки член на екипа по проекта е отговорен за поддържането на определеното ниво на качество.

През целият жизнен цикъл на проекта са налице строг контрол на качеството, следене, тестване, проверка и представяне на доклади. Ръководителят по качеството на проекта от екипа на изпълнителя осигурява качеството по време на всички етапи чрез налагането на стандарти и процедури за качество, посредством официални прегледи на качеството и списъци за проверки.

Очакванията към качеството могат да бъдат разгледани в много области.

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679



Планирането на процеса по качеството и правилното му разполагане в процеса на управление на проекта са едни от ключовите елементи за изпълнението на проекта в рамките на договорения срок и с максимална полза за Възложителя.

Ръководителят за осигуряване на качеството е отговорен за определянето на екипа на Изпълнителя, поддръжката му и спазването на прилагането на Качеството на проекта.

Ръководителят за осигуряване на качеството помага на Ръководителя на проекта да изгради и реализира частта, свързана с качеството от плана за реализация. Той отговаря за проверката на правилното му прилагане чрез непрекъснато наблюдение.

Реализацията на качеството включва:

- Планиране на качеството;
- Оценка на риска;
- Управление на действията;
- Контрол на проектирането;
- Контрол на доставката;
- Проследимост;
- Проверка и тестване;
- Коригиращи и превантивни действия.

Планирането на качеството се осъществява, в съответствие с проекта и неговото развитие.

Определените дейности по качеството са:

- Прегледите на качеството;

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

- Участието във вътрешни срещи по проекта, ако е необходимо;
- Проследяването на индикатори на качеството;
- Проследяване на потвърждаването на резултати от тестовете;
- Настройването на проекта с оглед на препоръките.

Всяка дейност по качеството включва отчет.

Ръководителят за осигуряване на качеството на проекта взема участие, или определя представител във всички прегледи. Той отговаря за контролирането на:

- Съответствието на организацията на прегледите;
- Контрол на представената документация (наличност, изчерпателност, съответствие);
- Проследяване на качеството.

Предвижда се провеждане на следните вътрешни прегледи:

- Преглед на договора;
- Преглед на стартирането на проекта;
- Преглед на дизайна;
- Преглед на спецификациите;
- Преглед подготовка за монтаж;
- Преглед на процеса на тестове и изпитания;
- Преглед на процеса на поддръжка.

Цел на Плана по качеството е определяне и документиране на дейностите, свързани с качеството, които ще се прилагат в хода на реализацията на проекта, с цел:

- да се осигури съответствие на междинния или крайния продукт с изискванията на проекта;
- да се осигурят ефективни комуникациите между всички участници в процеса за реализация на проекта;
- да се осигури адекватен контрол на всички промени в план-графиците, спецификациите, и др.;
- да се осигури унификация между участниците в проекта по отношение на стандартите, процедурите и методите, които се прилагат за постигане целите на проекта;
- да се приложат процедури за осигуряване доставката на системи, съответстващи на изискванията на договора и отговарящи на стандартите и критериите за качество и сроковете за доставка.

Използване на международно признати стандарти

Важно значение за гарантиране качеството на изпълнението на проекта са внедрените системи за управление на качеството по международно признати стандарти от Изпълнителя, както следва:

- ISO 9001:2008;
- ISO 20000-1:2011;
- ISO 27001:2013;
- ISO 14001:2004;
- OHSAS 18001:2007

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

Дата: 27.09.2019 г.
Гр. София
Място и дата на издаване

Подпис, печат: .....
Манол Илиев
(име, длъжност)

Изготвил:В.Димитрова

Съгласувал: В.Стоев

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679



чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

CERTIFICATE

No. 3591318

Този сертификат е издаден за Системата за управление

на дружеството

ЛИРЕКС БГ ООД

ж.к. Младост 3, бл. 306, вх. 2
1712 гр. София
България

е оценена и установена, че съответства на изискванията на стандарта

ISO 9001:2015

За обхвата на сертификацията

Системна интеграция на ИТ проекти - консултации, системен анализ, проектиране, разработка, внедряване, поддържане и управление на ИТ проекти. Мрежова интеграция - консултации, системен анализ, проектиране, разработка, внедряване, поддържане и управление на мрежови проекти. Проектиране, разработване, внедряване и поддръжка на програмни продукти. Одит на информационни системи. Аутсорсинг на ИТ бизнес процеси. Проектиране, строителство, ремонт и реконструкция на административни, обществени, промишлени обекти и инфраструктурни проекти. Търговия с ИТ и мрежови продукти, офис консумативи и копирна хартия. Технически сервиз на ИТ продукти и мрежови комуникационни системи. Провеждане на обучения. Разпространение, инсталация и поддръжка на програмни продукти. Разработване, внедряване и поддръжка на системи за управление на качеството, ИТ услуги, информационна сигурност.

Този сертификат е валиден до 3591318 и подлежи на
ежегодно надзорно одитиране.

IAF

S 3137

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

Вярно с оригинала

Verification code: B231FF09-792



чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

CERTIFICATE

No. 3590860

LL-C
Certification

Този сертификат се издава да удостовери, че Системата за управление на околната среда на

ЛИРЕКС БГ ООД

ж.к. Младост 3, бл. 306, вх. 2
1712 София
България

Включително филиал:
ж.к. Младост, бл. 54 А, вх. 1, партер, гр. София 1784

е оценена и е установено, че съответства на изискванията на стандарта

ISO 14001:2015

за обхват на сертификация

Системна интеграция на ИТ проекти – консултации, системен анализ, проектиране, разработка, внедряване, поддържане и управление на ИТ проекти. Мрежова интеграция - консултации, системен анализ, проектиране, разработка, внедряване, поддържане и управление на мрежови проекти. Проектиране, разработване, внедряване и поддръжка на приложни програмни продукти. Одит на информационни системи. Аутсорсинг на ИТ бизнес процеси. Проектиране, строителство, ремонт и реконструкция на административни, обществени, промишлени обекти и инфраструктурни проекти. Търговия с ИТ и мрежови продукти. Технически сервиз на ИТ продукти и мрежови комуникационни системи. Провеждане на обучения. Разпространение, инсталация и поддръжка на програмни продукти.

Този сертификат е издаден под номер **3590860** и е валиден от 9. Ноември 2017 до 8. Ноември 2020. Дата на първи сертификат 9. Ноември 2014.

Approved by

Printed by

IAF

S 3137

Validity code: **18F60295-168**

За проверка на сертификата на www.ll-c.info

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

ЛИРЕКС БГ ООД ГР. СОФИЯ

Вярно с оригинала



чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

CERTIFICATE

No. 3590860

LL-C Certification

Този сертификат се издава да удостоверява, че Системата за управление на здравословни и безопасни условия на труд на

ЛИРЕКС БГ ООД

ж.к. Младост 3, бл. 306, вх. 2
1712 София
България

Включително филиал:
ж.к. Младост, бл. 54 А, вх. 1, партер, гр. София 1784

е оценена и е установено, че съответства на изискванията на стандарта

BS OHSAS 18001:2007

за обхват на сертификация

Системна интеграция на ИТ проекти – консултации, системен анализ, проектиране, разработка, внедряване, поддържане и управление на ИТ проекти. Мрежова интеграция - консултации, системен анализ, проектиране, разработка, внедряване, поддържане и управление на мрежови проекти. Проектиране, разработване, внедряване и поддръжка на приложни програмни продукти. Одит на информационни системи. Аутсорсинг на ИТ бизнес процеси. Проектиране, строителство, ремонт и реконструкция на административни, обществени, промишлени обекти и инфраструктурни проекти. Търговия с ИТ и мрежови продукти. Технически сервиз на ИТ продукти и мрежови комуникационни системи. Провеждане на обучения. Разпространение, инсталация и поддръжка на програмни продукти.

Този сертификат е издаден под номер **3590860** и е валиден от 9. Ноември 2017 до 8. Ноември 2020. Дата на първи сертификат 9. Ноември 2014.

Approved by

Issued by

S 3137

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

validity code: **E651A6D2-1A1**
код за валидност на сертификата на www.ll-c.info

Вярно с оригинала

www.ll-c.net

Лирекс БГ ООД
1712 София, ж.к. Младост 3, бл. 306
Телефон: 02/ 9 691 691, Факс: 02/ 9 691 692
www.lirex.bg

ЕИК: 121057952
Банка: Алианц Банк България АД
IBAN: BG46BUIN95611010007719

ЛИРЕКС БГ

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

Приложение № 4
към Техническо предложение

ПРЕДЛОЖЕНИЕ НА ПЛАН ЗА УПРАВЛЕНИЕ НА УСЛУГИТЕ

за участие в открита процедура за възлагане на обществена поръчка с предмет:

„Поддръжка на локалната информационна инфраструктура на МТСП и Единната комуникационна инфраструктура на Министерството на труда и социалната политика и структурните звена“

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

Съдържание

1. Капацитет и ресурси за изпълнение на предоставяните услуги 3
1.1. Човешки ресурси 3
1.2. Хардуер 3
1.3. Софтуер 3
1.4. Документация 4
2. Управление на капацитета на услугата 4
3. Процедури и инструкции за изпълнение на доставяната услуга 4
3.1. Процедури и инструкции: 4
4. Управление на непрекъснатостта и наличността на услугата 4
4.1. План за управление на непрекъснатостта на услуга 4
4.2. План за управление на наличността на услуга 4
5. Управление на промените 4
6. Управление на нивото на обслужване 6
6.1. Схема за ескалация 7
6.2. SLA с поддоставчици. Контролирани показатели: 9
7. Управление на конфигурациите 9
8. Управление на инциденти и проблеми 15
8.1. Управление на инциденти 15
8.2. Система за приоритизация на инцидентите (услуга тип 3) 17
8.3. Управление на проблемите 18
9. Управление на рекламации 21
10. Отчитане и оценяване на ИТ услугите 21

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

1. Капацитет и ресурси за изпълнение на предоставяните услуги

1.1. Човешки ресурси

За успешното изпълнение на поръчката е предвидено използването на следните човешки ресурси:

1.1.1. Ключови експерти

- **Ключов експерт № 1 – Ръководител на екипа (проекта)** – Николина Петрова, с образование, квалификация и опит, съответстващ на изискванията на Възложителя и подробно описани в приложен Списък с експерти.
- **Ключов експерт № 2 – Експерт поддръжка на сървърни операционни системи** – Светослав Манев, с образование, квалификация и опит, съответстващ на изискванията на Възложителя и подробно описани в приложен Списък с експерти.
- **Ключов експерт № 3 – Експерт електронна пощенска услуга** – Христо Христов, с образование, квалификация и опит, съответстващ на изискванията на Възложителя и подробно описани в приложен Списък с експерти.
- **Ключов експерт № 4 – Експерт мрежова инфраструктура** – Данчо Митев, с образование, квалификация и опит, съответстващ на изискванията на Възложителя и подробно описани в приложен Списък с експерти.
- **Ключов експерт № 5 – Експерт мрежова сигурност** – Петър Петров, с образование, квалификация и опит, съответстващ на изискванията на Възложителя и подробно описани в приложен Списък с експерти.
- **Ключов експерт № 6 – Експерт поддръжка на софтуерни телефонни централи** – Здравко Ножаров, с образование, квалификация и опит, съответстващ на изискванията на Възложителя и подробно описани в приложен Списък с експерти.
- **Ключов експерт № 7 – Експерт информационна сигурност** - Боян Янчев, с образование, квалификация и опит, съответстващ на изискванията на Възложителя и подробно описани в приложен Списък с експерти.

1.1.2. Неключови експерти

- Хелпдеск специалисти, **двама души, които ежедневно в рамките на работното време на ВЪЗЛОЖИТЕЛЯ от 09:00 до 17:30 се ангажират на място с поддръжка.**
- Администратор на проекта
- Експерт логистика
- Експерт оценка на риска
- Ръководител по качеството

1.2. Хардуер

От гледна точка на необходимите технически ресурси за изпълнение на поръчката е предвидено използването на транспортни средства, инструменти, консумативи и други. Партньорите в дружеството притежават следното материално-техническо оборудване:

- Check Point Security Appliance T-180 - за извършване на първоначално сканиране на входящия и изходящия интернет трафик;
- диагностична и сервизна апаратура;
- детайлна сервизна документация, предоставена от фирмите-производители;
- средства за мобилна комуникация на сервизните инженери и сервизните коли;
- персонални комплекти с инструменти.

1.3. Софтуер

От гледна точка на необходимите софтуерни ресурси за изпълнение на поръчката е предвидено използването на:

- Internet-базирани системи за документални справки и експертна техническа помощ от фирмите-производители;
- Софтуер за IP телекомуникации;

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

1.4. Документация

Спецификация	Място
Оперативни документи	https://portal.lirex.com

Всички форми за документиране на изпълними дейности, изисквани от процедурите се одобряват от отговорника на услугата и клиента.

Процесът на създаване, премахване и актуализация на документи се извършва в съответствие с изискванията на Възложителя.

При извънредни ситуации, екипът който изпълнява услугата може да пази локални копия на процедурите и плановете, като отговорникът за услугата отговаря за осигуряване на съответствие с техните контролирани еквиваленти.

2. Управление на капацитета на услугата

Управлението на капацитета на услугата се извършва на базата на процедура LSP702 „Управление на капацитета" от СУКИС на ЛИРЕКС.КОМ. Процедурата е приложена към техническото предложение.

За предоставяне на услугата ще бъдат използвани ресурсите отбелязани в точка 1 от настоящия документ.

3. Процедури и инструкции за изпълнение на доставяната услуга

3.1. Процедури и инструкции:

Изпълнението на услугата се извършва в съответствие с:

- LPP009 „Управление на outsourcing процеси";
- LPP013 „Управление на външни ИТ услуги".
- LPP301 „Организация и управление на мрежово сервизно обслужване (Support)"
  Процедурата определя общата схема за организация и управление на процесите за реализация на мрежово сервизно обслужване в Лирекс
- LPI301 „Сервизно поддържане на мрежови решения (Support)"
  Определя реда за поддържане на мрежови решения с приложението на мрежови технологии в съответствие със задълженията на партньорите в дружеството, произтичащи от сервизни договори с партньори и дефинира ескалационния процес при решаване на мрежови проблеми и реда за неговата реализация.

Процедурите и инструкциите са приложени към техническото предложение.

4. Управление на непрекъснатостта и наличността на услугата

4.1. План за управление на непрекъснатостта на услуга

Планът за управление на непрекъснатостта на услугата е съгласно процедура LSP900 от СУКИС на ЛИРЕКС.КОМ, приложена към техническото предложение.

4.2. План за управление на наличността на услуга

Планът за управление на наличността на услугата е съгласно процедура LSP900 от СУКИС на ЛИРЕКС.КОМ, приложена към техническото предложение.

5. Управление на промените

Целта на управлението на промените е да осигури дисциплиниран процес за представяне на промените, които е необходимо да се направят в ИТ средата с минимално прекъсване на текущите дейности.

Процесът на управление на промените има следните цели:

- Да инициира по шаблонен начин промяна чрез подаване на заявка за промяна.

- Да постави приоритет и категория на промяната след оценяване на нейната спешност и влияние върху инфраструктурата. Тази оценка въздейства на скоростта, с която ще се направят промените и начина, по който ще се оторизират.
- Да установи ефикасен процес за преминаване на заявките за промяна към служителя отговорен за управлението им и борда за одобрение или отхвърляне на промяна.
- Да планира развитието на промените, да внедри процес, който може да варира в обхвата и да включва преглед на ключови важни събития.
- След внедряване на промените да ръководи процес, който да проверява дали направените промени са постигнали поставените целите и да определя дали промяната се запазва или не.

Във връзка с контекста на управление на промените, като промяна се дефинира всичко (хардуер, софтуер, компоненти на системата, обслужване, документи или процеси) в ИТ средата, което може да въздейства на съгласуваните нива на ИТ поддръжка или въздейства върху функционирането на средата, или на един от компонентите и. Промените могат да бъдат временни и постоянни. Промените могат напълно да заменят текущата версия на компонентите или с нов компонент, или с променена версия на стария, също така могат да включват инсталация на напълно различни компоненти или премахване на излезлите от употреба.

Управлението на промените може да управлява всички промени в ИТ средата. Това е важно, защото промените могат:

- Да въздействат на много потребители.
- Потенциално да разстроят критични услуги за бизнеса.
- Усложнят хардуера (като сървъри или мрежово оборудване) или софтуерните модификации.
- Да въздействат на данни съхранени в ИТ системите. (Това зависи от вида на данните; например, актуализиране на ценова листа на електронна търговия през Web страница може да се ръководи от процеса на управление на промените, докато актуализирането на информацията в базата данни на компанията на клиента не подлежи на управление).
- Да усложнят работните модификации и процесите, като по този начин въздействат на голям брой потребители.

Промените могат графично да се представят като диаграма на потока на процесите, която представя ключовите задачи, които е необходимо да се изпълнят с цел успешното въвеждане на промяната.

Основните катализатори на промените са:

- Софтуерни промени
  - BIOS
  - Firmware
  - Драйвери
  - Операционни системи или актуализации (patch) на приложенията (при опасност за сигурността или подобрение на продукта)
  - Операционни системи или пакети за обслужване на приложенията (при опасност за сигурността или подобрение на продукта)
  - Софтуер извън поддръжка или край на живота му
  - Нови версии на операционни системи или приложения
  - Нови нужди наложени от пазара или потребителя
- Хардуерни промени
  - Нови модели
  - Интеграция на специфични компоненти като комуникационни устройства
- Проблеми на потребителите като повтарящи се локални инциденти

Формалният катализатор на промяната е заявката за промяна. Тя се подава от оторизиран представител на Възложителя.

Друг катализатор на промяна може да бъде предварителния план на промените FSC (Forward Schedule of Changes). Планът предварително се съгласува с представител на Възложителя. На базата на него предстоящите събития за промяна и обхват им са известни, планът може да се използва за непредвидени (не спешни) промени.

Друга входна информация на процеса е информацията от базата данни за управлението на конфигурацията относно повредени конфигурационни компоненти и връзките, които съществуват между тях. Тази съществена информация допринася за оценката, която процеса на управление на промените трябва да направи за влиянието (потенциално или не) или предложената промяна.

Процесът на промяна се извършва в съответствие с процедура LPP012 „Управление на промените", приложена към техническото предложение.

След съгласуване и приемане от Възложителя (и от доставчика на свързани услуги – ако е необходимо) на промените, по разпореждане на ръководителя на функционалното звено - доставчик на услугата, се изготвя и утвърждава нова редакция на настоящия План за нейното управление и променената ИТ услуга се въвежда в конкретната работна среда. Старата редакция на Плана се съхранява (в електронен вид или на хартия) в съответния архив на ИТ услугата.



6. Управление на нивото на обслужване

Процесът на управление на нивото на обслужване контролира качеството на доставените услуги в съответствие с писмени споразумения с клиента, наречени съгласувани нива на обслужване (SLAs).

Основна цел на управлението на нивата на обслужване е да поддържа и постепенно да подобрява качеството чрез постоянен процес, който включва наблюдение, отчитане и преглеждане на постигнатото и премахване на неприемливите нива на обслужване.

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

Внедряването на процес на управление на нивата на обслужване следва тези стъпки:

- Създаване на каталог на обслужване
- Разработване на съгласувани нива на обслужване
- Наблюдение и отчитане
- Извършване на редовни прегледи на нивото на обслужване

Отговорности:

- Уточнява изискванията и очакванията на клиента относно обслужването.
- Измерване и отчитане на:
  - Нивото на обслужване, което в действителност е постигнато спрямо целта
  - Необходимите ресурси
  - Разходите за обезпечаване на обслужването
- Непрекъснатото подобряване на нивата на обслужване заедно с бизнес процесите и с програмата за подобрение на обслужването.
- Координира другите управления на услугите и функции за поддръжка включително и доставчици от трета страна.
- Преглежда съгласуваните нива на обслужване, за да посрещне променящите се бизнес нужди или разрешаването на важни проблеми
- Изработва, преглежда и поддържа каталог на услугите

Организацията на поддръжката в дружеството и връзките между звената – център за връзка, сервизен център и хардуерни и софтуерни експерти е представена в Приложение№ 1.

Времената на реакция и разрешаване на възникнал проблем са посочени в Приложение №2, т. 3.

6.1. Схема за ескалация

Схемата за ескалация е съгласно приложени към техническото предложение инструкции LPI301 "Сервизно поддържане на мрежови решения (Cisco Support)" и LPI 601 "Сервиз на технически и базови програмни средства" от СУКИС на Лирекс.КОМ.

Схемата за ескалация на проблемите се основава на приоритета на съответния проблем:

- Ескалационен процес за критични инциденти

Контролно време	Уведомявано длъжностно лице	Действия на длъжностните лица	
		Длъжностно лице	Действия
30 минути	Хелпдеск специалист	Хелпдеск специалист	Регистрира case в специализираната система. Докладва на ключовия експерт и изпълнява неговите нареждания. Информира клиента за ситуацията и предприеманите действия.
		Ключов експерт	Анализира проблема и ситуацията. Съвместно с екипа за работа по case, прави анализ и план за действие.
1 час	Ключов експерт	Ключов експерт	Анализира проблема и ситуацията. Взема решение за действие. Докладва на р-л проект и изпълнява неговите нареждания. Съвместно с екипа за работа по case, прави анализ и план за действие. Информира клиента за ситуацията и предприеманите действия.
2 часа	Р-л проект	Р-л проект	Определя ключов експерт за ръководител на екипа / отговорен хелпдеск специалист за работата по case. Информира клиента за ситуацията и предприеманите действия.
		Ключов експерт	Съвместно с екипа за работа по case, прави анализ и план за действие. Актуализира информацията за case в специализираната система.

3 часа	Управител	Управител	Ангажира всички фирмени ресурси за решаване на проблема. Информира клиента за ситуацията и предприеманите действия.
		Р-л проект	Консултира екипа за работа по case.
		Ключов експерт	Установява контакт с представител на партньора. Съвместно с екипа за работа по case, прави анализ и план за действие.

- Ескалационен процес за инциденти застрашаващи работата на сегмент/част от системата

Контролно време	Уведомявано длъжностно лице	Действия на длъжностните лица	
		Длъжностно лице	Действия
2 часа	Хелпдеск специалист	Хелпдеск специалист	Регистрира case в специализираната система. Докладва на ключовия експерт и изпълнява неговите нареждания. Информира клиента за ситуацията и предприеманите действия.
		Ключов експерт	Анализира проблема и ситуацията. Съвместно с екипа за работа по case, прави анализ и план за действие.
4 часа	Ключов експерт	Ключов експерт	Анализира проблема и ситуацията. Взема решение за действие. Докладва на р-л проект и изпълнява неговите нареждания. Съвместно с екипа за работа по case, прави анализ и план за действие. Информира клиента за ситуацията и предприеманите действия.
6 часа	Р-л проект	Р-л проект	Определя ключов експерт за ръководител на екипа / отговорен хелпдеск специалист за работата по case. Информира клиента за ситуацията и предприеманите действия.
		Ключов експерт	Съвместно с екипа за работа по case, прави анализ и план за действие. Актуализира информацията за case в специализираната система.
8 часа	Управител	Управител	Ангажира всички фирмени ресурси за решаване на проблема. Информира клиента за ситуацията и предприеманите действия.
		Р-л проект	Консултира екипа за работа по case.
		Ключов експерт	Установява контакт с представител на партньора. Съвместно с екипа за работа по case, прави анализ и план за действие.

- Ескалационен процес за инциденти, застрашаващи работата на отделни елементи на системата

Контролно време	Уведомявано длъжностно лице	Действия на длъжностните лица	
		Длъжностно лице	Действия
4 часа	Хелпдеск специалист	Хелпдеск специалист	Регистрира case в специализираната система. Докладва на ключовия експерт и изпълнява неговите нареждания. Информира клиента за ситуацията и предприеманите действия.

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

		Ключов експерт	Анализира проблема и ситуацията. Съвместно с екипа за работа по case, прави анализ и план за действие.
6 часа	Ключов експерт	Ключов експерт	Анализира проблема и ситуацията. Взема решение за действие. Докладва на р-л проект и изпълнява неговите нареждания. Съвместно с екипа за работа по case, прави анализ и план за действие. Информира клиента за ситуацията и предприеманите действия.
8 часа	Р-л проект	Р-л проект	Определя ключов експерт за ръководител на екипа / отговорен хелпдеск специалист за работата по case. Информира клиента за ситуацията и предприеманите действия.
		Ключов експерт	Съвместно с екипа за работа по case, прави анализ и план за действие. Актуализира информацията за case в специализираната система.
12 часа	Управител	Управител	Ангажира всички фирмени ресурси за решаване на проблема. Информира клиента за ситуацията и предприеманите действия.
		Р-л проект	Консултира екипа за работа по case.
		Ключов експерт	Установява контакт с представител на партньора. Съвместно с екипа за работа по case, прави анализ и план за действие.

6.2. SLA с поддоставчици. Контролирани показатели:

Не е приложимо.

7. Управление на конфигурациите

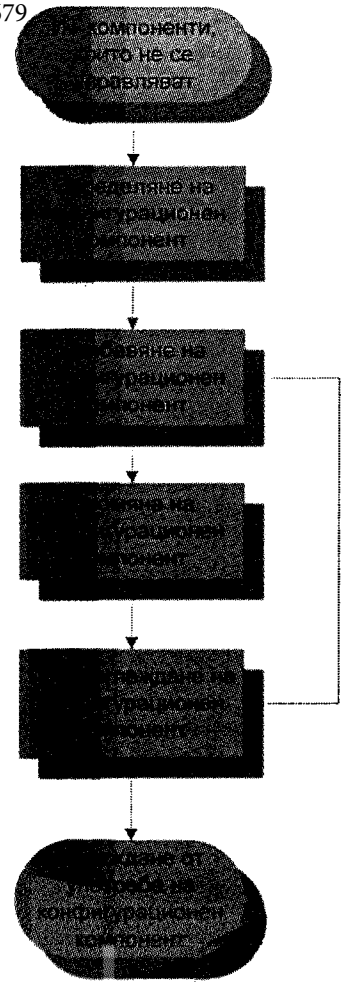
Управлението на конфигурацията е критичен процес отговорен за идентифицирането, контролирането и проследяването на всички версии на хардуера, софтуера, документацията, процесите и всички други компоненти от организацията на информационните технологии.

Процесът на управление на конфигурацията може да се счита като основен за всички други (особено за поддръжка на услугите) процеси. Управлението на конфигурацията се счита за централен и поддържащ останалите.

Цел на управлението на конфигурацията е да гарантира, че само оторизирани компоненти определени като конфигурационни (CIs), се използват в ИТ средата и всички промени на тези компоненти се записват и проследяват през жизнения им цикъл.

Управлението на конфигурацията е графично представено под формата на диаграма на потока на процесите, която идентифицира дейностите необходими за успешното управление и контрол на ключовите компоненти на инфраструктурата.

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679



Основните цели на процеса на управление на конфигурацията:

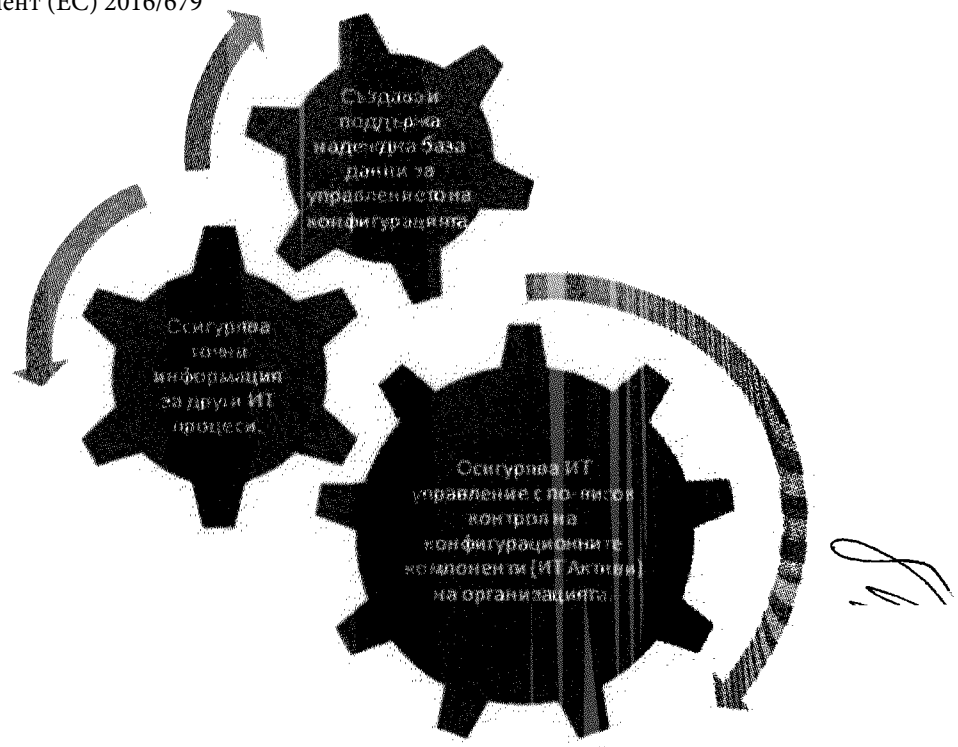
Голяма част от входната информация идва от управлението на промените и изисква информация относно компонентите, които ще въздействат на статуса на променените компоненти.

Процесът стартира с проектиране, попълване и внедряване на база данни за управлението на конфигурацията.

Отговорност на управлението на конфигурацията е да поддържа база данни за управление на конфигурацията.

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679



7.1 Дейности на процеса на управление на конфигурацията са:



- **Планиране**

Това включва определяне граници на проекта като цел, обхват, цели, политики, процедури и очаквано взаимодействие с други процеси.

Задача на управление на конфигурацията е да определи какво може да се постигне, на каква цена – спрямо бизнес изискванията. Тази комбинация влияе на нивото на детайла и колко C.I.'s ще бъдат посочени.

- **Идентификация**

Дейността по идентификацията включва набирането на цялата C.I. информация в рамките на обхвата на проекта. C.I. информацията се събира или ръчно и/или посредством автоматизирани средства. При събиране на данни всеки CI следва да бъде означен за нуждите на справка и контрол.

- **Контрол**

Преди обявяването на БДУК процедури по контрол следва да се създадат. Жизнено важно е промените в БДУК и в CI's да са направени само със съответно разрешение. Трябва да се направят процедури, така че всички промени да са винаги документиране, например с оторизиран RFC's.

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

Можем да започнем да виждаме много силната връзка, която управлението на промените и конфигурацията споделят.

- **Определяне на статуса**

Определянето на статуса е дейност, която записва настоящото и историческото състояние на С.І. така че всяка промяна в С.І. да е проследима. Нивото на статуса може да се определи като част от процеса по планиране (напр. При поръчка, В употреба, В неизправност, В ремонт, Оттеглено).

- **Проверка и одит**

Посредством регулярни одити, организацията може да провери дали всички С.І.'s са записани коректно.

Първият одит следва да бъде направен веднага след въвеждане на БДУК, за да се провери правилното представяне на реалната инфраструктура.

Друго време за одити са след бедствия, основни промени и след предефиниране на графика.

Честотата на одитите ще вземе предвид резултатите от одита и съответните разходи. Частични одити, регулярни одити са всички възможни стратегии, за да се почувства нивото на точност на С.І.

Една от основните ползи, предоставени от управление на конфигурацията в допълнение към управление на активите, е моделирането на взаимоотношенията между елементите. Тези взаимоотношения се нуждаят от определение и изграждане на връзките между конфигурационните части, с оглед моделиране на реална ситуация. Например, работна станция се изгражда от компютър, операционна система и апликации, и работната станция се свързва с и използва мрежата. Правилното разбиране и документирането на връзките между елементите прави възможно детайлното изпълнение на анализ на въздействието по предложената промяна

Установяването на подходяща база за *управлението на конфигурацията* изисква следните принципни процедурни стъпки:

- изготвяне на проект на базова документация на конфигурацията, предложена от Изпълнителя на Възложителя;
- преглед на проекта от Възложителя и Изпълнителя;
- внедряване на необходимите промени, резултат от прегледа;
- одобрение на базовата документация на конфигурацията от страна на Възложителя.

7.2 Основни цели на управлението на конфигурацията

- **идентификация** на конфигурацията на продукта или на негови компоненти (елементи и/или система);
- **контрол** на промените в конфигурациите, с цел поддържане интегрираност на продукта или услугата;
- **проследимост** на конфигурациите за периода на жизнения цикъл на продукта или услугата.

Идентификация на конфигурациите

Конфигурационни елементи

Хардуерът, софтуерът, базите данни, процесите, формите, документацията и/или системите от продукта или услугата трябва да се групират в *конфигурационни елементи* – за краткост наричани в настоящата процедура *конфигурации*. Всяка конфигурация се разглежда като независима единица от системата за УК. Като общо правило, конфигурацията се определя за "делими" части от хардуера, софтуера и/или системите, които могат да бъдат проектирани, тествани и внедрени относително самостоятелно. Приложими са и други критерии за дефиниране на конфигурациите. (Например: за оборудване на функционално работно място, за изпълнение на определена системна функция, по вид оборудване по технически и операционни характеристики.)

Декомпозирането на продукта на конфигурации може да бъде специфицирано в изискванията на клиента, или да бъде извършено в процеса на анализа и дефинирането на изискванията към проекта. Определянето на конфигурациите трябва да завърши преди планиране изпълнението на проекта.

За всеки продукт се определят конфигурациите, които определят основните характеристики на продукта - т.н. базови конфигурации. Те също трябва да бъдат описани в разработената документация за конфигурацията.

Идентифицируемост и проследимост

Всяка конфигурация на продукта трябва да получи уникален и предварително съгласуван идентификатор ID, който се определя както е подходящо. Последният се ползва в административните и техническите документи по управлението и за проследяване и доклад на статуса на конфигурацията.

Идентификаторът ID трябва да отразява:

- самата конфигурация, в контекста на описанието й;
- реализацията (екземпляра) на конфигурацията, ако съществуват повече такива;
- версията на конфигурацията, ако същата е променена.

Структурата на идентификатора ID се определя от директора на проекта/отговорника за услугата в зависимост от естеството на продукта, респ. конфигурацията.

Описание на конфигурация

Описанието на дадена конфигурация се определя от директора на проекта или отговорника за предоставяне на услугата и може да има различна степен на детайлност и форма на представяне. С напредване на процеса за проектиране и разработка на продукта/услугата описанията на конфигурациите стават все по-подробни.

Описанието на конфигурация може да включва:

утвърдена спецификация	какво трябва да представлява продуктът и неговите физически/технически характеристики. Може да бъдат представени като схеми, диаграми и скици на продукта/конфигурацията, да се описват технически и/или функционални характеристики;
техническа спецификация	списък на елементите, които изграждат конфигурацията, с техните количества. Може да включва логическо описание на конфигурацията – логическа схема (описателна или графична) на свързаност на елементите;
параметри и настройки	списък от параметри и настройки (различни от стойностите по подразбиране), използвани при конфигурирането на хардуерните и/или софтуерните елементи на конфигурацията (напр., параметри на хардуерните елементи в системата, директория за инсталиране на ОС, тип/брой на инсталираните лицензи, права и ограничения за достъп, други);
взаимовръзките с други конфигурации	включване в състава на друга конфигурация, влияние при промяна, въздействие върху базови конфигурации, други зависимости;
технологична карта за инсталация	списък от дейности, които изпълнени в описания ред водят еднозначно до описаната конфигурация;
план за действие при аварийни ситуации	списък с предварително идентифицирани потенциални проблеми и начин за тяхното предотвратяване или преодоляване.

Описанията на конфигурацията се документират по подходящ начин, определен от директора на проекта/отговорника за услугата, в досието на проекта/плана за управление на услугата.

Контрол на промените

Инициране на промени

Промяна на конфигурация се налага по различни поводи, някои от които са:

- промяна в спецификациите на проекта/конфигурацията;
- невъзможност да се достави определен елемент от системата;

- доказана невъзможност (по техническа информация или в резултат от опитна постановка) определен елемент от системата да изпълнява функции, които се изискват от утвърдените спецификации;
- промяна в логическата схема на свързаност, която изисква съответна промяна в използваните хардуерни/софтуерни елементи;
- промяна в параметрите и настройките на конфигурацията в резултат на оптимизация на производителността и/или цената;
- промяна в технологичната карта за инсталация на конфигурацията;
- промяна в хардуера и/или софтуера през периода на сервизно поддържане.

Оценка на промените

Всяко предложение за промяна в конфигурациите се анализира за въздействие върху безопасността, надеждността, възможностите за поддържане, функционалностите на системата/продукта, взаимовръзките между компонентите в системата/продукта, цената, графиците за изпълнение, изискванията на клиента/потребителя.

В зависимост от степента на влияние и изискваното ниво за одобряване, промените в хардуера, софтуера и/или системите и тяхната документация се класифицират, както следва:

клас 1 промени, които влияят на системните изисквания, външните интерфейси на системата, общата стойност и/или сроковете за доставка/внедряване. Трябва да се утвърдят от упълномощен представител на Възложителя и Директора на проекта или услугата;

клас 2 промени, които могат доведат до изменения в интерфейсите или във функциите на отделните елементи в рамките на конфигурацията, в цената и/или сроковете за доставка/внедряване в границите на допустимото ниво на компетентност. Одобряват се от директора на проекта или услугата;

клас 3 промени относно вътрешния дизайн и функционалностите на конфигурациите, без да се отразяват на утвърдените изисквания, цената и сроковете за изпълнение. Одобряват се от специалиста (експерта), отговарящ за техническото дефиниране (определяне) на конфигурацията.

Реализация на промените

Внедряването на промяна включва:

- дейности (проектантски, търговски, други) за реализация на промяната;
- актуализация на описанието (и документацията) на конфигурацията и създаването ѝ на нова версия, ако се прилага такъв механизъм. За нова версия се документира (записва): причината за пораждането ѝ; новото описание на промените елементи; реферирането на непроменените елементи към предишна версия;
- преглед на описанията на конфигурациите, които са свързани с променяната, и отразяване на промяната, ако има необходимост;
- уведомяване на всички заинтересовани лица от екипа на проекта за внедрявана промяна;
- изготвяне на план за действие при непредвидени ситуации и възникване на проблеми;
- актуализация на плана на проекта/услугата от директора на проекта/отговорника на услугата, ако се налага.

Координацията на дейностите за внедряване на промените се осъществява от служителя, отговорен за контрола на конфигурациите.

Актуализацията на описанията се извършва от специалистите (експертите), които отговарят за съответната конфигурация, и се контролира от служителя – оторизиран за контрол на конфигурациите.

Верификация на промените

Внедряваните промени в конфигурация се верифицират. Това може да изисква повторно провеждане на тестове, съгласно плана за пускане в действие , или разработката и провеждането на допълнителни тестове. За промени в софтуер, в теста трябва да се включи и регресионно

тестване, за да се гарантира, че не са допуснати грешки от промяна на съществуващи функционалности. Проведените тестове се документират.

Свидетелство за извършени промени в хардуера, софтуера и/или системи, са положителни резултати от проведени тестове за пускане в действие на промените, документирани по надлежен начин.

Контрол за статуса на конфигурации

Контролът на статуса на конфигурацията осигурява проследимост на всички промени в базовите конфигурации, като записите трябва да съдържат необходимата информация за идентификация и управление на произтичащите от промените действия.

Следенето на статуса на конфигурациите започва от първичния им дизайн, продължава през всички стадии на разработката, внедряване и поддръжка, т.е. през целия жизнен цикъл на продукта. Записите за статуса на конфигурациите включват информация за характеристиките на системата, версиите на използваните конфигурации, списък с направените промени, състояние на изпълнение на последните промени, и пр. Степента на тяхната детайлизация зависи от фазата, в която се намира проекта и се определя в плана за УК или в плана на проекта/услугата, където се определя и формата за реализация на записите.

Минималните изисквания за контрола на статуса на конфигурацията трябва да се концентрират върху следенето на заявките за промени, както следва:

- номер, дата, наименование, основание и приоритет;
- идентификация на равнозначните заявки;
- идентификация на елементите на конфигурацията;
- програма за обработката (одобрение, отхвърляне, внедряване на одобрената промяна).

Контролът на статуса на базовите конфигурации включва и периодични прегледи, така както е предвидено в плана на проекта/услугата или в плана за УК, ако е разработен такъв.

Удостоверяване (одит) на конфигурация

Проверката (одитът) на конфигурация може да бъде:

- техническа – проверява се дали конфигурацията включва всички елементи според описанията в техническата спецификация. Осигурява, че промените и всички изисквани елементи (хардуер, софтуер, и/или системи), процедури и експлоатационна документация са включени в доставяната версия на продукта. Обикновено се извършва при инсталация и предаване на продукта.
- функционална – проверява се дали конфигурацията функционира според утвърдените изисквания. Осъществява се при провеждане на функционални тестове за валидация на продукта.

8. Управление на инциденти и проблеми

8.1. Управление на инциденти

Основна цел на управлението на инцидентите е да се възстанови нормалната работа на услугата възможно най-бързо и да се минимизира неблагоприятното влияние върху бизнес процесите, по този начин се гарантира, че най-добрите възможни нива на качество на обслужване са спазени. Нормалната работа на услугата се дефинира като работа на услугата с ограничени съгласувани нива на обслужване SLA (Service Level Agreement).

Процесът на управление на инцидентите гарантира, че инцидентите се откриват и заявленията за обслужване се записват. Записването гарантира, че няма загуба на инциденти или заявления за обслужване, позволява проследяване на записите и осигурява информация в помощ на управлението на проблемите и планиране на дейностите.

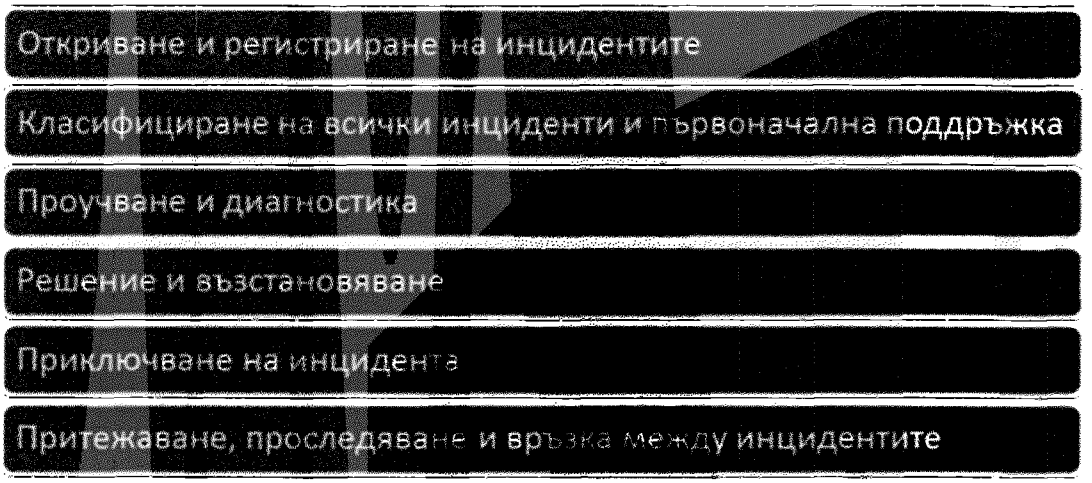
Инцидентът е: Всяко събитие, което не е част от стандартната работа на услугата, което причинява или може да причини прекъсване или намаляване на качеството на услугата.

Инцидентите се класифицират, за да се гарантира, че са с правилен приоритет и подход и да се коригират ресурсите за поддръжка. Управлението на инцидентите включва първоначален процес на поддръжка, който гарантира, че новите инциденти ще бъдат проверени за познати грешки и

проблеми, така че всякакви предишно идентифицирани алтернативни начини за решаването на инцидентите могат да бъдат бързо локализирани.

Управлението на инцидентите осигурява структура, на базата, на която се извърша проучване, диагностика, разрешаване и затваряне на инцидентите. Процесът гарантира, че инцидентите се притежават, проследяват и наблюдават през целият им жизнен цикъл.

Отговорности на управлението на инцидентите:



Процес на управление на инцидентите:

По-важните процеси в рамките на управлението на инцидентите са:

Регистриране, самообслужване, и записване. Този процес се заема с първоначалното регистриране на инцидента. Инцидентите се докладват чрез свързване с центъра за връзка на Изпълнителя, използват се предварително дефинирани комуникационни канали като телефон, факс, e-mail, Trouble Ticket или Lirex CTS (Web базирана проследяваща система).

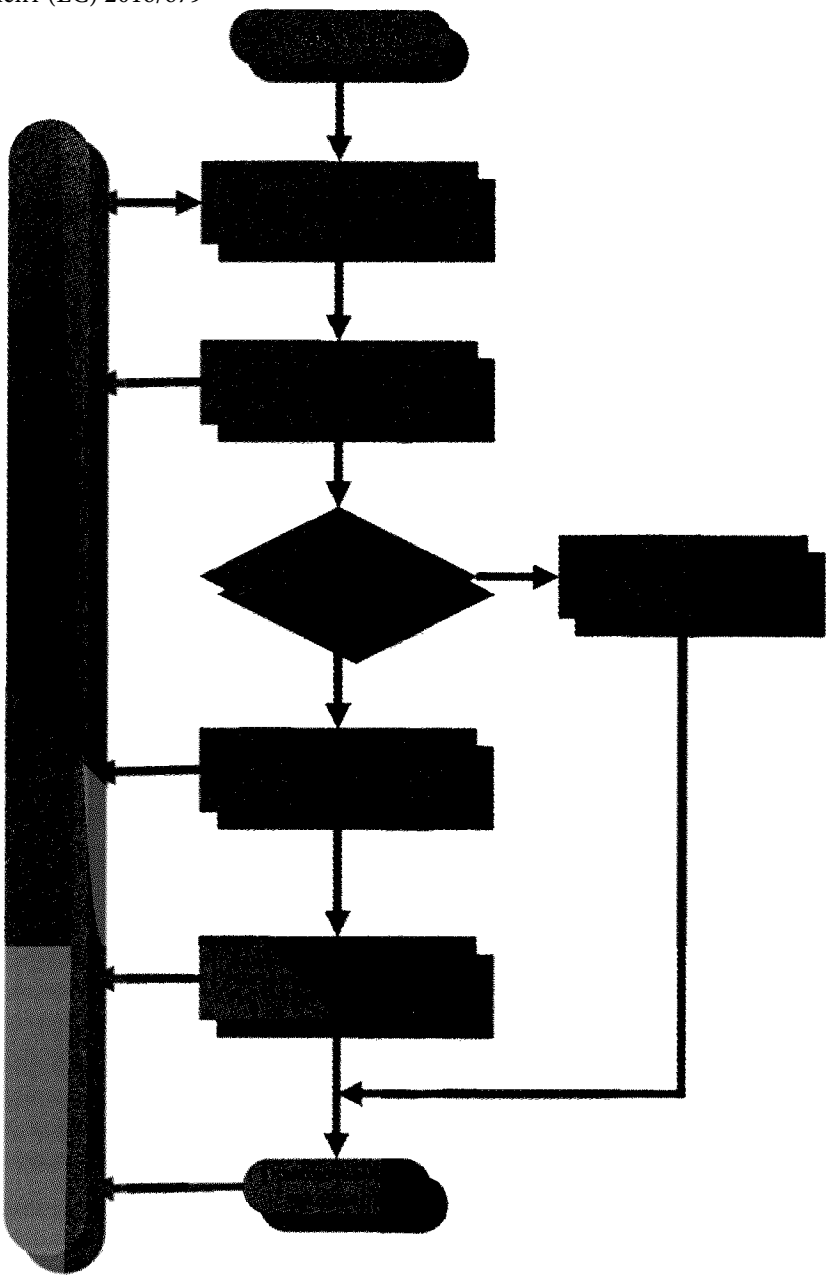
Всеки инцидент се записва, така че е възможно да се проследи, наблюдава и актуализира по време на целия му жизнен цикъл. Информацията след това може да се използва при управление на проблемите, процесът на оптимизация и за цели на планирането.

Управление на заявките за обслужване. Този процес позволява обработването и разпределението на заявките за обслужване. Различните видове заявки изискват управление по различен начин. Центърът за връзка на Изпълнителя може да обработва известен брой заявки, част от заявките е необходимо да се насочват към други процеси, като например управление на промените.

Класифициране и първоначална поддръжка. Процесът на класификация категоризира инцидентите и използва информация за влиянието и неотложността им, за да се определи приоритета на инцидента. Процесът на първоначална поддръжка има за цел да осигури решение на първо ниво. Това може да се постигне чрез проверяване за познати грешки, съществуващи проблеми и предишни инциденти с цел да се идентифицира документиран алтернативен начин за решаването му.

Проучване и диагностика. Този процес се заема с проучването на инцидентите и събиране на данни за диагностика. Центърът за връзка на Изпълнителя използва този процес да идентифицира начините, по които инцидентите могат да се решават възможно най-бързо. Процесът позволява управление на ескалацията или функционална ескалация с цел да се постигнат целите поставени със съгласуваните нива на обслужване SLA.

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679



Важни процедури при инцидентите. Процедурите при възникване на инцидент съществуват, за да управляват онези критични инциденти, които изискват отговор над и извън тези осигурени от процеса на нормалните инциденти. Въпреки, че критичните инциденти следват нормалния цикъл на живот на инцидентите, ускоряването им чрез процедура осигурява по-добра координация, ескалация, комуникация и ресурси, които тези по-високо приоритетни събития изискват.

Разрешаване и възстановяване. Този процес включва стъпките необходими да се разреши инцидент, често взаимовръзка с процеса на управление на промените. След което дейностите се поемат от центъра за връзка, успехът от разрешаване на даден инцидент се проверява.

Затваряне. Този процес гарантира, че инцидентът е разрешен и може да се затвори записа на инцидента.

Процесът също следи дали записа на инцидента е напълно актуализиран и дали е назначена категория на затваряне.

8.2. Система за приоретизация на инцидентите

При подаване на заявката трябва да бъде избран приоритет. Предложените приоритети са описани в следващата таблица:

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

приоритет	*естество на проблема*
Приоритет 1 (П1) **(изключително висок)**	Цялата поддържана мрежа/ система не функционира и това може да повлияе критично на бизнес операциите на клиента, ако проблемът не бъде отстранен. *Дружеството* и клиентът са готови да ангажират денонощно всички свои ресурси до идентифициране на проблема и неговото отстраняване.
Приоритет 2 (П2) **(Висок)**	Проблемът в поддържаната мрежа / система засяга важни аспекти на бизнес операциите на клиента. *Дружеството* и клиентът са готови да ангажират напълно своите ресурси в границите на нормалното работно време за отстраняване на проблема. Работата по сервизна заявка (СЗ) започва в рамките на 2 часа от получаване на съобщението за възникнал проблем.
Приоритет 3 (П3) **(Среден)**	Съществува проблем в поддържаната мрежа / система. Цялостната функционалност е нарушена, но по-голямата част от бизнес операциите на клиента не са възпрепятствани. *Дружеството* и клиентът са готови да ангажират своите ресурси в границите на нормалното работно време за отстраняване на проблема. Работата по СЗ започва в рамките на 12 часа от получаване на съобщението за възникнал проблем.
Приоритет 4 (П4) **(Нисък)**	Клиентът изисква информация или консултация относно възможностите на хардуерни / софтуерни ресурси, конфигурация или инсталация. Времето за реакция (начало на работата по СЗ) е в рамките на 24 часа от получаване на съобщението за възникнал проблем.
Приоритет 5 (П5) **(Информационен)**	Клиентът изисква обща информация или консултация, която не е с особена важност. Времето за реакция е в рамките на 72 часа от получаване на заявката.

Приоритетът на сервизната заявка се определя и променя по следните правила:

• При първоначално съобщение за възникнал проблем, клиентът задава приоритета по негова преценка, след като му бъде разяснено значението на отделните приоритети.

• Реалният приоритет на сервизната заявка се определя от сервизния инженер, изпълняващ сервизната заявка, след анализ на ситуацията при започване на работа по проблема.

• Приоритетът на сервизната заявка може да се промени в процеса на работа при следните условия:

➢ намерено е временно решение, с което е възстановена напълно или частично функционалността на устройство / система. Приоритетът може да се намали, с цел обективно иницииране на ескалационен процес;

➢ клиентът не приема определения като реален от сервизния инженер приоритет. Приоритетът в случая се определя по преценка на Duty manager - сервизен инженер, контролиращ работата на сервизните инженери. или на ръководителя на отдела.

• Всяка промяна на приоритет се съгласува с клиента.

8.3. Управление на проблемите

Целта на управлението на проблемите в да минимизира вредното влияние върху работоспособността на бизнеса, инцидентите и проблемите причинени от грешки в ИТ инфраструктурата и да предотврати повтаряне на инциденти свързани с тези грешки. С цел да се постигне това, управлението на проблемите търси да установи първопричината за инцидентите, след което започва действие за подобряване и коригиране на ситуацията.

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

Проблемът е непозната съществена причина за един или повече инциденти. След като са известни първопричината и временните алтернативни начини за решаването и или е идентифицирана постоянна алтернатива, грешката се определя като позната (Known Error).

Управлението на проблемите има за цел да гарантира, че всички проблеми и познати грешки, които въздействат на ИТ инфраструктурата са идентифицирани и записани. Записаните проблеми и познатите грешки гарантират, че всички проблеми могат да се управляват и проследяват по време на жизнения им цикъл, осигурявайки стойностна информация за други процеси като например управление на инцидентите. Процесът гарантира, че основните идентифицирани проблеми са свързани със съответните възникнали инциденти. Допълнително, процесът открива подходящи алтернативни начини за решаване на инцидентите от центъра за обслужване на Изпълнителя, докато се намери постоянно решение.

Проблемите се класифицират чрез оценка на влиянието им върху бизнеса, анализиране на неотложността им и ресурсите, които се изискват, за временното им или постоянно решаване. Класификацията гарантира, че проблемите са с точни приоритети и са разпределени към подходяща група за анализ.

Отговорности

- Управление на проблемите
- Идентификация и запис на проблемите
- Класифициране на проблемите
- Проучване и диагностика на проблемите
- Управление на грешките
- Идентификация и запис на грешката
- Оценка на грешките
- Записване на решенията на грешката
- Прекратяване на грешката
- Наблюдение на развитието на решенията
- Подпомагане на управлението на важни инциденти
- Подобрения за предотвратяване на проблемите
- Анализ на тенденциите
- Планиране на дейностите по поддръжка
- Осигуряване на информация за организацията
- Получаване на информация за управление на данни при проблем
- Преглед на важни проблеми

Управлението на проблемите се фокусира върху трансформиране на проблемите в познати грешки.

Процесът по управление на проблемите се фокусира върху откриване на слабостите и използване на управлението на промените за премахването им, така че да не се получават бъдещи пробиви.

Процесът фокусира върху откриване на модел (шаблон) между инцидентите, проблемите и познатите грешки. Тези три сфери са ключови, за системното търсене на първопричината. Процесът стартира с много възможности и се стеснява до крайната първопричина.

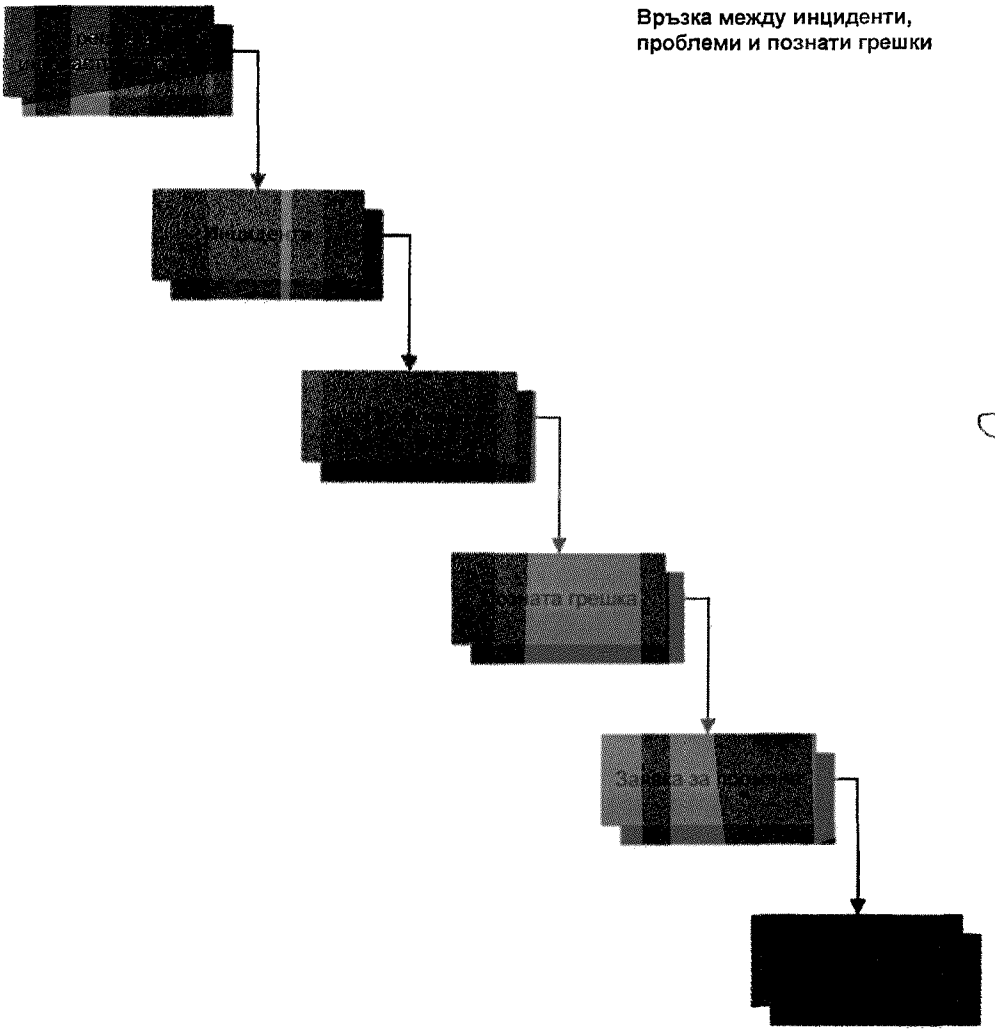
Управлението на проблемите също се занимава с процедурите или практиките, които може да са причина за възникването на проблеми. Управлението на проблемите касае средата на живот и развитие; директно взаимодейства и работи успоредно с процесите за управление на промените.

Процесът на управление на проблемите изисква следната входна информация:

- Записи на инциденти и детайли относно тях
- Познаване на грешките
- Информация относно компонентите на конфигурацията от базата данни за управлението на конфигурацията CMDB (Configuration Management Database)
- Информация от други процеси (Управлението на нивото на обслужване осигурява информация относно изисканите времеви рамки; Управлението на промените осигурява информация за текущите промени, които са част от идентифицирането на познатите грешки).

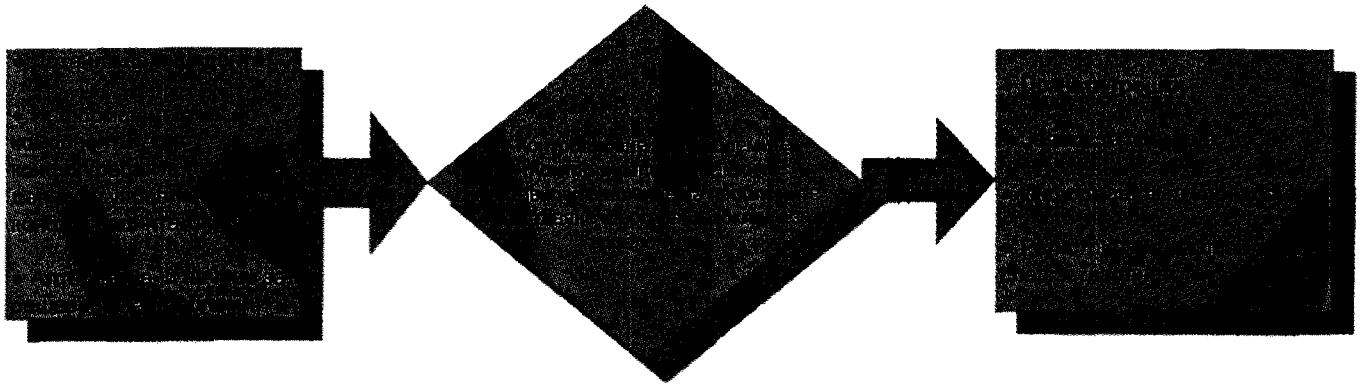
чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

Връзка между инциденти,
проблеми и познати грешки



Изходна информация от процеса са:

- Заявка за промяна RFC's (Request for Change), стартира процес на промяна, за да се решат познати грешки
- Управление на информацията
- Алтернативни начини за решаването на проблеми
- Познати грешки
- Актуализиране на записите с проблеми и записите с решени проблеми, ако познатата грешка вече е решена.



чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

9. Управление на рекламации

Рекламации от клиенти (писмено или устно изразено недоволство от предлаганата услуга) се получава от клиентите по установените канали за комуникация, посочени в договора, приложенията към него или Споразумението за ниво на услугата, както и по начина, посочен в приложената към техническото предложение процедура LAP001 „Измерване степента на удовлетвореност на клиентите".

Приелият рекламацията служител уведомява отговорника на съответното звено с цел вземане на отношение и предприемане на превантивни или коригиращи действия.

За получените рекламации, на първото мениджърско събиране, ръководителите на съответните дейности/процеси докладват за всеки конкретен случай, както и за резултатите от анализа и предприетите мерки по този повод.

Когато клиентът не е доволен от уреждането на неговата рекламация или има спор по изпълнението на договора за доставка на ИТ услугата, както и за всички въпроси, неуредени в този договор, се прилага българското гражданско и търговско право, като страните уреждат отношенията си чрез споразумение. При непостигане на съгласие спорът се отнася за решаване пред компетентния съд.

10. Отчитане и оценяване на ИТ услугите

Отчети за услугата се предоставят месечно под формата на месечен доклад за извършените дейности включващи:

- анализ на получената информация от извършвания мониторинг на сървърната инфраструктура и мрежовото оборудване;
- изпълнени дейности и разрешени проблеми;
- неразрешени инциденти и проблеми;
- наличност на архивите;
- планирани дейности за следващия период;
- препоръки.

Резултатите за предоставяните ИТ услуги от съответните функционални звена се докладват от техните ръководители на Прегледите от ръководството на СУКИС.

Дата: 26.09.2019 г.
Гр. София
Място и дата на издаване

Подпис, печат: .....

Манол Илиев
Име, длъжност

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

Изготвил: В.Димитрова

Съгласувал: Б. Корчев, В.Стоев

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

Лирекс БГ ООД
1712 София, ж.к. Младост 3, бл. 306
Телефон: 02/ 9 691 691, Факс: 02/ 9 691 692
www.lirex.bg

ЕИК: 121057952
Банка: Алианц Банк България АД
IBAN: BG46BUIN95611010007719

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

Приложение№ 5
към Техническо предложение

ПРЕДЛОЖЕНИЕ ЗА УПРАВЛЕНИЕ НА РИСКА

за участие в открита процедура за възлагане на обществена поръчка с предмет:

„Поддръжка на локалната информационна инфраструктура на МТСП и Единната комуникационна инфраструктура на Министерството на труда и социалната политика и структурните звена“

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

Съдържание

1. Управление на риска при изпълнение на поръчката 3
1.1. Методология 3
1.1.1. Идентифициране на рисковете 3
1.1.2. Оценка на рисковете 3
1.1.3. Избор на мерки за предотвратяване и преодоляване на рисковете 6
1.1.4. Непрекъснато проследяване и контрол на рисковете 7
2. Регистър на Рисковете 7

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

1. Управление на риска при изпълнение на поръчката

Реализацията на всеки един проект предполага неизбежно поемане на известно количество риск по пътя на постигане на проектните цели.

С управлението на риска се цели предприемане на конкретни действия така, че излагането на рискови условия да бъде максимално ограничено при запазване на търсената ефективност. Управлението на риска на ниво проект е насочено към поддържане на степента на нежеланите резултати и отклоненията от заданието на поръчката до минималната възможна, без да се нарушава качеството на изпълнението в рамките на обхвата, бюджета и времевия график на поръчката. Това е един систематичен процес на идентифициране, анализиране и предприемане на мерки за въздействие, мерки за недопускане/предотвратяване и съответно преодоляване на последиците при настъпване на рискови събития в проекта.

Всяка поръчка е обект на постоянна промяна по отношение на работната и околна среда. Рисковата обстановка, както и приоритетите на предоставяните дейности по поръчката и съответната значимост на рисковете също се променя. В този смисъл е необходимо да се преразглеждат и преценяват рисковете, свързани с изпълнението на дейностите по поръчката на определен период от време.

1.1. Методология

Цикълът на управление на риска при изпълнението на поръчката включва следните фази:

1.1.1. Идентифициране на рисковете

На тази стъпка се идентифицират потенциалните рискове (или пък възможности), които се появяват при изпълнението на дейностите по поръчката. Съществуват различни категории, които могат да се ползват като изходна точка при идентификацията на рисковете. След като се идентифицират рисковете, те се систематизират в Регистър на Рисковете (Risk Log), който е управленски инструмент на ръководителя на проекта, осигуряващ му възможност за бърз преглед на списъка с основните рискове в проекта, какви действия по управлението им трябва да се предприемат и от кого.

1.1.2. Оценка на рисковете

В оценката на риска се включват тези процеси, системи и активи, при които са възможни последствия като загуба на поверителност, на цялостност и наличност на информацията, както и потенциални щети, пропуснати ползи или неблагоприятно влияние върху дейността на МТСП, в следствие на инцидент, свързан с тях.

Оценката на рисковете се занимава с оценяване на вероятността и влиянието (въздействието) на всеки един риск, като се взема предвид областите на проявлението на всеки риск, както и наличието на взаимозависимости или други външни фактори.

Вероятността представлява оценената възможност за реално случване на конкретно последствие, включително съобразяването на честотата, с която може да възникне конкретния резултат.

Влиянието представлява оценения ефект или резултат при реалното случване на конкретно последствие от риск. Оценка на влиянието се прави от гледна точка на времето, качеството, ползата и ресурсите (хората) в проекта.

Методиката за оценка на рисковете, която ще бъде използвана, ще се базира на отчитане на вероятността от проявата на дадени заплахи и тяхното влияние върху изпълнението на дейностите по поръчката.

За оценка на риска на активите, процесите и системите е избран метод, основан на експертната оценка на всички заплахи и свързаните с тях уязвимости, за всеки един актив, процес и система.

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

Количествените показатели за рисковете ще бъдат измервани по формулата:

Риск = Вероятност Х Влияние

При определяне на вероятността за появата на определена заплаха се взема предвид следното:

- привлекателността на актива, процеса или системата, свързан със съответната заплаха;
- уязвимостта на актива към приложението на съответната заплаха;
- техническите възможности на реализация на заплахата;
- въведените мерки и контроли за защита на съответния актив;
- други

Вероятността ще бъде измервана в степени от 1-5:

Вероятност	Описание (честота на проява на заплахата)	Степен
Незначителна	Изключително малка вероятност да се случи	**1**
Ниска	Слаба вероятност – 1 път в рамките на изпълнение на поръчката	**2**
Средна	Възможна е проява 1-3 пъти в рамките на изпълнение на поръчката	**3**
Висока	Проява 4-5 пъти в рамките на изпълнение на поръчката	**4**
Много висока	Висока проява – над 5 пъти в рамките на изпълнение на поръчката	**5**

Влиянието се определя експертно като ще се използват качествени критерии. При определяне на критериите ще бъдат отчитани критичността и значимостта на съответната система, процес или актив, нуждата от висока наличност както и потенциалните щети или неблагоприятното влияние върху изпълнението на дейностите по поръчката.

Влиянието върху изпълнението на поръчката ще бъде измервано количествено в степени от 1-5:

Влияние	Описание	Степен
Незначително	Не оказва влияние върху изпълнението на дейностите по поръчката	**1**
Минимално	Оказва слабо влияние върху изпълнението на дейностите по поръчката. Не са необходими усилия/средства, за да се възстанови дадена услуга	**2**
Средно	Възможни са забавяния при изпълнението на дейностите по поръчката Наличие на реални щети. Необходими са усилия/средства, за да се възстанови или поправи	**3**
Значително	Затруднения при изпълнението на дейностите по поръчката Продължително отпадане на актив/услуга и/или загуба на свързаност. Значителни разходи на усилие и/или средства, за да се възстанови или поправи	**4**

Изключително	Невъзможност за изпълнение на дейностите по поръчката Отпадане на услуга и невъзможност за възстановяването ѝ	**5**

За оценката на риска е необходимо съответният актив (или група от активи), процеси или системи, да се съпостави с възможната за него заплаха и отговарящата ѝ уязвимост.

Заплахите могат да бъдат:

- форсмажорни събития;
- организационни проблеми;
- човешки грешки;
- технически грешки;
- преднамерени, злоумишлени деяния.
- други

Заплахите могат да бъдат случайни или предумишлени. И случайните и предумишлените източници на заплаха трябва да бъдат отчетени и да бъде оценена вероятността за тяхната поява.

Ако за един актив, процес или система са възможни няколко заплахи или няколко уязвимости, свързани с определена заплаха, то рискът се оценява поотделно за всеки отделен случай.

Наличието на уязвимост само по себе си не причинява вреда. Необходимо е да има налична заплаха, която да използва тази уязвимост. При уязвимост, на която не съответства заплаха, не се изисква прилагането на защита, но тя трябва да бъде разпозната и да се наблюдава за промени. Трябва да се отчете, че неправилно въведените, не функциониращите или неправилно използваните защити могат сами по себе си да бъдат уязвимост.

Нивото (степента на критичност) на риска се изчислява по следната скала:

Риск	Скала
Незначителен	1-3
Нисък	4-7
Среден	8-13
Висок	14-17
Критичен	18-25

На базата на нивото на риска се определят приоритетите за въздействие върху идентифицираните рискове като рисковете с най-висок приоритет се включват за третиране в най-кратки срокове в плана за третиране на рисковете за проекта.

Началната оценка за рисковете се прави от работна група под ръководството на Ръководителя на проекта.

Входящите данни за оценката на риска се получават от отговорниците и потребителите, от специалистите, които планират активите, процесите и системите и ги поддържат. Друг източник на информация за оценка на рисковете, са приложимите за дейността на МТСП законови и други нормативни актове.

За приемливи рискове на активите, процесите или системите (информационни системи или други активи), се приемат тези със стойност до ниско ниво включително. За активите, процесите и системите, с оценка на риска над ниско ниво се въвеждат нови мерки за защита и се прави повторна оценка на риска.

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

Този цикъл се повтаря, докато се получат приемливи стойности на риска. Нова оценка се прави и когато настъпят съществени изменения в структурата на активите, процесите и системите или са въведени нови.

Резултатите от анализа на риска водят до избор и въвеждането на защитни мерки (контроли), които да бъдат използвани за намаляване на оценените рискове до приемливо ниво. Защитните мерки се описват в графата „Действия/Контроли насочени срещу риска" от Регистъра на рисковете.

1.1.3. Избор на мерки за предотвратяване и преодоляване на рисковете

Процесът на ограничаване на последствията от рисковете включва идентифициране и оценяване на набора от възможности за недопускане/предотвратяване на рисковете, както и подготвяне и въвеждане на планове за преодоляване на рисковете.

Възможните действия, които биха могли да се предприемат в отговор на даден риск, се групират в пет основни направления, описани в следната таблица:

Избягване на риска	Прекратяване на риска чрез заобикалянето му, в случаите, в които е възможно нещата да се случат по различен от първоначално предвидения начин. За целта се взимат превантивни мерки, които да спрат заплахата от случване, или да предотвратят въздействието й върху проекта или засегнатите бизнес процеси.
Смекчаване на риска	Третиране на риска чрез предприемане на действия за контролирането му, такива че или да намалят вероятността за появата му или да ограничат въздействието му върху проекта до приемливи нива.
Прехвърляне на риска	Прехвърлянето на риска в специфична форма на редуцирането на риска, при която управлението на риска се пренасочва към трета страна, например чрез застраховане, така че въздействието на риска да не бъде вече заплаха за проекта. Не всички рискове могат да се манипулират по този начин.
Приемане на риска	Толериране (приемане) на риска поради това, че нищо, на приемлива цена, не може да бъде предприето в посока смекчаването му, или просто защото заплахата и въздействието от него са в приемливи граници.
Непредвидимост (рисково планиране)	Такива действия се предприемат с цел борба и за да влязат в сила срещу резултатите от появата на риска в случай, че никое от горните действия не може да се предприеме.

Срещу почти всеки конкретен риск могат да се предприемат действия в един или няколко от горепосочените аспекти.

Защитите, въведени след прегледа на анализа на риска трябва да бъдат допълнение на вече съществуващите, за да се избегне излишното дублиране на защити. Проверява се дали избраните защити са съвместими със съществуващите и планираните защити, т.е. избраните и съществуващите защити трябва да бъдат съвместими, тъй като защитата, която не функционира правилно, е източник на възможна уязвимост.

За изпълнение на защитните мерки се назначава съответен отговорник, изпълнител, както и предварителен срок за изпълнение. Разработва се съответния План за третиране на риска, в който се адресират всички остатъчни рискове над приемливото ниво.

В плана за третиране на риска за всяка мярка (или комплекс от мерки) се прилага оценка на остатъчния риск след прилагането на мярката. Оценката на риска се провежда по методологията, дадена по-горе в настоящата процедура.

1.1.4. Непрекъснато проследяване и контрол на рисковете

Този процес включва извършване на постоянен контрол на идентифицираните рискови дейности, откриване на нововъзникнали такива и контрол на изпълнението на мерките за предотвратяване и преодоляване на рисковете.

2. Регистър на Рисковете

Съществуват рискове, които са идентифицирани предварително преди стартирането на проекта и които могат да произтекат по време на изпълнението на дейностите по поръчката. Необходимо е да бъде ясно определен обхвата и степента на въздействие на тези рискове за да могат да бъдат предприети контролни и коригиращи действия още от началните етапи на проекта с цел недопускане/предотвратяване на риска или избор на мерки за преодоляване на рисковете в случай, че те вече са се проявили.

За да са ефективни прилаганите мерки за предотвратяване на рисковете трябва да е налице постоянен ангажимент от страна на висшите управленски нива по отношение на дейностите свързани с управлението на рисковете в проекта.

С цел управлението на рисковете при изпълнението на дейностите по поръчката е създаден следния Регистър на рисковете, който включва детайлен списък на идентифицираните рискове, техния обхват и степен на въздействие върху изпълнението на обществената поръчка. Описани са мерките за недопускане/предотвратяване на рисковете, както и мерките за преодоляване на рисковете в случай, че те вече са се проявили.

Регистърът на рисковете е динамичен и отворен документ, който ще търпи изменения в хода на изпълнението на дейностите в случай, че са открити нови рискове или са минимизирани съществуващи такива.

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

Риск №	Идентифициран на дата	Категория на Риска	Наименование на Риска	Област на проявление на Риска	Последици от настъпването на риска	Вероятност	Влияние	Ниво	Стратегия за справяне с Риска	Отговорник	Мерки за предотвратяване/ преодоляване на рисковете	Ниво след прилагане на мерките
1	дд.мм.гггг	Организационни	Права за изпълнение на роли в проекта	Съществува риск, че ключовия персонал, ангажиран с проекта, няма необходимите права, за да изпълнява ролята си в проекта	Невъзможност за пълноценно съдействие при изпълнение на дейностите	3	4	12	Смекчаване	Ръководител Екип (проект)	Вземане на управленско решение от страна на Възложителя и при необходимост издаване на вътрешен акт за създаване на необходимата организация и даване на необходимите права за достъп на служителите.	4
2	дд.мм.гггг	Организационни	Достъп до системи и ресурси	Съществува риск от недопускане /неосигуряване на съответните права на достъп на служителите на Изпълнителя до инфраструктурни/системни ресурси на МТСП, които са предмет на обследване, по смисъла на Договора .	Липса на оторизация / достъп до ресурси и системи, които подлежат на обследване би довело до допълнителни разходи и забавяния по проекта.	3	4	12	Смекчаване	Ръководител Екип (проект)	Договорно МТСП трябва да осигури необходимите нива на достъп до системи, инфраструктура и ресурси, преди началото на дейностите по проекта, според одобрения проектен план график.	4
3	дд.мм.гггг	Организационни/ Ресурси	Координация и сътрудничество	Съществува риск от липса или недостатъчна координация и сътрудничество между екипите на Възложителя и Изпълнителя, което би довело до забавяне на изпълнението на дейностите по поръчката.	Забавяне на изпълнението на дейностите по поръчката, отпадане на услуги.	2	3	6	Смекчаване	Ръководител Екип (проект)	Гаранция на управленско ниво от двете страни за сътрудничество и взаимопомощ. Силна проектна координация и комуникация. Създаване на ескалационни процеси в случай на проявление на риска.	3

Риск №	Идентифициран на дата	Категория на Риска	Наименование на Риска	Област на проявление на Риска	Последици от настъпването на риска	Вероятност	Влияние	Ниво	Стратегия за справяне с Риска	Отговорник	Мерки за предотвратяване/ преодоляване на рисковете	Ниво след прилагане на мерките
4	дд.мм.гггг	Договорен/ Обхват	Обем на дейностите	Съществува риск, че поради големият обем на дейностите и интензитета на проекта може да се изостане спрямо графика за изпълнение	Пропуснати срокове за извършване на дейности.	2	3	6	Смекчаване	Ръководител Екип (проект)	Правилно планиране. Междинен контрол на изпълнението на дейностите по график. Организиране на контролни срещи за статуса на изпълнение.	3
5	дд.мм.гггг	Договорен/ Ресурси	Проектен екип	Съществува риск, че поради напускане/невъзможност за изпълнение на задълженията по проекта от ключови експерти от екипа на Изпълнителя, ще бъде забавено изпълнението.	Временна или постоянна невъзможност за член на екипа да осъществява дейности по проекта	1	4	4	Смекчаване	Ръководител Екип (проект)	Осигуряване на гаранция от страна на Изпълнителя за запазване на предложения екип. При необходимост, да се гарантира взаимозаменяемост с експерт отговарящ на същите изисквания.	4
6	дд.мм.гггг	Клиент/ Организация	Съпротива срещу промяната	Съществува риск от създаване на затруднения от звена и отделни служители на Възложителя при внедряването на нови процеси и системи - резултат от дейностите по проекта.	Неизпълнение на дейностите по поръчката. Невъзможност за оптимизиране на процесите.	2	3	6	Смекчаване	Ръководител Екип (проект)	Осигуряване на помощни процедури и компетентна помощ за плавно внедряване на нови процеси.	3
	дд.мм.гггг	Договорен / Приемо-предаване	Промени на критериите за приемо-предаване	Съществува риск, че критериите за приемане на изпълнените дейности от страна на МТСП ще се променят по време изпълнение на поръчката в резултат от промени в политиките и	Това би довело до непредвидими закъснения при приемане на резултатите от изпълнените дейности от страна на	2	3	6	Смекчаване	Ръководител Екип (проект)	Уточняване и подписване на твърди SLA. След подписване на договора двете страни да се съгласят на ясен процес за управление на промяната / искане за промяна с цел да осигури защита от неблагоприятни резултати.	3

Риск №	Идентифициран на дата	Категория на Риска	Наименование на Риска	Област на проявление на Риска	Последици от настъпването на риска	Вероятност	Влияние	Ниво	Стратегия за справяне с Риска	Отговорник	Мерки за предотвратяване/ преодоляване на рисковете	Ниво след прилагане на мерките
				приоритетите на клиента.	клиента							
8	дд.мм.гггг	Договорен / Обхват	Промяна на изискванията	Съществува риск, че изпълнението на дейностите по проекта ще се забавят, поради промени в изискванията, приоритетите и политиките, които са извън контрола на МТСП.	Допълнителни разходи и забавяния по проекта.	2	3	6	Смекчаване/ Прехвърляне	Ръководител Екип (проект)	След подписване на договора двете страни да се съгласят на ясен процес за Управление на промяната. Описаният в документацията документ с окончателният обхват на дейностите да бъде единственият ръководещ по отношение на обхвата.	3
9	дд.мм.гггг	Клиент / Ресурси	Ресурси на МТСП	Съществува риск, че Възложителя няма да разполага с необходимите ресурси, за да приеме договорните резултати според графика за изпълнение. Това би довело до допълнителни разходи и забавяния по проекта.	Пропуснати срокове за приемо-предаване.	2	3	6	Смекчаване/ Прехвърляне	Ръководител Екип (проект)	Двустранно одобрение на окончателния план-график по проекта. Силна проектна координация и комуникация. Пренасочване на налични компетентни ресурси при необходимост	3
10	дд.мм.гггг	Договорен / Приемо-предаване	Промени на обхвата на проекта	Съществува риск, че по време на фазата на изпълнение на Проекта, обхвата на договора ще бъде намерен за непълен, във връзка със "забравени" системи и ресурси при описанието на обхвата.	Допълнителни разходи и забавяния по проекта.	1	4	4	Смекчаване/ Прехвърляне	Ръководител Екип (проект)	МТСП поема пълната отговорност за спецификацията на изискванията, посредством двустранното подписване на окончателен проектен план и спецификация както и твърди SLA. Всички промени ще бъдат предмет на договорената процедура по Управление на	4

Риск №	Идентифициран на дата	Категория на Риска	Наименование на Риска	Област на проявление на Риска	Последици от настъпването на риска	Вероятност	Влияние	Ниво	Стратегия за справяне с Риска	Отговорник	Мерки за предотвратяване/ преодоляване на рисковете	Ниво след прилагане на мерките
											промените.	
11	дд.мм.гггг	Обхват / Методология	Методология за осъществяване на дейностите	Съществува риск, че може да се породят несъгласия между Изпълнителя и МТСП по отношение на най-добрия подход за реализация на дейностите и на мерките и предписанията, защото Възложителя има предварителни концепции за някои решения	Възложителят отказва приемането и подписването на докладите и предписанията, което води до неизпълнение на клаузи по договора	3	3	9	Смекчаване	Ръководител Екип (проект)	Правилно планиране на комуникацията и съгласуването с Възложителя.	3
12	дд.мм.гггг	Клиент / Ресурси	Липса на мотивация	Съществува риск, че при изпълнение на проекта, поради натовареност, ангажираност и/или неразбиране на целите на проекта, отделни служители на Възложителя не осигуряват съдействие, според плана.	Неоказване на съдействие при изпълнение на дейностите водещо до забавяне на изпълнението на дейностите по проекта	3	3	9	Смекчаване	Ръководител Екип (проект)	Вземане на управленско решение от страна на Възложителя и при необходимост издаване на вътрешен акт за създаване на необходимата организация и мотивация на служителите. Създаване и одобрение на ескалационни процеси.	6
13	дд.мм.гггг	Управленски	Управленска некомпетентност	Недостатъчната управленска компетентност води до риск от некоректно възприемане на управленските практики.	Невъзможност за пълноценно съдействие при изпълнение на дейностите	1	3	3	Смекчаване	Ръководител Екип (проект)	Сертифициран ръководител на проекта.	3

Риск №	Идентифициран на дата	Категория на Риска	Наименование на Риска	Област на проявление на Риска	Последици от настъпването на риска	Вероятност	Влияние	Ниво	Стратегия за справяне с Риска	Отговорник	Мерки за предотвратяване/ преодоляване на рисковете	Ниво след прилагане на мерките
14	дд.мм.гггг	Човешки ресурси	Роли и отговорности	При неясно дефинирани роли и отговорности, съществува риск за подаване на неточна или непълна информация.	Невъзможност за пълноценно съдействие при изпълнение на дейностите	1	3	3	Смекчаване	Ръководител Екип (проект)	Правилно дефиниране на ролите и отговорностите по изпълнението на дейностите по поръчката.	3
15	дд.мм.гггг	Човешки ресурси	Здраве и безопасност	Съществува риск от появата на препятствия, свързани със здравословното състояние на служителите.	Закъснение в сроковете	3	3	9	Смекчаване	Ръководител Екип (проект)	Определяне на допълнителни кадри, които биха могли да заместят болните отговорни лица.	6
16	дд.мм.гггг	Организационни	Липса на оперативна подкрепа	Липсата на оперативна подкрепа създава риск от забавяне в сроковете и допускане на грешки в документацията	Пропуснати срокове за приемо-предаване.	2	3	6	Смекчаване	Ръководител Екип (проект)	След подписване на договора двете страни да се съгласят на ясен процес за оказване на съдействие.	3
17	дд.мм.гггг	Управленски	Лошо ръководене	Лошото ръководене на проекта създава риск от закъснение в сроковете, конфликти в екипа	Компрометиране на крайния резултат	2	3	6	Смекчаване	Ръководител Екип (проект)	Ясно разписани правила за управление на проекта, утвърдени от двете страни. Посочени изисквания за квалификацията на ръководител проект в техническото задание	3
18	дд.мм.гггг	Форс-мажорни	Наводнения	Съществува риск от наводняване на сървърни помещения и поражения върху инсталираното оборудване поддържано от Изпълнителя по	Отпадане на системи и услуги, загуба на данни, безвъзвратна повреда на оборудването и необходимост от неговата	1	5	5	Прехвърляне / Избягване	Ръководител Екип (проект)	Застраховане на оборудването и данните. Осигуряване на архиви и съхранението им на място отделно от помещението, в което функционират архивираните системи. Създаване на планове за действие при бедствени	5

Риск №	Иденти-фициран на дата	Категория на Риска	Наиме-нование на Риска	Област на проявление на Риска	Последици от настъпването на риска	Вероятност	Влияние	Ниво	Стратегия за справяне с Риска	Отговор-ник	Мерки за предотвратяване/ преодоляване на рисковете	Ниво след прилагане на мерките
				договорения обхват.	подмяна.						ситуации, както и на процедури за архивиране и възстановяване.	
19	дд.мм.гггг	Форс-мажорни	Пожар	Съществува риск от възникване на пожар в сървърни помещения и поражения върху инсталираното оборудване поддържано от Изпълнителя по договорения обхват.	Отпадане на системи и услуги, загуба на данни, безвъзвратна повреда на оборудването и необходимост от неговата подмяна.	1	5	5	Прехвърляне / Избягване	Ръководи-тел Екип (проект)	Застраховане на оборудването и данните. Осигуряване на архиви и съхранението им на място отделно от помещението, в което функционират архивираните системи. Създаване на планове за действие при бедствени ситуации, както и на процедури за архивиране и възстановяване.	5
20	дд.мм.гггг	Технически/ Сигурност	Вандализ ъм/ Човешка грешка	Съществуват рискове от неоторизирана или неумишлена зловредна намеса в настройки и конфигурации на системи от обхвата на поръчката.	Загуба или кражба на данни, отпадане на системи и услуги.	1	4	4	Смекчаване	Ръководи-тел Екип (проект)	Предоставяне на права за достъп до поддържаните системи само за оторизирани лица. Непрекъснато проследяване и контрол на дейностите по поддръжката извършвани по време на изпълнение на поръчката. Предлагане на контролни мерки за повишаване сигурността и защитата на системите и данните.	4
21	дд.мм.гггг	Технически	Липса на архиви	Съществува риск от неуспешно създаване на архиви на данни и системи в МТСП, включени в обхвата на поръчката.	Невъзможност за възстановяване на данни и системи в случай на необходимост от възстановяване в следствие на	3	4	12	Смекчаване/ Прехвърляне	Ръководи-тел Екип (проект)	Създаване на процеси и документиране на процедури за архивиране и проверка на наличните архиви. Своевременна проверка за успешно създадени архиви след всяко архивиране съгласно	4

Риск №	Идентифициран на дата	Категория на Риска	Наименование на Риска	Област на проявление на Риска	Последици от настъпването на риска	Вероятност	Влияние	Ниво	Стратегия за справяне с Риска	Отговорник	Мерки за предотвратяване/ преодоляване на рисковете	Ниво след прилагане на мерките
					бедствено или друго събитие. Отказ от услуги. Загуба на данни.						графика. Провеждане на тестови възстановявания с цел гарантиране на възможността за възстановяване и проверка на консистентността на архивите.	
22	дд.мм.гггг	Технически	Повреда в поддържаното оборудване	Съществува риск от повреда в поддържаното сървърно и/или комуникационно оборудване, която може да предизвика прекъсване на работата на засегнатото устройство.	Отпадане на услуги, загуба на данни	2	4	8	Смекчаване	Ръководител Екип (проект)	Осигуряване на възможност за временна замяна на повреденото сървърно или комуникационно оборудване. Поддържане на актуални архиви на системите и данните. Създаване на процедури за действие при бедствия и аварии, както и за архивиране и възстановяване на системи и данни.	4
23	дд.мм.гггг	Технически	Повреди в системите за on-line приемане на заявки	Съществува риск от повреда в автоматизираната система за приемане на On-line заявки и невъзможност за регистриране на заявки за възникнали инциденти	Невъзможност за регистриране на инцидент водещ до отказ от услуги.	2	3	6	Смекчаване	Ръководител Екип (проект)	Осигуряване на отказоустойчивост на системата за регистриране на on-line заявки от страна на Изпълнителя и предоставяне на алтернативни канали за регистриран на инциденти в случай на необходимост.	3
24	дд.мм.гггг	Правни/ Регулаторни	Недобро познаване на относимата Норматив	Недоброто познаване на относимата Нормативна уредба може да доведе до несъответствия в изпълнението на услугите спрямо	Несъответствия в изпълнението на дейностите по поръчката спрямо българското	1	3	3	Смекчаване	Ръководител Екип (проект)	Запознаване в детайли със законите и подзаконовите нормативни актове към тях, свързани с изпълняваните дейности по поръчката.	3

Риск №	Идентифициран на дата	Категория на Риска	Наименование на Риска	Област на проявление на Риска	Последици от настъпването на риска	Вероятност	Влияние	Ниво	Стратегия за справяне с Риска	Отговорник	Мерки за предотвратяване/ преодоляване на рисковете	Ниво след прилагане на мерките
			на уредба	законодателството; изпълнение на справки и отчети от съответните поддържани и разработвани системи, които не са в съответствие с действащата нормативна уредба.	законодателство							
25	дд.мм.гггг	Търговски	Неправилно остойностяване на услугите	Съществуват рискове от неправилно остойностяване на услугите при създаване на техническото предложение от страна на Изпълнителя, което може да доведе до некачествено или непълно изпълнение на съответната услуга поради необходимост от допълнителни неостойностени разходи.	Некачествено или непълно изпълнение на дадена услуга	1	4	4	Смекчаване	Ръководител Екип (проект)	Правилно разбиране на изискванията по заданието за изпълнение на услугите по поръчката. Задаване на конкретни въпроси за уточняване. Коректно планиране и остойностяване на предоставяните услуги чрез проверка за актуалност на ценови листи, правилно оразмеряване на необходимите ресурси, проверка за пълнота на предвидените дейности по услугите. Изпълнение на правилата за оптимално използване на ресурсите.	4

Дата: 27.09.2019 г.
Гр. София
Място и дата на издаване

Подпис, печат:

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

Манол Илиев
(име, длъжност)

Изготвил: В.Димитрова
Съгласувал: В.Сидев

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

Лирекс БГ ООД
1712 София, ж.к. Младост 3, бл. 306
Телефон: 02/ 9 691 691, Факс: 02/ 9 691 692
www.lirex.bg

ЕИК: 121057952
Банка: Алианц Банк България АД
IBAN: BG46BUIN95611010007719

ЛИРЕКС БГ

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

Процедури и инструкции - част от Системата за Управление на Качеството и Информационната Сигурност (СУКИС) на „Лирекс БГ“ ООД

гр. София
2019 г.

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

ЛИРЕКС.КОМ	Процедура: Идентификация и проследимост на продукти и услуги	Версия 3
	LPP002	1 от 5

1. История на редакциите

версия	описание на промяната	автор	проверил	утвърдил	дата на въвеждане
1	Редакция след документален одит на СУК	Д. Кънчев	Т.Петров	Д.Илиева	19.02.2001
2	Въвеждане на изискванията на ISO/IEC 27001:2005	В.Иванов	Б.Йорданов	Д.Илиева	04.02.2009
3	Актуализиране на документите от СУКИС	М.Йончева	В.Иванов	Д.Илиева	01.08.2019

2. Предназначение

Целта на процедурата е да определи политиката за идентифициране и проследимост на материални продукти (стоки) и на услугите, обект на търговската дейност на дружествата Лирекс.ком.

3. Приложимост

Изискванията на процедурата се прилагат по отношение на продуктите (стоките) и услугите, които са предмет на търговската дейност на дружествата.

Идентификацията и проследимостта на регистрираните случаи в Call центъра за Интернет услуги, на заявките за сервизно обслужване от сервизните центрове и регистрираните случаи за мрежово поддържане се осъществява в съответствие с реда за управление на съответните процеси / дейности.

Проследимостта на продукти на клиент / партньор, предоставени във връзка с изпълнението на договорни отношения, се осъществява в съответствие с реда, определен в процедура *LPP003*.

В случаите когато се налагат специални изисквания за идентификация и проследимост на продуктите, се предвиждат средства за уникална идентификация, като същата се реализира като запис по качеството, съгласно процедура *LMP002*.

4. Отговорности

Процедурата се изпълнява от всички длъжностни лица, чиято дейност е пряко свързана с продуктите и услугите, които са предмет на търговската дейност на дружествата.

4.1. Служителите от отдел *Логистика*

- Осигуряват проследимост на продуктите при:
  - доставката на стоките и материалите от доставчиците;
  - съхранението на стоките в складовете на дружествата;
  - прехвърлянето на стоките от едно място (склад) в друго;
  - опаковането и експедирането на продуктите към клиента;
  - смяна състоянието на продуктите.

4.2. Служителите от функционалните звена

- Осигуряват вярна идентификация на продуктите при изготвянето на документи и записи по качеството.

- Осъществяват регламентираните операции за осигуряване проследимостта на продуктите.

5. Процедура

5.1. Идентификация

5.1.1. Идентификация по вида на продукта / услугата

Идентификацията е предназначена да отличи един вид продукт от друг - например, да се отличи стоката *монитор* от стоката *модем*, услугата: *електронна поща* от услугата *сервизно обслужване* и т.н. Осъществява се посредством продуктовите и/или серийните номера на производителя или доставчика.

Идентификацията по вида на продукта/ услугата се прилага при документиране предаването (предоставянето) на продукта / услугата на клиент.

Продуктовите и/или серийните номера на производителя или доставчика се въвеждат в използваните ЕРП системи (*MS Dynamics NAV*).

Всички служители, които имат пряко отношение към документиране предаването/ предоставянето на продуктите / услугите на клиенти, трябва да назначават (избират) еднозначно продуктови и/или серийни номера от въведените такива.

5.1.2. Идентификация по отношение индивидуалността

Идентификацията по отношение индивидуалността на продукта / услугата е предназначена да отличи един екземпляр на продукта / услугата от друг. Осъществява се посредством:

- ***серийни номера*** - този начин за идентифициране е приложим за продукти, които са индивидуално отличими един от друг. Например: *монитор, модем, клавиатура*;
- ***партидни номера*** - този начин за идентифициране е приложим за продукти, които са отличими един от друг по партиди на доставка. Например, *мастила за принтер;*
- ***идентификатори ID*** – този начин за идентифициране е приложим за услуги и нематериални продукти (например: *проекти*, *сделка*).

Серийните и партидните номера на стоките се задават от производителя. Задължение на служителите, боравещи пряко със стоките, е да работят вярно с тези номера - стоките да се въвеждат и изписват в/от склада с верните серийни или партидни номера.

Продуктите, които не могат да бъдат отличени един от друг (интерфейсни кабели, крепежни елементи, кабелни канали, и др.) се идентифицират само с продуктовите си номера.

Услугите и други нематериални продукти, обект на фирмените дейности, се идентифицират с подходящи уникални идентификатори ID. (Например: номер на заявка за сервизно обслужване, наименование на тръжен проект, заявка за доставка, дата и регистрационен номер на оферта, други). Последните се формират по правила, определени в регламентирания ред за съответните фирмени дейности (процеси) .

5.2. Проследимост

Целта на проследимостта е да се осигури във всеки един момент информация за местоположението на продуктите (стоките) и/или статуса на продуктите / услугите.

5.2.1. За стоките проследимостта се отчита по отношение на:

Местоположението, което може да бъде: в склада на дружествата, в офис на дружествата, дадена за временно ползуване на друга организация като оборотна стока или за проби и изпитания.

Местоположението на стоките се установява, както следва:

- със средствата на MS Dynamics NAV;
- от информационните фондове на звената за сервизно обслужване (сервизни центрове, Cisco Support);
- от информационните фондове на отдел Логистика;
- от досиетата на проекти и сделки – при работа с продукти на клиенти, съгласно изискванията на процедура LPP003.

Състоянието на съответната стока: изправна, разкомплектована, дефектна, несъответстваща на изисквания, с изтекъл срок на годност.

Контролира се за стоки – предмет на търговската дейност на дружеството.

Всяка разкомплектована / дефектна / с изтекъл срок на годност стока се маркира с подходящ по цвят етикет и надпис върху етикета, при необходимост.

Състоянието на приети за сервизно обслужване продукти се отразява в записи по качеството (дневници и регистри, заявки, протоколи), съгласно установения ред за изпълнение на съответната дейност / процес.

Състоянието на продукти на клиент / партньор, приети по условията на процедура *LPP003*, се контролира съгласно изискванията на същата процедура.

Собствеността на стоката: на *Лирекс БГ*, чужда собственост, на отговорно съхранение от дружеството.

Предоставените на отговорно съхранение стоки се съхраняват в складовите помещения на дружествата на специално определени за целта места, съгласно изискванията за съхранение от процедура *LPP004*.

Проследимостта на услуги и нематериални продукти (проекти, сделки, други) се отчита по отношение степента на изпълнимост (статуса).

Състоянието на изпълнимост се отразява в дневници, регистри и досиета, съгласно регламентирания ред за изпълнението на съответните дейности / процеси.

6. Блок схеми

Не се прилагат блок – схеми.

7. Термини и съкращения

Идентификация на продукт	Метод, позволяващ да се отличи един продукт от друг. Отличаването може да бъде по продуктов номер, по сериен номер, по идентификатор и др.
Проследимост на продукт	Механизъм, даващ възможност да се проследи местоположението и/или състоянието (статуса) на индивидуален продукт (стока) / услуга / нематериален продукт.

Запис (по качеството)	Електронен или хартиен документ, представляващ обективно доказателство за степента/ постигнати резултати при изпълнение на определена дейност/ процес/ операция. Документирано (в електронен вид или на хартиен носител) обективно доказателство за степента/ постигнати резултати от изпълнение на определена дейност/ процес/ операция. Характеризира се със съдържание, контекст и структура, и е обект на управление. Може да бъде изпълнен като : ♦ самостоятелен документ, ♦ запис(и) от БД, ♦ елемент (определена част) от документ, която отговаря на изискванията от процедура *LMP002*.
СУКИС	Система за Управление на Качеството и Информационната Сигурност в дружествата *Лирекс.ком*.
Лирекс.ком	Дружествата Лирекс БГ, Лирекс БС, **Лирекс Хай Тех, Беолик, Лирекс Скопие, Теза**

8. Препратки към документи

ID на документа	*наименование на документа*
LMP002	Процедура: Управление на документи и записи за реализация на фирмените дейности
LPP003	Процедура: Работа с продукти на клиент
LPP004	Процедура: Манипулиране, съхранение, опаковане и доставка на продукти
	Ръководство за работа с MS Dynamics NAV

9. Оценки

Оценките, свързани с изпълнението на дейностите по настоящия документ, се представят на Годишния преглед от ръководството.

10. Документирана информация

Сигурността на информацията, свързана с идентификацията и проследимостта на продуктите и услугите, предоставяни на клиентите, се осигурява от процедурите и инструкциите на въведената Система за управление на качеството и информационната сигурност.

Информацията, свързана с личните данни и търговската дейност на доставчиците се събира и използва само във връзка с точното и навременно изпълнение на договорите за доставка и осигуряване на необходимото им качество.

Не се изисква прилагането на унифицирани бланки и форми.

За актуалната редакция и съдържание на процедурата проверете в *LODIS*.

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

Приложение 1

ПРАВИЛА
за маркировки и съхранение на стоки
в складови помещения

категория стоки	*съхранение съгласно изискванията на процедура LPP004*	*маркировки*
за търговска дейност (отговаря на изискванията)	отделно по видове продукти	без специална маркировка
чужда собственост на отговорно съхранение	отделно по собственик и вид на продукта	зелен етикет, при необходимост с надпис за собственика
с изтекъл срок за годност	отделяне и обозначаване	оранжев / жълт етикет
с несъответствие на определени изисквания (разкомплектовани, неизправни, други)	отделно	бял етикет с подробно описание за причината, свързани документи и евентуални указания за последващи операции
изписани за офис ползване, съхранявани в склада	отделно по вид на продукта	червен етикет

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

ЛИРЕКС.КОМ	Процедура: Работа с продукти на клиент	Версия 4
	LPP003	1 от 6

1. История на редакциите

версия	описание на промяната	автор	проверил	утвърдил	дата въвеждане
2	Отразяване на промени във връзка с направени забележки и препоръки от одит на адекватност на документите от СУК за сертификация по AQAP 2110	М.Цолов	Д.Кънчев	Д.Илиева	14.03.2005
3	Въвеждане на изискванията на ISO 9001:2008 и ISO/IEC 27001:2005	Б.Йорданов	Вл.Иванов	Д.Илиева	08.02.2009
4	Актуализиране на документите от СУКИС	М.Йончева	Вл.Иванов	Д.Илиева	01.08.2019

2. Предназначение

Процедурата определя реда за управление на продукти (материали, технически устройства, софтуер, компоненти, писмени материали, чертежи, скици, други), собственост на клиент и предоставяни за изпълнението на проекти, разработки и сервизни дейности – обект на договорни отношения между страните. Управлението включва входен контрол, съхранение и поддържане на предоставената собственост на клиента до момента на използването или обратното й предаване на собственика.

3. Приложимост

Процедурата е приложима от всички организационни звена, които в изпълнение на своите функции работят с продукти на клиент. Изискванията на процедурата се съблюдават до приключване на операциите с предоставената чужда собственост, независимо от нейната приложимост и обработка.

Изискванията на процедурата са приложими и относно продукти, предоставени на дружеството от партньори за провеждане на експерименти, съвместни разработки и други аналогични дейности.

Процедурата определя общите правила за работа с продукти на клиент/партньор за периода от приемането до предаването им на собственика им.

Спецификата за приложението на общите правила от настоящата процедура в сервизната дейност се определя в съответните процедури и работни инструкции - процедура *LPP302*, процедура *LPP601*.

В случай на изключения от общите правила и регламентирания ред, правилата се определят в писмено споразумение със собственика (клиент, партньор) на предоставените продукти.

4. Отговорности

4.1. Висше ръководство

- утвърждава протоколи за повреди, загуби и установени нефункционалности на чужда собственост и определя последващите действия.

4.2. Отговорният ръководител

(ръководители на сервизни центрове/звена, ръководител отдел *Логистика*, ръководители на проекти)

- осигурява изпълнението на договорените изисквания относно предоставена от клиент/партньор чужда собственост;
- организира дейностите с чужда собственост, съгласно изискванията на настоящата процедура, другите документи на СУКИС и установения ред;
- контролира подчинените си служители за съблюдаване на реда за работа с чужда собственост;
- организира и контролира документирането на работата с чужда собственост и съхранението на изготвените документи (записи по качеството).

4.3. Отговорният(те) за съхранението служител(и)

- идентифицира получената чужда собственост, документира приемането ѝ, и осигурява проследимостта ѝ, съгласно установения ред;
- осъществява входящ контрол за получените продукти;
- документира установени несъответствия при входящия контрол, загуби и повреди, крайното състояние преди предаване;
- документира по установения ред предаването на чуждата собственост.

5. Процедура

5.1. Приемане и контрол

Всяка чужда собственост се приема от оторизираните служители с документиран запис (приемо-предавателен протокол, заявка за сервизно обслужване, друга подходяща форма), в който се описва:

- получаваната чужда собственост и нейната идентифицируемост, съгласно изискванията на процедура *LPP002*;
- поводът за получаване;
- проведеният входящ контрол за състоянието и приложимостта, и резултатите от него.

Приемането на чужда собственост за сервизно обслужване се документира по реда определен в съответните процедури (*LPP302*, *LPP601*). В останалите случаи, за приемането се съставя протокол по образец (форма *L-ADM-012-RPR*) или по форма, съгласувана с клиента.

Оригиналите на приемателните протоколи се съхраняват, както следва:

- за приети продукти за сервизно обслужване – в определените фондове на звената, осъществяващи сервизната дейност;
- протоколите по форма *L-ADM-012-RPR* - в дело "*Приемателни протоколи – чужда собственост*" в отдел *Логистика*. При необходимост за оперативната практика, от оригиналите се правят копия;
- други форми, съгласувани с клиентите – в досиета на проекти/клиенти.

При изпълним контрол за функционалност в процеса на работа с чужда собственост и установени несъответствия се съставя протокол (форма *L-ADM-003-LDP*), и се уведомява собственика на стоката/продукта.

Работата с продукти и материали, несъответстващи на определените изисквания, се осъществява в съответствие с изискванията на процедура *LAP004*.

5.2. Съхранение на чужда собственост

Осъществява се в съответствие с установения ред за изпълнение на функционалните дейности/процеси, или ако не е регламентиран такъв – съгласно устните разпореждания на съответния отговорен ръководител. Чужда собственост със степен на поверителност се съхранява само от ръководни служители (управител, директор, управляващ дейност/процес). Същите определят и правилата за работа с нея, като ограничават достъпа на изпълнителите.

Работа с чужда собственост се изпълнява само от служители по силата на техните служебни задължения.

5.3. Ремонт и преработка на чужда собственост

Реализира се само по отношение на предадени за сервизно обслужване продукти и само с потвърдено от собственика съгласие.

Включване на собственост на клиента в друг продукт се осъществява само в съответствие с изискванията за разработката При необходимост от приложението на собствеността на клиента за други цели, се иска неговото изрично (писмено/устно) съгласие.

5.4. Повреди, загуби и нефункционалност

За повредена, загубена или доведена до състояние на функционална неприложимост чужда собственост в процеса на работа с нея отговорният ръководител определя комисия, която съставя писмен протокол (форма *L-ADM-003-LDP*). Протоколът се утвърждава от управител, който определя и последващите действия. За случая отговорният ръководител уведомява собственика.

При договори с държавна гаранция на качеството, ПДГК трябва да бъде информиран незабавно в случай, че с продукта, осигурен от Възложителя, е налице събитие, водещо до загуба, повреда или друго, което го прави неподходящ за употреба във връзка с договора.

5.5. Предаване на чуждата собственост

Предава се на нейния собственик, независимо от получения резултат при работа с нея, с надлежно оформен писмен документ. Формата и съдържанието на документа се определят в зависимост от изпълнените операции и приложимостта на стоката/продукта.

6. Блок схеми

За процедурата не се прилага блок-схема.

7. Термини и съкращения

Клиент	Юридическо или физическо лице, с което се сключва споразумение/договор за доставка на продукт или услуга.
Чужда собственост (ЧС)	Материал, компоненти, продукти (технически устройства, програмни средства), чертежи, строителни и монтажни проекти, интелектуална собственост (включително и конфиденциална информация), и др., които се доставят от клиент/партньор с цел: сервизно поддържане, приложимост в разработки и проекти, проверка за функционалност, и пр.

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

Отговорен за съхранението (на чужда собственост)	Служител на дружеството, на когото е възложено приемането, входящия контрол, съхранението, контрола за изправността при приложението на чуждата собственост. (Диспечер или оперативен дежурен в сервизен център/звено, служител от Търговската приемна, служител в отдел Логистика, специалист от проектен екип.)
Отговорен ръководител (мениджър)	Ръководен служител, в чиито задължения е контрол за приемането, съхранението и приложимостта на чужда собственост.
Лирекс.ком	Дружествата Лирекс БГ, Лирекс БС, Лирекс Хай Тех, Лирекс Скопие, Беолик, Теза
Система за управление на качеството и информационната сигурност (СУКИС)	Организационната структура на *Лирекс.ком* в комплекс с регламентирания ред, процесите и ресурсите, необходими за управление качеството и информационната сигурност на предлагани продукти и услуги.
LOMIS	Он-лайн управленска информационна система на *Лирекс.ком*.
ДГК	Държавната гаранция за качеството представлява процес, с помощта на който съответните национални органи вдъхват увереност в това, че договорните изисквания по отношение на качеството са изпълнени.

8. Препратки към документи

ID на документа	*наименование на документа*
LMP002	Процедура: Управление на документи и записи за реализация на фирмените дейности
LPP002	Процедура: Идентификация и проследимост на продукти
LPP004	Процедура: Манипулиране, съхранение, опаковане и доставка на продукти
LPP302	Процедура: Техническа поддръжка на мрежови системи (Cisco Support)
LPP601	Процедура: Сервиз на технически и базови програмни средства
LAP004	Процедура: Работа с продукти, несъответстващи на определените изисквания

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

9. Оценки

Не се правят измервания за оценка.

10. Документирана информация

Сигурността на информацията, свързана с изпълняваните дейности по управление на продукти (технически устройства, софтуер, компоненти, писмени материали, чертежи, скици, други), собственост на клиент се осигурява от процедурите и инструкциите на въведената Система за управление на качеството и информационната сигурност.

Информацията, свързана с личните данни и търговската дейност на страните по договора се събира и използва само във връзка с посочените дейности и осигуряване на необходимото качество на тяхното изпълнение.

Приложимите записи за приемане, входящ контрол, проследимост и предаване на чужда собственост за сервизно обслужване се описват в процедурите и работните инструкции за реализация на функционалните дейности. Записите се съхраняват по установения ред в *LOMIS* или в други информационни фондове.

За случаите, които не се регламентират в документи на СУКИС се правят следните записи:

Протокол за повреда, загуба или нефункционална чужда собственост (форма *L-ADM-003-LDP*)		*симв.наименование*	Протокол за повреда, загуба или нефункционална чужда собственост
		индексация	по дата на изготвяне
	е-фонд	*активен*	*\LOMIS\Nonconforming\Foreign Products*
		достъп	
		съхранение	администратор *LOMIS;* 1 година
		архивен	*\LOMIS\Archiv\Nonconforming\Foreign Products*
		достъп	
		съхранение	администратор *LOMIS;* 5 години
	doc-фонд	*активен*	*"Повреди и загуби на материални ценности"*
		достъп	
		архивен	
		достъп	
		съхранение	деловодител, 5 години

приемателен протокол за чужда собственост (форма *L-ADM-012-RPR*)	*симв.наименование*		**RPRnnn** (nnn – пореден номер)
	индексация		nnn – пореден номер на протокола
	е-фонд	*активен*	*\LOMIS\Logistic\Receiving*
		достъп	C,W,U – автора, R - свободен
		съхранение	администратор *LOMIS;* 1 година
		архивен	*\LOMIS\Archiv\Logistic\Receiving*
		достъп	само R
		съхранение	администратор *LOMIS;* 5 години
	doc-фонд	*активен*	"*Приемателни протоколи – чужда собственост*"
		достъп	с разрешение на ръководител отдел *Логистика*
		съхранение	ръководител отдел *Логистика*; до връщане стоката на собственика
		архивен	архивно дело "*Приемателни протоколи-чужда собственост*"
		достъп	с разрешение на ръководител отдел *Логистика*
		съхранение	ръководител отдел *Логистика*; 3 години

10.1. Форми и бланки

ID на формата	*наименование на формата*
L-ADM-003-LDP	Протокол за загубена, повредена или нефункционална чужда собственост
L-ADM-012-RPR	Приемателен протокол за чужда собственост

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

ЛИРЕКС.КОМ	Процедура: Манипулиране, съхранение, опаковане и доставка на продукти	Версия 3
	LPP004	1 от 4

1. История на редакциите

версия	описание на промяната	автор	проверил	утвърдил	дата въвеждане
1	Редакция след документален одит	Д.Кънчев		Д.Илиева	01.09.2000
2	Въвеждане на изискванията на ISO/IEC 27001:2005	Д.Кънчев	Б.Йорданов	Д.Илиева	04.02.2009
3	Актуализиране на документите от СУКИС	М.Йончева	Вл.Иванов	Д.Илиева	01.08.2019

2. Предназначение

Тази процедура определя изискванията и методите за манипулиране, съхранение, опаковане и доставка на продукти (стоки), с цел осигуряване на тяхното качество (технически и функционални характеристики, окомплектованост, търговски вид).

Идентификацията и проследимостта на продуктите (стоките) се осъществява съгласно изискванията на процедура *LPP002*.

3. Приложимост

Процедурата се прилага по отношение на продуктите, които фирмата съхранява и обработва във всички свои офиси и доставя на свои клиенти.

4. Отговорности

4.1. Висше ръководство

- Организира цялостната дейност за манипулиране, съхранение, опаковане и доставка на продукти във фирмата.

4.2. Ръководителят на отдел *Логистика*

- Определя общите изисквания за манипулиране, съхранение, опаковане и доставка на продукти във фирмата, в съответствие със специфичните изисквания на всеки един от тях.
- Организира в звената от административно-стопанското направление общи и специфични процедури (ред) за манипулиране, съхранение, опаковане и доставка на продукти, и контролира за изпълнението им .

4.3. Управляващите процес / дейност

- Контролират съблюдаването в ръководените функционални звена на регламентирания ред за манипулиране, съхранение, опаковане и доставка на продукти.
- Определят реда, по който да се прилагат общите и специфични изисквания към манипулиране, съхранение, опаковане и доставка на продукти в офисните помещения, ползвани от подчинените им служители.

4.4. Завеждащ склад

- Организира и осигурява съхранението на продуктите в склада в съответствие с изискванията на настоящата процедура.

5. Процедура

5.1. Манипулиране

Манипулирането трябва да осигури начините за работа с продукт , така че последният да не се повреждa и да не влошава състоянието си.

Стандартните операции по манипулиране с продуктите при транспортиране, в складови или други помещения на фирмата, без да се нарушава техния външен вид и работоспособно състояние са приемливи, освен ако не се изисква специално манипулиране.

Разглобяването на устройство за промяна на окомплектоването му не трябва да води до повреждане или промяна на външния му фабричен вид.

Електронните носители се манипулират в съответствие с препоръките на производителя им.

5.2. Съхранение

Съхранението предпазва продуктите от повреда и от влошаване на състоянието им от момента на получаване във фирмата до момента на доставянето (предаването) им на клиента.

Стандартните условия за съхранение на продуктите в складови помещения по отношение на температура, влажност и противопожарна безопасност са приемат за достатъчни, освен ако не се изисква специално съхранение.

Продуктите могат временно да се съхраняват извън складовите помещения - в офисните помещения на фирмата, в Сервизния Център и на други места, като се спазват общите условия за съхранение. В този случай, ръководителят на съответното функционално звено определя допустимите места и начини на съхранение и лично инструктира подчинените си служители.

В складовите помещения продуктите се подреждат по рафтове и на пода, така че да бъдат достъпни без излишно преместване. При складирането стоките се подреждат по видове. Положението на кашоните трябва да съответства на указанията, отпечатани върху тях. Кашоните трябва да се подреждат с етикета отпред, за да може продуктите бързо да се идентифицират.

Продуктите с изтекъл срок за годност (мастила, тонери) в складовите помещения се съхраняват отделно от същите с неизтекъл срок и маркират с цветен етикет по установения начин.

Продукти, неотговарящи на изискванията (за окомлектованост и функционалност), се съхраняват на определени за целта места в складовите помещения и сервизните офисни помещения. Същите се маркират с цветен етикет по установения начин и пояснителни надписи върху етикета, ако е целесъобразно и необходимо.

Чужда собственост, получена за временно съхранение, се съхранява в складовите помещения отделно от другите продукти.

5.3. Опаковане

Опаковането осигурява качественото състояние на продукта при транспортиране и съхраняване .

Продуктите, които фирмата закупува от доставчиците, трябва да се съхраняват и транспортират в оригиналната си опаковка.

В случаите, когато не се разполага с оригинални опаковки, продуктите трябва да се поставят в подходящи по размери и здравина кашони. Празното пространство в кашоните трябва да се уплътни с хартия, а кашоните да се залепят с подходяща лепенка и етикет, показващ вида на стоката в кашона.

Ако габаритите на опакованата стока не позволяват пренасянето в помещенията на склада или в автомобила, то се допуска стоката да бъде освободена от тарата и по този начин да се пренесе. Тарата се съхранява и използва в оригиналния си вид впоследствие при доставка на клиента.

5.4. Доставка

Доставката осигурява транспортирането на продукти до и предаване на клиентите или между офисите на фирмата. При транспортиране се осигурява пълна съхраненост и окомплектованост на продуктите/ материалите.

Стандартните условия за транспортиране с лекотоварните автомобили на фирмата са приемливи.

Допустимо е доставката да се извърши посредством спедиторска фирма или чрез куриер, както и с транспорт на клиента. При доставката чрез куриер, на продукта трябва да се залепи етикет с адреса на клиента и на изпращача. Транспортните средства трябва да са пригодени за превозване на компютърна и комуникационна техника.

При транспортирането стоките се подреждат и ориентират, така както е предвидил производителят. Те трябва да се укрепват, така че да не бъдат повредени при аварийно спиране на автомобила.

Ако в договора с клиента са уговорени специални условия на транспортиране при доставката, ръководителят на отдел *Логистика* дава указания на специалистите как те да бъдат изпълнени.

6. Блок схеми

Не се изисква блок-схема за този документ.

7. Термини и съкращения

Продукт	Стоки, предмет на търговската дейност на фирмата. Технически средства и устройства, стандартен и базов софтуер, дистрибутивен материал за софтуер, или други компоненти и елементи, които се интегрират в разработвани и тествани от фирмата продукти или се доставят на клиентите по спецификация. Фабрично изработени или доокомплектовани / изработени стоки, които фирмата доставя на клиентите си.
Клиент	Юридическо или физическо лице, с което се сключва споразумение / договор за доставка на продукт или услуга.
Сигурност на информацията (информационна сигурност)	Запазване на поверителност, цялостност и наличност на информацията.
Състояние на продукт	Технически и функционални характеристики, окомплектованост, търговски вид.

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

Управляващ процес / дейност	Служител , в чиито правомощия и отговорности е дефинирано правото да управлява съответен процес / функционална дейност.

8. Препратки към документи

ID на документа	*наименование на документа*
LPP002	Процедура: Идентификация и проследимост на продукти

9. Оценки

Не се прилагат измервания.

10. Документирана информация

Сигурността на информацията, свързана с изпълняваните дейности по доставката на продукти и предаването им на клиентите се осигурява от процедурите и инструкциите на въведената Система за управление на качеството и информационната сигурност.

Информацията, свързана с личните данни и търговската дейност на клиентите се събира и използва само във връзка с точното и навременно извършване на доставките и осигуряване на необходимото качество на тяхното изпълнение.

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

1. История на редакциите

версия	описание на промяната	автор	проверил	утвърдил	дата въвеждане
2	Въвеждане на изискванията на ISO 9001:2008 и ISO/IEC 27001:2005	П.Димков	Б.Янчев	Д.Илиева	08.02.2008
3	Въвеждане на изискванията на стандарт ISO/IEC 20000-1:2005	П.Димков	Б.Йорданов	Д.Илиева	17.02.2010
4	Актуализиране на документите от СУКИС	М.Йончева	Б.Янчев	Д.Илиева	02.08.2019

2. Предназначение

- Дефинира управлението на конфигурация (УК).
- Определя ролята на УК, основните функции и процедури за реализацията им, неговите връзки с други процеси от СУКИС.
- Процедурата определя правилата за приложимостта на УК към специфичните изисквания на проектите и услугите.

3. Приложимост

Процедурата дефинира изискванията за УК, които се прилагат към хардуер, софтуер документация, данни и/или системи, доставяни на клиентите от *Лирекс.ком* и към свързани с проектите и услугите документи (планове, спецификации, чертежи и други), така както са определени в проекта или плана за управление на съответната външна ИТ услуга.

Процедурата се прилага от всички функционални звена на Лирекс.ком при създаване, описване, контролиране и промяна в характеристиките на конфигурации.

Общите изисквания към управлението на проекти и програми са определени в процедура *LPP006 Подготовка, преглед и сключване на договори*, а за реализацията на ИТ проекти – от модела, описан в документ LPN001.

Общите изисквания към управлението на външни ИТ услуги са описани в процедура *LPP013 – Управление на външни ИТ услуги*, като специфичните изисквания към всяка услуга са дефинирани в плановете за управление на съответната външна ИТ услуга.

Изискванията от тези документи трябва да се ползват и прилагат съвместно с настоящата процедура, за да се осигури установяването на подходяща система за управление на конфигурациите (УК) за продуктите, доставяни на клиенти.

Управлението на конфигурациите (УК) при сервизно поддържане се осъществява, като изискванията от настоящата процедура се ползват и прилагат съвместно с реда, определен в процедури *LPP301 Организация и управление на мрежово сервизно обслужване (Support)* и *LPP601 Организация и управление на сервизната дейност*, ако не е предвидена друга специфична за проекта процедура за целта.

4. Отговорности

4.1. Отговорен ръководител

- утвърждава промени от клас 1, съгласно възприетата класификация на промените.

4.2. Ръководител на проекта/ Отговорник за услугата

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

- организира и контролира всички дейности от процесите за управление на конфигурациите;
- определя и дефинира базовите конфигурации за проекта;
- планира дейностите за управление на конфигурацията;
- определя реда за обработка на предложения за промени в конфигурациите;
- одобрява предложения за промени от клас 2, съгласно възприетата класификация на промените;
- при необходимост, актуализира плана на проекта/плана за управление на услугата във връзка с промени на конфигурациите.

4.3. Отговорен за контрол на промените служител

- организира (и сам осъществява) поддържането в актуално състояние на описанията на конфигурациите, съгласно указанията на ръководителя на проекта;
- обработва постъпили предложения за промени в конфигурациите и съхранява документите във връзка с предложенията за промени.

4.4. Експерти

- внедряват (реализират) одобрени/утвърдени предложения за промени и верифицират извършваните промени;
- вземат решение за осъществяване на промени от клас 3, ако това е от тяхната компетенция;
- поддържат в актуално състояние описанията на конфигурацията и съпътстващата документация, съгласно изискванията от плана на проекта/плана за управление на услугата.

5. Процедура

5.1. Обект на управлението и същност на процеса

Установяването на подходяща база за *управлението на конфигурацията* изисква следните принципни процедурни стъпки:

- изготвяне на проект на базова документация на конфигурацията, предложена от изпълнителя на клиента;
- преглед на проекта от клиента и изпълнителя;
- внедряване на необходимите промени, резултат от прегледа;
- одобрение на базовата документация на конфигурацията от страна на клиента.

Основни цели на управлението на конфигурацията са:

- идентификация на конфигурацията на продукта или на негови компоненти (елементи и/или система);
- контрол на промените в конфигурациите, с цел поддържане интегрираност на продукта или услугата;
- проследимост на конфигурациите за периода на жизнения цикъл на продукта или услугата.

Управлението на конфигурацията (*УК*) се състои от четири основни процеса:

- *идентификация и документация* на конфигурация(ите), които гарантират качество на продукта или предоставяната услуга, съгласно определените изисквания и нива на удовлетвореност;

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

- *контрол на промените* на конфигурация(ите);
- *контрол* (наблюдение, следене), документиране и доклад за статуса на конфигурацията(ите);
- *удостоверяване* на конфигурация(ите) за съответствието им на изискванията.

Управлението на конфигурацията трябва да бъде планово през целия жизнен цикъл на продукта. За целта:

- При разработката на проект, моделът за УК се определя на етапа Предварителен проект (от фазата Системен анализ и планиране), съгласно LPN001 и се включва в документите за официално предложение към клиента, съгласно процеса за преглед на договора от процедура LPP001. След като се извърши преглед на изискванията на клиента (Възложителя) се изготвя техническа спецификация, която служи за база за идентификация и документиране на основната функционална документация.
- На по-късен етап се извършва преглед и анализ на проекта, за да се достигне до убеденост, че съставните елементи ще удовлетворят изискванията на системата. Положителните резултати от прегледа дават възможност документацията на конфигурацията да стане основна документация на разработката.

На този етап, в зависимост от изискванията на Възложителя, се определя най - ниското ниво на идентификация на елементите на конфигурацията.

Моделът установява основните изисквания на УК за доставяните продукти (хардуер, софтуер, системи) – базови конфигурации, управлявани конфигурации, изисквания за документиране, категоризация на промените, приложими методи и средства за верификация/валидация, проверка и документиране на статуса на конфигурация.

- Дейностите за УК трябва да се документират в плана по качеството или в самостоятелен *план за УК*. Ръководителят на проект или отговорника за предоставяне на услуга, в зависимост от мащаба на проекта/услугата и поетите ангажименти по договора, определя дали се разработва отделен план за УК. Планирането на дейностите за УК трябва да отчита изискванията на описаните по-долу части от описанието относно идентифицируемостта, промените, наблюдението и удостоверяването на конфигурацията(ите). Планът определя: извършваните дейности, длъжностните лица и техните отговорности; цитира или описва приложимите процедури, работни инструкции, наръчници и др. документи, чиито изисквания трябва да се спазват.

В зависимост от спецификата на проекта, планът за УК може да бъде одобрен от орган на възложителя, който го управлява или участва в управлението му.

Примерно съдържание на план за УК е представено в Приложение 1.

За периода на реализация на проекта или услугата до внедряването на продукта, ръководителят на проекта/отговорника за предоставяне на услугата организира и ръководи всички дейности във връзка с УК. За целта, определя от екипа на проекта служител, който отговаря за контрола на конфигурациите.

В течение на фазата за сервизно поддържане, ако е предвидена такава, УК се осъществява и в съответствие с процедурите за управление на мрежи *LPP301* или за управление на сервизната дейност *LPP601*. За идентифицирани специфични изисквания в проекта, на етапа *Работен проект* трябва да се разработят процедури, приложими за УК през периода на сервизното поддържане.

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

За периода на сервизно поддържане дейностите за УК се организират и ръководят от ръководителите на съответните функционални звена.

5.2. Идентификация на конфигурациите

5.2.1. Конфигурационни елементи

Хардуер, софтуер, бази данни, процеси, форми, документация и/или системи от продукта или услугата трябва да се групират в *конфигурационни елементи* – за краткост наричани в настоящата процедура *конфигурации*. Всяка конфигурация се разглежда като независима единица от системата за УК. Като общо правило, конфигурацията се определя за "делими" части от хардуера, софтуера и/или системите, които могат да бъдат проектирани, тествани и внедрени относително самостоятелно. Приложими са и други критерии за дефиниране на конфигурациите. (Например: за оборудване на функционално работно място, за изпълнение на определена системна функция, по вид оборудване по технически и операционни характеристики.)

Декомпозирането на продукта на конфигурации може да бъде специфицирано в изискванията на клиента, или да бъде извършено в процеса на анализа и дефинирането на изискванията към проекта. Определянето на конфигурациите трябва да завърши преди планиране изпълнението на проекта.

За всеки продукт се определят конфигурациите, които определят основните характеристики на продукта, - т.н. *базови конфигурации*. Те също трябва да бъдат описани в разработената документация за конфигурацията.

5.2.2. Идентифицируемост и проследимост

Всяка конфигурация на продукта трябва да получи уникален и предварително съгласуван идентификатор ID, който се определя както е подходящо. Последният се ползва в административните и техническите документи по управлението и за проследяване и доклад на статуса на конфигурацията.

Идентификаторът ID трябва да отразява:

- самата конфигурация, в контекста на описанието ѝ;
- реализацията (екземпляра) на конфигурацията, ако съществуват повече такива;
- версията на конфигурацията, ако същата е променена.

Структурата на идентификатора ID се определя от ръководителя на проекта/отговорника за услугата в зависимост от естеството на продукта, респ. конфигурацията.

5.2.3. Описание на конфигурация

Описанието на дадена конфигурация се определя от ръководителя на проекта или отговорника за предоставяне на услугата и може да има различна степен на детайлност и форма на представяне. С напредване на процеса за проектиране и разработка на продукта/услугата, описанията на конфигурациите стават все по-подробни.

Описанието на конфигурация може да включва:

утвърдена спецификация	какво трябва да представлява продуктът и неговите физически/технически характеристики. Може да бъдат представени като схеми, диаграми и скици на продукта/конфигурацията, да се описват технически и/или функционални характеристики;

техническа спецификация	списък на елементите, които изграждат конфигурацията, с техните количества. Може да включва логическо описание на конфигурацията – логическа схема (описателна или графична) на свързаност на елементите;
параметри и настройки	списък от параметри и настройки (различни от стойностите по подразбиране), използвани при конфигурирането на хардуерните и/или софтуерните елементи на конфигурацията (напр., параметри на хардуерните елементи в системата, директория за инсталиране на ОС, тип/брой на инсталираните лицензи, права и ограничения за достъп, други);
взаимовръзките с други конфигурации	включване в състава на друга конфигурация, влияние при промяна, въздействие върху базови конфигурации, други зависимости;
технологична карта за инсталация	списък от дейности, които изпълнени в описания ред водят еднозначно до описаната конфигурация;
план за действие при аварийни ситуации	списък с предварително идентифицирани потенциални проблеми и начин за тяхното предотвратяване или преодоляване.

Описанията на конфигурацията се документират по подходящ начин, определен от ръководителя на проекта/отговорника за услугата, в досието на проекта/плана за управление на услугата.

5.3. Контрол на промените

5.3.1. Иницииране на промени

Промяна на конфигурация се налага по различни поводи, някои от които са:

- промяна в спецификациите на проекта/конфигурацията;
- невъзможност да се достави определен елемент от системата;
- доказана невъзможност (по техническа информация или в резултат от опитна постановка) определен елемент от системата да изпълнява функции, които се изискват от утвърдените спецификации;
- промяна в логическата схема на свързаност, която изисква съответна промяна в използваните хардуерни/софтуерни елементи;
- промяна в параметрите и настройките на конфигурацията в резултат на оптимизация на производителността и/или цената;
- промяна в технологичната карта за инсталация на конфигурацията;
- промяна в хардуера и/или софтуера през периода на сервизно поддържане.

За всеки проект се създава система за управление на промените по модел, описан в процедура LPP012, където се проследява процеса на изпълнение на всяка промяна. При предоставянето на външни ИТ услуги се създава аналогично система за управление на промените за всяка конкретна услуга.

Ако е предвидено сервизно поддържане, промяна на конфигурацията при изпълнението му се осъществява в съответствие с установения ред за процесите за сервизно поддържане (процедури *LPP301* и *LPP601*) или с разработената за целта процедура (LPP012).

Контролът на конфигурациите започва от момента на първоначалното утвърждаване на описанията на продуктите и конфигурациите. Всяко предложение за промяна на конфигурациите се документира в системата за управление на промените, като за целта се попълва стандартната електронна бланка по образец, описан в процедура LPP012 "Управление на промените". Предложение може да даде клиент / потребител или всеки член на екипа за изпълнение на проекта. Ако предложението идва от клиент, заявката за промяна въвежда в системата упълномощен служител от името на клиента.

Заявките се приемат, обработват и докладват на ръководителя на проекта/отговорника за услугата от служителя, на когото е възложен контролът на конфигурациите. Последващите действия относно предложенията се определят от ръководителя на проекта/отговорника за услугата. Той отговаря за осигуряването на съхранението на всички заявки, както и обосновките за последващи действия (одобрение/ отхвърляне) към тях.

5.3.2. Оценка на промените

Всяко предложение за промяна в конфигурациите се анализира за въздействие върху безопасността, надеждността, възможностите за поддържане, функционалностите на системата/продукта, взаимовръзките между компонентите в системата/продукта, цената, графиците за изпълнение, изискванията на клиента/потребителя.

В зависимост от степента на влияние и изискваното ниво за одобряване, промените в хардуера, софтуера и/или системите и тяхната документация се класифицират, както следва:

клас 1	промени, които влияят на системните изисквания, външните интерфейси на системата, общата стойност и/или сроковете за доставка/внедряване. Трябва да се утвърдят от упълномощен представител на клиента и отговорния ръководител за проекта или услугата;
клас 2	промени, които могат доведат до изменения в интерфейсите или във функциите на отделните елементи в рамките на конфигурацията, в цената и/или сроковете за доставка/внедряване в границите на допустимото ниво на компетентност. Одобряват се от ръководителя на проекта/услугата;
клас 3	промени относно вътрешния дизайн и функционалностите на конфигурациите, без да се отразяват на утвърдените изисквания, цената и сроковете за изпълнение. Одобряват се от специалиста (експерта), отговарящ за техническото дефиниране (определяне) на конфигурацията.

5.3.3. Реализация на промените

Одобряването на промяна се извършва следвайки процеса на одобрение описан в процедура LPP012, и е основание за реализацията й.

Внедряването на промяна включва:

- дейности (проектантски, търговски, други) за реализация на промяната;

- актуализация на описанието (и документацията) на конфигурацията и създаването ѝ на нова версия, ако се прилага такъв механизъм. За нова версия се документира (записва): причината за пораждането ѝ; новото описание на промените елементи; реферирането на непроменените елементи към предишна версия;
- преглед на описанията на конфигурациите, които са свързани с променяната, и отразяване на промяната, ако има необходимост;
- уведомяване на всички заинтересовани лица от екипа на проекта за внедрявана промяна;
- изготвяне на план за действие при непредвидени ситуации и възникване на проблеми;
- актуализация на плана на проекта/услугата от ръководителя на проекта/отговорника на услугата, ако се налага.

Координацията на дейностите за внедряване на промените се осъществява от служителя, отговорен за контрола на конфигурациите.

Актуализацията на описанията се извършва от специалистите (експертите), които отговарят за съответната конфигурация, и се контролира от служителя – оторизиран за контрол на конфигурациите.

5.3.4. Верификация на промените

Внедряваните промени в конфигурация се верифицират в съответствие с процедура LSP701 Управление на пускане в действие. Това може да изисква повторно провеждане на тестове, съгласно плана за пускане в действие , или разработката и провеждането на допълнителни тестове. За промени в софтуер, в теста трябва да се включи и регресионно тестване, за да се гарантира, че не са допуснати грешки от промяна на съществуващи функционалности. Проведените тестове се документират съгласно утвърдения в процедура LSP701 начин.

Свидетелство за извършени промени в хардуера, софтуера и/или системи, са положителни резултати от проведени тестове за пускане в действие на промените, документирани по надлежен начин.

5.4. Контрол за статуса на конфигурации

Контролът на статуса на конфигурацията осигурява проследимост на всички промени в базовите конфигурации, като записите трябва да съдържат необходимата информация за идентификация и управление на произтичащите от промените действия.

Следенето на статуса на конфигурациите започва от първичния им дизайн, продължава през всички стадии на разработката, внедряване и поддръжка, т.е. през целия жизнен цикъл на продукта. Записите за статуса на конфигурациите включват информация за характеристиките на системата, версиите на използваните конфигурации, списък с направените промени, състояние на изпълнение на последните промени, и пр. Степента на тяхната детайлизация зависи от фазата, в която се намира проекта и се определя в плана за УК или в плана на проекта/услугата, където се определя и формата за реализация на записите.

Минималните изисквания за контрола на статуса на конфигурацията трябва да се концентрират върху следенето на заявките за промени, както следва:

- номер, дата, наименование, основание и приоритет;
- идентификация на равнозначните заявки;
- идентификация на елементите на конфигурацията;

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

- програма за обработката (одобрение, отхвърляне, внедряване на одобрената промяна).

Контролът на статуса на базовите конфигурации включва и периодични прегледи, така както е предвидено в плана на проекта/услугата или в плана за УК, ако е разработен такъв.

5.5. Удостоверяване (одит) на конфигурация

Проверката (одитът) на конфигурация може да бъде:

- ***техническа*** – проверява се дали конфигурацията включва всички елементи според описанията в техническата спецификация. Осигурява, че промените и всички изисквани елементи (хардуер, софтуер, и/или системи), процедури и експлоатационна документация са включени в доставяната версия на продукта. Обикновено се извършва при инсталация и предаване на продукта.
- ***функционална*** – проверява се дали конфигурацията функционира според утвърдените изисквания. Осъществява се при провеждане на функционални тестове за валидация на продукта.

Проверките и резултатите от тях се документират съгласно плана на проекта/услугата.

Проверка от независима трета страна се извършва, ако това се изисква от договора с клиента. За целта се разработва методика за изпълнение на проверката

6. Блок схеми

Не се прилагат блок – схеми.

7. Термини и съкращения

Клиент	Юридическо или физическо лице, с което се сключва или е сключен договор/споразумение за доставка на продукт .
Проект	Съвкупност от координирани и контролирани действия за реализацията на уникален продукт, при което се отчитат: • специфичните изисквания към характеристиките и качеството на продукта; • жизнения цикъл на проекта; • ограниченията във времето за изпълнение; • изискваните ресурси; • евентуални ограничения за цена.
Жизнен цикъл на проект	Поредица от събития, операции и процеси, които включват проектиране, разработка, инсталация, тестване, системна интеграция, експлоатация, сервиз и излизане от употреба (действие) на продукта на проекта.

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

Система	Комбинация от елементи, които функционират заедно за постигане/задоволяване на определени цели/потребности. Тези елементи могат да включват: хардуер; софтуер; оборудване; персонал; технологични процеси и процедури.
Елементи	Включват (без да изчерпват) устройства, компоненти и/или софтуер, които се интегрират в крайния продукт.
Конфигурация	Конфигурация от хардуер и/или софтуер, или системи, която се характеризира с: ➢ технически и операционни параметри с техните настройки; ➢ функционалности; ➢ реализуеми функции. Определя се в техническа/проектна документация и е реализирана в продукта.
Базова конфигурация	Конфигурация от хардуер и/или софтуер, и/или системи, която определя основните характеристики на продукта за определен период от жизнения му цикъл. Служи за основа за отчитане на промените в конфигурацията.
Верификация	Дейност, осъществявана на подходящи етапи от процеса за реализация на проект/система с цел гарантиране, че полученият резултат отговаря на изискванията за този етап. Може да се състои от преглед на дизайна, изчисления, анализи, проверки и/или тестове.
Валидация	Дейност за преглед и/или тестване за получаване на обективни доказателства, че конфигурацията отговаря на изискванията и ще изпълни своето предназначение.
Отговорен ръководител (ОР)	Лице, притежаващо пълномощия за възлагане ръководство на проект, за преглед и одобряване на записи по качеството за проект.
Ръководител на проект (РП)	Лице, отговорно за оперативното (административно и техническо) ръководство на проект.

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

Одобряване	Акт за съгласие (приемане) със съдържанието на записа/ документа, респ. предвидените действия. Може да се осъществи със собственоръчен/електронен подпис, с e-mail, факс – съобщение.
УК	Управление на Конфигурацията
План за управление на конфигурацията (УК)	Документ, който описва обхвата и организацията на УК, използваните процедури и необходимото взаимодействие с представители на всички заинтересовани страни.
ИТ	Информационни технологии.
ДГК	Държавната гаранция за качеството представлява процес, с помощта на който съответните национални органи вдъхват увереност в това, че договорните изисквания по отношение на качеството са изпълнени.
Система за управление на качеството и информационната сигурност (СУКИС)	Организационната структура на *Лирекс.ком* в комплекс с регламентирания ред, процесите и ресурсите, необходими за управление качеството и на информационната сигурност на предлагани продукти и услуги.
Лирекс.ком	Дружествата Лирекс БГ, Лирекс БС, Лирекс Хай Тех, Беолик, Лирекс Скопие, Теза

8. Препратки към документи

ID на документа	*наименование на документа*
LMP002	Процедура: Управление на документи и записи за реализация на фирмените дейности
LPP006	Процедура: Управление на програми и проекти
LPP012	Процедура: Управление на промените
LPP013	Процедура: Управление на външни ИТ услуги
LPN001	Модел за реализация на ИТ проект
LPP301	Процедура: Организация и управление на Cisco Support
LPP601	Процедура: Организация и управление на сервизната дейност

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

9. Оценки

Не се прилагат.

10. Документирана информация

Планът за УК, ако се разработва такъв, се съхранява в досието на проекта/услугата, съгласно изисквания от процедура *LPP006 Управление на програми и проекти, LPP013 Управление на външни ИТ услуги* и от *модела за управление на ИТ проект LPN001*.

Заявките за промени, както и резолюциите за внедряването им се съхраняват в системата за управление на промените към съответния проект/услуга или в централната система. Записите се съхраняват в електронна форма в дневника на промените.

Описанията на конфигурациите се съхраняват в :

- досието на проекта/услугата, съгласно изисквания от процедури *LPP006 Управление на програми и проекти и LPP013 Управление на външни ИТ услуги* и от *модела за управление на ИТ проект LPN001;*
- в досието на клиента/ обекта, където е локализирана конфигурацията, съгласно изискванията на процедури *LPP301* и *LPP601* за управление на сервизните дейности.

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

Приложение 1

ПЛАН ЗА УПРАВЛЕНИЕ НА КОНФИГУРАЦИЯТА

(примерно съдържание)

1. Предназначение и обхват;
2. Описание на елементите на конфигурацията;
3. Дефиниции;
4. Приложими документи – спецификации, стандарти, ръководства и др. документи;
5. Организация на управлението на конфигурацията:
   - основни положения;
   - отговорности и правомощия на участниците (групи и организации);
   - органи по управлението на конфигурацията и техните отговорности, правомощия и принадлежност;
   - взаимоотношения в рамките на организацията на проекта;
   - функционална организация;
   - организация по УК;
   - услуги по поддръжка.
6. Идентификация и документиране на конфигурацията
7. Определя реда за осъществяване на:
   - избор и идентификация на конфигурационни елементи, включително връзката с работната структура на конфигурацията;
   - усъвършенстване, номериране, промени и поддържане на спецификации и тяхната взаимовръзка;
   - подготовка, идентификация и ревизия на документация и каталози;
   - установяване на базова конфигурация за съответната фаза от жизнения цикъл на проекта;
   - определяне на номенклатури и серийни номера;
   - официално одобряване на документацията на конфигурацията.
8. Контрол на конфигурацията:
9. Определя реда за осъществяване на:
   - контрол на конфигурацията;
   - подготовка, преглед и предаване за обработка на предложения (заявки) за промени;
   - подготовка, преглед и предаване за обработка на предложения за отклонения и разрешенията за отклонения;
   - обявяване на решенията относно предложения за изменения, предложения за отклонения и разрешенията за отклонения;
   - осигуряване на актуализация на документацията на конфигурацията с одобрените промени;
10. Контрол на статуса на конфигурацията
11. Определя реда за събиране, документиране, преглед и поддържане на данните, които са необходими за изготвяне на отчети:
    - форма и необходими данни за записите за статуса на конфигурацията;
    - съдържание и форма на докладите за статуса на конфигурацията.
12. Одити на конфигурацията:

За актуалната редакция и съдържание на процедурата проверете в *LODIS*.

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

- процедури за функционален и технически одит;
- форма за доклад на резултатите от одитите;
- график за одити.

13. График за извършване на прегледи на проекта;
14. Основни контролни точки за всички фази от жизнения цикъл на проекта.

За актуалната редакция и съдържание на процедурата проверете в *LODIS*.

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламейт (ЕС) 2016/679

ЛИРЕКС.КОМ	Процедура: Управление на outsourcing процеси	Версия 3
	LPP009	1 от 7

1. История на редакциите

версия	описание на промяната	автор	проверил	утвърдил	дата въвеждане
1	Въвеждане на изискванията на ISO 9001:2008 и ISO/IEC 27001:2005	П.Димков	М.Цолов	Д.Илиева	02.02.2004
2	Въвеждане на изискванията на ISO/IEC 20000-1:2005	П.Димков	Б.Йорданов	Д.Илиева	10.02.2009
3	Актуализиране на документите от СУКИС	М.Йончева	Б.Янчев	Д.Илиева	05.08.2019

2. Предназначение

Процедурата определя основните етапи на реализация на outsourcing процеси.

3. Приложимост

Определеният в процедурата ред трябва да се прилага от всички функционални звена при сключване на договори за outsourcing на бизнес процеси.

Поради разнообразието и сложността на бизнес-процесите при потенциалните клиенти, всички случаи на outsourcing се разглеждат като самостоятелни проекти и се управляват в съответствие с изискванията на настоящата процедура и на процедурите LPP013 "Управление на външни ИТ услуги" и LPP013 "Управление на програми и проекти".

4. Отговорности

4.1. Висше ръководство

- осигурява политиката за управление на ИТ услугите да съответства на целите на дружествата Лирекс.ком, да гарантира изпълнението на предоставяните ИТ услуги в съответствие с приложимите законови и други приети или договорени изисквания, да бъде периодично преглеждана за адекватност и актуализирана при необходимост с цел непрекъснато подобряване на дейността;
- осигурява необходимите и достатъчни ресурси за изпълнение на договорените ИТ услуги;
- съвместно с ръководителите на функционалните звена определя целите по въведения ISO/IEC 20000-1 в СУКИС на дружествата Лирекс.ком;
- разработва стратегията за постигане на целите по ISO/IEC 20000-1 в СУКИС, като осигурява необходимите кадрови и материални ресурси;
- определя правомощията и отговорностите на служителите за гарантиране, че процесите за управление на ИТ услуги са проектирани, планирани, изпълнявани и подобрявани в съответствие с политиката и целите за управление на услугите;
- ежегодно прави преглед за съответствие на дефинираните цели с декларираните политики по въведеният ISO/IEC 20000-1 в СУКИС,
- съвместно с ръководителите на функционални звена анализира степента на постигане на определените цели по ISO/IEC 20000-1 и ги актуализира в зависимост

от пазарните условия, законовите промени и изискванията и очакванията на клиентите

4.2. Ръководители на функционални звена

- планират необходимите и достатъчни ресурси за изпълнение на договорените ИТ услуги;
- организират взаимодействието и комуникацията с клиентите във връзка с исканите от тях ИТ услуги;
- организират и координират дейностите във връзка с прегледа на договорите и уточняване на изискванията на клиентите;
- организират документирането на дейностите във връзка с договорените ИТ услуги в съответствие с изискванията на приложимите в процеса процедури по СУКИС;
- гарантират, че активите, включително лицензите, използвани при доставянето на ИТ услугите, се управляват в съответствие с приложимите законови изисквания и други договорени задължения;
- информират служителите за важността на спазването на въведената политика, на изискванията на стандарта ISO/IEC 20000-1 и последствията от тяхното нарушаване, както и необходимостта от непрекъснато им подобряване;
- организират и координират всички дейности във връзка с изпълнение на целите по договорените ИТ услуги, като при необходимост възлагат на друг служител организацията и координацията на конкретна услуга;
- одобряват и утвърждават документите и записите във връзка с изпълнението на договорите за доставка на ИТ услуги;
- периодично отчитат и докладват за състоянието, постигнатите резултати, проблемите и предстоящите задачи по изпълнението на ИТ услугите от ръководените от тях звена;

4.3. Отговорник за ИТ услугата

- изпълнява дейности съвместно с ръководителя на функционалното звено или по негово нареждане във връзка с прегледа на договора и уточняване на изискванията на клиентите;
- по нареждане от ръководителя на функционалното звено организира и координира дейностите във връзка с изпълнението на договорените ИТ услуги;
- по нареждане от ръководителя на функционалното звено комуникира с клиентите във връзка с исканите от тях обучения;
- отговаря за съставянето, правилното поддържане, съхранение и архивиране на всички записи в процеса на изпълнение на договора за доставка на ИТ услуги на клиента.
- обобщава резултатите от мненията и препоръките на клиентите за предоставяните им ИТ услуги.

4.4. Упълномощен представител на ръководството

- отговаря за координацията и управлението на всички външни ИТ услуги, предоставяни от дружествата Лирекс.ком;
- осигурява интегрирането на всички дейности по предоставянето на ИТ услуги във въведената СУКИС в дружествата Лирекс.ком;

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

- организира и участва съвместно с ръководителите на функционалните звена и отговорниците на услуги в изработването на документирани процедури и планове за управление на предоставяните ИТ услуги
- организира провеждането на Прегледи от ръководството на СУКИС, на които се обсъжда изпълнението на целите по управление на външните ИТ услуги по стандарта ISO/IEC 20000-1, тяхната ефективност, подобряване и приемането на нови цели.

5. Процедура

5.1. Общи изисквания

Процесът на outsourcing преминава през следните етапи:

- идентификация на изискванията на клиента и проучване на процеса с цел изясняване на възможностите за outsourcing;
- съгласуване на SLA, подготовка и сключване на договор;
- приемане управлението на процесите, предмет на outsourcing от екип на клиента;
- извършване на договорените дейности, предмет на договора (вкл. генериране на периодични отчети за нивото на извършваните услуги, съгласно SLA) и текущото управление;
- предаване управлението на предмета на outsourcing на екип на клиента.

Управлението на процеса се реализира съобразно процедура LPP013 и има за цел:

- осигуряване на условия за пълно удовлетворяване изискванията на клиента, според SLA;
- прилагане на единни принципи за осигуряване качеството на всички стадии от процеса;
- контрол за изпълнението на дейностите от всеки елемент на процеса в съответствие с изискванията на СУКИС, определени от общосистемните процедури.

Организацията и координацията на дейностите във връзка с договора за outsourcing се осъществява от отговорника на услугата, който се определя съгласно изискванията на процедура *LPP013*.

Документиране на операциите и дейностите във връзка с реализацията на дейностите се осъществява в съответствие с изискванията на приложимите в процеса общосистемни процедури за управление на ИТ услуга (и процедура *LMP002*) и съгласно изискванията за информационна сигурност. За документирането отговорят служителите, участващи в предоставянето на услугата и отговорника на съответната услуга.

Взаимодействието и комуникациите с клиента се организират от отговорника на услугата, определен съгласно процедура *LPP013*.

5.2. Идентификация на изискванията на клиента и проучване на процеса

Предмет на дейността е преглед на изискванията на клиента, текущите му и предполагаемите му бъдещи потребности, основните характеристики на процесите и възможностите на Лирекс.ком да посрещне потребностите на клиента с ресурси и технологични познания. Прегледът се ограничава до обхвата (Scope) на договора, освен ако страните не смятат, че предоставянето на допълнителна информация, би довело до по-прецизна оценка за изискванията на клиента.

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

5.3. Съгласуване на SLA, подготовка и сключване на договор

Осъществява се по реда, определен в процедура *LPP013 Управление на външни ИТ услуги.*

Съгласуването на SLA трябва да се извърши между клиента и екипа в Лирекс.ком, отговорен за реалното извършване на договаряните услуги.

5.4. Приемане управлението на процесите от екип на клиента

Преди процеса на реално приемане на процесите за управление, се извършва детайлно проучване, събиране и запознаване с експлоатационната документация за начините на текущо извършване на процесите, набори от конфигурации и параметри които се следят и поддържат, и др.

При встъпване в ролята на outsourcing организация, Лирекс.ком приема управлението на процесите от екип на клиента(или от друг outsourcing provider). В някои случаи е възможно за определено време процесите да бъдат наблюдавани и управлявани от съвместен екип на клиента и Лирекс.ком (преходен период). При приемането на дейностите за управление се подписвана двустранен констативен протокол. В протокола се описват всичката необходима информация за коректното изпълнение на дейностите (пароли за достъп до информационни системи, списъци с потребители и др.), както и текущото състояние на управляемите системи.

5.5. Извършване на договорените дейности, предмет на договора

За периода на действие на outsourcing договора, Лирекс.ком извършва дейностите, съгласно утвърдения Scope, SLA и в съответствие с политиката на СУКИС.

При извършването на дейностите се спазват формални процедури за работа, които са:

- предложени от клиента и приети от звеното на Лирекс.ком (ръководителя на проекта), извършващо услугите; или
- стандартни процедури на Лирекс.ком и приети от клиента; или
- разработени и предложени от звеното на Лирекс.ком (ръководителя на проекта) специално за конкретния договор и приети от клиента.

Ако отговорникът на услугата сметне за целесъобразно провеждането на допълнително обучение за специалистите на доставчика на аутсорсинг услуги, с цел постигане (поддържане) на необходима квалификация за изпълнение на outsourcing дейностите, той планира такова обучение в съответствие с процедура *LPP013* и по реда на процедура *LRP001* в отделен план за обучение, различен от плана за обучение на специалистите в Лирекс.ком, към което те се числят.

Ако в договора има дефинирани срокове за отчитане на следените параметри по SLA, то отчетите се предоставят на клиента според тях, ако такива срокове няма фиксирани, то отчетите се предоставят през първата седмица на всяко започнало тримесечие по договора.

5.6. Предаване управлението на процесите от екип на клиента

След изтичане срока на договора, Лирекс.ком има задължението обратно да предаде на екип на клиента (или на друг outsourcing provider) поддържаните системи/услуги в работоспособен състояние. Предава се също и техническата документация, която е изготвена във връзка с разработени обслужващи системи, фигуриращи в обхвата на договора, справки за системните услуги, параметри за настройка и др.

При предаване се подписва двустранен констативен протокол.

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

6. Блок схеми

Не се прилага блок схема за описанието на процеса.

7. Термини и съкращения

Outsourcing (Превъзлагане)	Договор, сключен между юридическо лице и друго юридическо или физическо лице за временно цялостно възлагане на управлението и /или подобрението на дейности, отнасящи се частично или напълно към: • технологична инфраструктура (информационни системи – хардуер и софтуер, системи за сигурност, телекомуникационни мрежи и др.) • приложения (поддръжка email, управление / хостване на бази данни, управление на ERP, CRM и др.) • оперативни процеси (доставки на материали, промишлено производство, управление на телекомуникационна среда, поддръжка на потребители и др.) • бизнес процеси (управление на човешките ресурси, маркетинг, ТРЗ, фактуриране и др.) • реструктуриране на бизнес процеси При сключването на договора за outsourcing се прехвърля и отговорността за извършване на възложените процеси според съответно договорен SLA (service level agreement). Превъзлагането може също да включва прехвърляне на материални активи и/или човешки ресурси.
Scope (Обхват)	Съвкупност от всички услуги, предмет на outsourcing договора.
SLA (service level agreement), договор за нива на обслужване	Документ – самостоятелен или част от договора за outsourcing, който определя критериите за минимално допустими нива на обслужване
Клиент	Юридическо или физическо лице, с което се сключва или е сключен договор / споразумение за доставка на продукт / услуга.
Продукт	Разработки, стоки и услуги, предмет на търговската дейност на фирмата.

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

Стока	Фабрично производство, със стандартни (технически и функционални) характеристики и гаранционни условия.
Договор / Споразумение	Документирана договореност за предоставяне на продукт от фирмата на клиент, с точно определени изисквания, потвърдени от двете страни.
Преглед на договора	Дейности преди подписване на договора за удостоверяване, че всички изисквания на клиента относно качеството на предоставяните продукти са точно и еднозначно определени, документирани и могат да се изпълнят.
Проект	Съвкупност от координирани и контролирани действия за реализацията на уникален продукт и/или услуга, при което се отчитат: • ограничения на времето за изпълнение (начална и крайна дата); • специфични изисквания към характеристиките и качеството на продукта / услугата; • изискваните ресурси; • евентуални ограничения за цена.
Сделка	виж **Договор / Споразумение**
Водещ сделка	Служител, на когото е възложено организацията на прегледа по договора на постъпила заявка за сделка и координацията по изпълнението на сделката.
ИТ	Информационни технологии.
Система за управление на качеството и информационната сигурност (СУКИС)	Организационната структура на *ЛИРЕКС.КОМ* в комплекс с регламентирания ред, процесите и ресурсите, необходими за управление качеството и на информационната сигурност на предлагани продукти и услуги.
Лирекс.ком	Дружествата Лирекс БГ, Лирекс БС, Лирекс Хай Тех, Беолик, Лирекс Скопие, Теза
ERP	Enterprise Resource Planning – система за управление на бизнеса

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

CRM	Customer Relationship Management – система, обслужваща клиентски-ориентирана бизнес стратегия, включва обслужването на процесите маркетинг, продажби и услуги.

8. Препратки към документи

ID на документа	наименование на документа
LMP002	Процедура: Управление на документи и записи за реализация на фирмените дейности
LRP001	Процедура: Квалификация и обучение
LPP001	Процедура: Подготовка, прегледи и сключване на договори
LPP006	Процедура: Управление на програми и проекти
LPP013	Процедура: Управление на външни ИТ услуги
LPP007	Процедура: Управление на конфигурацията
LPN001	Модел за управление на проект
LQS Manual	Наръчник на СУКИС на Лирекс.ком

9. Оценки

Не се прилагат измервания.

10. Документирана информация

Необходимите записи се определят в съответните общосистемни процеси, приложими за управление на процеса.

Не се изисква приложението на специфични форми и бланки, а се прилагат изискваните от цитираните системни процедури такива.

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

1. История на редакциите

версия	описание на промяната	автор	проверил	утвърдил	дата въвеждане
1	Начална редакция	П. Димков	Б.Янчев	Д.Илиева	12.02.2009
2	Въвеждане на изискванията на стандарт ISO/IEC 20000-1	П. Димков	Б.Янчев	Д.Илиева	18.02.2010
3	Актуализиране на документите от СУКИС	П.Димков	Б.Янчев	Д.Илиева	05.08.2019

2. Предназначение

Процедурата определя процесите, изискванията и отговорностите, които трябва да се спазват при извършването на промени в ИТ инфраструктурата на дружествата Лирекс.ком, изпълнението на проекти и при предоставянето на външни услуги.

Целта на процеса по управление на промените е да гарантира, че всички промени са разгледани и изпълнени по рационален начин, водещ до повишаване на ефективността, намаляване на влиянието на инцидентите, свързани с извършването на промени, както и постепенно подобряване на ежедневните дейности в Лирекс.ком.

3. Приложимост

Процедурата е задължителна за всички служители, които имат и носят отговорност за извършването на промени в инфраструктурите на Лирекс.ком и неговите клиенти.

Прилага се при предоставянето на външни услуги, управлението на проекти, а така също и при управлението на информационните активи и ресурси, при контрола и защитата на корпоративната мрежа, при управлението и контрола на задаваните привилегии.

4. Отговорности

4.1. Висше ръководство

- одобрява вътрешнофирмената политика за управление на промените;
- налага по съответния ред дисциплинарни наказания на служителите, които не спазват политиката за управление на промените.

4.2. Заявител

- подготвя и подава заявка за промяна с цел удовлетворяване на възникнала нужда.

4.3. Консултативният съвет по промените

- приема дадената заявка и обсъжда заявената промяна;
- прави оценка на влиянието на предложената промяна върху извършващите се процеси;
- прави оценка на риска от промяната;
- налага спазването на процедурата за управление на промените;
- обновява процедурата за управление на промените.

4.4. Ръководителят на промените

- участва в Консултативния съвет при планирането на промените и при оценяване на рисковете;

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

- организира и координира дейностите във връзка с изпълнението на одобрените промени;
- следи изпълняващият промените за коректното им изпълнение;
- работи в тесни взаимоотношения с функционалните експерти при изработването на планове за изпълнение на промените, тестване и възстановяване в случай на възникване на проблеми;
- в зависимост от планираните дейности назначава изпълнители на отделните дейности по извършването на промените;
- приема доклади за изпълнение от изпълняващият промяната;
- обобщава резултатите от извършените промени и затваря заявката.

При промени, свързани с изпълнението на проект, за ръководител на промените се счита ръководителят на съответния проект.

При промени, свързани с предоставянето на външни услуги, за ръководител на промените се счита Отговорника по предоставянето на услугата.

4.5. Одобряващ промените

- лице или група лица, на които е поверена отговорността и задължението да преглеждат и одобряват заявките за изпълнение на промени, като позволяват стартирането на фазата на изпълнение;
- задълженията на одобряващият промените се дефинират предварително или се възлагат в процеса на работа.

По подразбиране за одобряващ промените се счита Консултативния съвет по промените, с изключение на случаите, в които има специално дефиниран одобряващ промените за определена категория или тип промяна.

При промени, свързани с предоставянето на услуги на външни клиенти, одобряващ промените е отговорно лице за контакт от страна на клиента дефинирано при съгласуването на договорните споразумения и описано в плана за управление на съответната услуга.

4.6. Изпълняващият промените

- създава план за тестване, изпълнение и възстановяване при подготовката за извършване на промяната;
- при необходимост и по нареждане на ръководителя на промените извършва предварителни тестове в тестовата среда преди изпълнението на промените в продуктивната среда;
- изпълнява дейности съвместно с ръководителя на промените или по негово нареждане във връзка със заявените промени;
- комуникира със заявителя на промяната, за да се гарантира, че извършваните промени отговарят точно на изискванията на заявителя;
- обновява документацията, свързана с извършените промени;
- докладва на ръководителя на промените за коректното изпълнение на дадена промяна.

5. Процедура

Процедурата за управление на промените описва процесите, които се извършват при подаването на заявка за промяна, нейното одобрение и изпълнение. Целта е да се постигне

прозрачност при извършването на промени, да се улесни комуникацията между различните заинтересовани страни и да се сподели технически опит и умения.

5.1. Обща политика

Целта на процеса по управление на промените е да гарантира, че всички промени са разгледани и изпълнени по рационален начин, водещ до повишаване на ефективността, намаляване на влиянието на инцидентите, свързани с промени, както и постепенно подобряване на ежедневните дейности в Лирекс.ком и неговите клиенти.

Не се допуска изпълнението на промени без да се следват изискванията и стъпките на настоящата процедура. При неспазване на това правило, служителите носят дисциплинарна отговорност.

5.1.1. Изпълнение на стандартна промяна

Стандартните промени следват пълния и предварително дефиниран процес по управление на промените. Те биват разглеждани, приоритизирани и одобрявани, като се насрочва дата/период за тяхното изпълнение.

Приоритизирането на промените се извършва в зависимост от разбирането за това какво влияние би оказала промяната върху бизнеса и с каква спешност би трябвало тя да бъде извършена. Приоритетите на стандартните промени биват разделени на:

- **висок приоритет** – промяната се планира за извършване в най-кратък срок. Забавянето на нейното изпълнение би довело до негативни последици за бизнеса на Лирекс.ком или на неговите клиенти.
- **среден приоритет** – промените се планират за извършване в нормалният график за извършване на промени. Този график се разглежда от консултативния съвет по промените веднъж седмично.
- **нисък приоритет** – промяна с нисък приоритет бива планирана за изпълнение в някакъв бъдещ период, но нейното забавяне по никакъв начин не би оказало влияние на дейностите, извършвани от Лирекс.ком.

Приоритизирането на промените се предлага от подаващият заявката за промяна, но се одобрява и при необходимост променя, от ръководителя на промените или от консултативния съвет по промените.

Одобрението се извършва от одобряващ промените или от консултативния съвет по промените на редовната му среща. Стандартните промени биват добавяни в графика за извършване на промените.

5.1.2. Изпълнение на критична промяна

Критичните промени са стандартни промени, които трябва да бъдат извършени незабавно и не може да бъдат планирани за изпълнение в бъдещ период. Тези промени са необходими в случаи, при които дадени основни системи или приложения са спрели да функционират и не са налични други стандартни методи за тяхното възстановяване. Критични промени се налагат, но не са ограничени, при случването на следните събития:

- прекъсване работата на мрежата;
- прекъсване на система или приложение, което води до отрицателно въздействие върху бизнеса;
- отрицателно въздействие върху голям процент от потребители, без възможност за алтернативен начин за разрешаването му;

- случай на природно бедствие;
- отговор на спешна бизнес нужда.

Тези промени се заявяват с най-висок приоритет (критичен) и степен на спешност. За изпълнението им е необходимо получаване на незабавно одобрение или отхвърляне от одобряващият промяната или при необходимост - от консултативния съвет по промените.

5.1.3. Изпълнение на предварително одобрена промяна

В случай, че дадена промяна вече е била извършвана като е преминала през нормалния процес на оценка и одобрение и е доказана нейната повтаряемост, е възможно тя да получи предварително одобрение за последващите й изпълнения. Този тип промени се въвеждат в матрицата на предварително одобрените промени. Трябва да се гарантира, че рискът от тяхното проявление е добре премерен и е дефиниран като приемлив.

Предварително одобрените промени притежават повечето или всяка от следните характеристики:

- промяната е успешно реализирана в миналото;
- промяната бива извършвана често;
- действията при изпълнението на промяната са повтаряеми и идентични;
- налични и достъпни са ефективни планове за извършването на промяната;
- промяната не е критична;

5.1.4. Категоризация на промените

Извършваните промени попадат в категориите, представени в следната таблица:

Код	*Категория*	*Описание*
HW	Хардуерни	Инсталиране на хардуерни компоненти. Промяна в конфигурацията на хардуера. Ликвидиране на хардуерни компоненти.
SW	Софтуерни	Внедряване на нов софтуер. Модификации в софтуерни настройки. Инсталиране/модифициране/премахване на операционни системи. Обновяване версии на софтуер. Инсталиране на „кръпки".
UR	Потребителски	Създаване/модифициране/изтриване на потребителски акаунти. Промени в достъпа на потребителите до ресурси и системи. Промени, свързани с използването на телефони от потребителите.
IN	Инфраструктурни	Инсталиране/модифициране/премахване на структурни кабелни системи. Конструктивни действия свързани със сървърни помещения и други инфраструктурни обекти. Промени в пожароизвестителна/пожарогасителна инсталация. Промени в климатичните системи. Промени в системите за контрол на достъпа.

Код	Категория	Описание
PR	Процедурни	Промени, свързани с модификации на съществуващи и създаване на нови процеси и политики. Промени по Системата за управление на качеството и информационната сигурност (СУКИС) на Лирекс.ком Промяна на документи и процедури, свързани с поддръжката и обслужването на информационните системи.
NW	Мрежови	Промени в мрежовите конфигурации и компоненти. Модификации в преносната среда.
CN	Договорни	Промени в съществуващи договори.
NP	Нов проект / Вътрешен портал	Промени свързани със създаването на нови проекти във Вътрешния Портал (http://eportal.lirex.com)
ES	Външни IT услуги	Внедряване на нова външна услуга Модифициране на обхвата на изпълнявана външна услуга Прекратяване предоставянето на външна услуга

5.2. Общи изисквания

Всички служители на Лирекс.ком, които подават заявки за извършване на промени са длъжни да познават и спазват процедурата за управление на промените. Неспазването на процедурата може да доведе до извършването на неоторизирани промени, които биха предизвикали смущения и евентуални загуби за Лирекс.ком.

Ръководителите на отделните звена са стимулирани да създават и доразвиват вътрешни добри практики, процедури и въпросници, които да подпомагат процесите по управление на промените. Те са длъжни да определят изискванията, които трябва да се покрият при изпълнението на дадена промяна ако тя е свързана с ИТ средата, управлявана от съответния ръководител.

При необходимост от извършване на промени, наложени от производители на хардуер и софтуер, използван от Лирекс.ком, съответните промени следват нормалния процес на управление на промените, описан в текущия документ.

За управлението на вътрешните промени се използва система за управление на промените, достъпна за служителите на Лирекс.ком. При предоставянето на услуги на външни клиенти, за всеки клиент се изгражда индивидуална система за управление на промените.

Възможно е при сключването на договор за предоставяне на услуги за клиент да бъде договорено използването на система за управление на промените при самия клиент ако той разполага с такава. В такъв случай е необходимо да бъде извършено обучение за използване на системата от страна на клиента към поддържащия екип.

5.3. Фази на изпълнение

Процедурата по управление на промените обхваща всички промени, които биха повлияли на нормалната работа на хардуер, софтуер, приложения работещи в продуктивната и тестова среда на Лирекс.ком и при неговите клиенти.

Източниците на промени включват, но не са ограничени до следния списък:

- поддръжка на хардуер и приложения;

- потребителски заявки за добавяне, модифициране или премахване на обекти от ИТ инфраструктурата;
- обновяване на хардуерни или софтуерни компоненти;
- реагиране при възникване на неочаквани събития – инциденти и проблеми;
- проактивни модификации и подобрения на инфраструктурата;
- специфични промени, свързани с конкретен проект.

По време на изпълнение на заявката в системата за управление на промените може да се проследява нейния статус, както следва:

- ***приета*** – заявката е постъпила за преглед на информацията и оценка;
- ***чакаща за одобрение*** – събрана е необходимата информация и заявката е пусната за одобрение от одобряващия промените;
- ***одобрена/отхвърлена*** – заявката е одобрена или отхвърлена от одобряващия промените. Ако е отхвърлена се преминава към затваряне;
- ***в изпълнение*** – след одобрение на заявката тя преминава във фаза на изпълнение;
- ***изпълнена*** – промяната е изпълнена и се чака потвърждение от заявителя за правилното й изпълнение;
- ***затворена*** – след получаване на потвърждение от заявителя, заявката за промяна се затваря в системата.

5.3.1. Подаване на заявка и планиране

По време на тази фаза се извършва попълването и подаването на заявка за промяна в системата за управление на промените. Електронната бланка за попълване е достъпна на следния адрес:

http://eportal.lirex.com/Projects/InternalSystems/ChangeManagement/default.aspx

За промени, свързани с конкретен проект, се попълва заявка за промяна от системата за управление на промени за съответния проект.

Заявки за промени от страна на клиенти на Лирекс.ком, подавани във връзка с изпълнението на дадена услуга се подават чрез създадената за клиента система или чрез електронна поща. Други начини за подаване на заявка от страна на клиент могат да бъдат договорени и описани в плана за управление на съответната услуга.

Следните детайли биват попълвани от заявителя при подаването на заявката:

- име на заявителя;
- дата на подаване на заявката;
- дата и час за изпълнение на промяната;
- приоритет;
- категория на промяната;
- тип на промяната;
- повтаряемост на промяната;
- засегната система/приложение;
- описание на промяната;
- детайлно описание на дейностите по извършване на промяната.

На база категорията на промяната се назначава ръководител на промяната в зависимост от определения такъв в матрицата на ролите. Прави се първоначален преглед за точност на

подадената информация в заявката. При необходимост към нея се прикачат планове за тестване, изпълнение и възстановяване в случай на възникване на неочаквано събитие.

В зависимост от въведените детайли ръководителя на промяната потвърждава или променя приоритета на заявката, както и времето за изпълнението й.

Ръководителят на промяната подготвя задачите за изпълнение, които разпределя по-късно по време на фазата на изпълнение.

5.3.2. Фаза на оценяване

Прави се детайлен преглед на информацията, подадена в заявката. Ръководителят потвърждава, че е предоставена достатъчна информация, за да бъде ясно разбрана заявката за промяна от одобряващия промените в следващата фаза на изпълнение.

Ръководителят на промяната, а при необходимост и консултативният съвет по промените, прави оценка на рисковете, влиянието върху бизнеса, критичността и сигурността на предложената промяна.

Ако се налага се извършват тестове на промяната в тестова среда съгласно инструкция LSI431 Работа в тестова среда.

При необходимост от повече информация се търси помощ от съответния функционален експерт или от заявяващия промяната.

След попълването и изчистването на всички детайли по заявката, тя се придвижва за одобрение.

5.3.3. Одобрение на промяната

През тази фаза се осигурява адекватното одобрение на промяната от съответните организационни одобряващи, от ръководителите на проекти (ако промяната е свързана с изпълнението на конкретен проект), от отговорниците за предоставяне на външна услуга и при необходимост, от консултативния съвет по промените.

В зависимост от въведените данни за категория, тип и описание, заявката се насочва към предопределените в матрицата на ролите одобряващи за получаване на одобрение.

Одобряващият промяната преценява дали е необходимо тя да бъде одобрявана от консултативния съвет по промените. Ако е необходимо, заявката се представя за разглеждане на редовната седмична среща. Ако е необходимо незабавно изпълнение се свиква извънредна сесия на съвета.

След одобрение, заявката преминава към фаза на изпълнение. Ако промяната бъде отказана, отказът се документира, съобщава се на заявителя и заявката бива отхвърлена.

5.3.4. Изпълнение на промяната

През тази фаза одобрената заявка за извършване на промяна бива включена в графика за изпълнение. Съобщава се на заявителя за одобрението на заявката му и за планираната дата и час на изпълнение.

Ръководителят на промяната разпределя задачите към изпълнителя/ите на промяната и следи за стриктното им изпълнение.

Ако при изпълнението на промяната се появи необходимост от извършване на допълнителни (донастройващи) действия, ръководителят на промяната решава дали може да се

продължи с изпълнението и да се извършат необходимите дейности или да се пусне нова заявка за промяна, която да премине през фазите на преглед, оценка и одобрение.

Ако изпълнението на промяната води до непредвидими и непланирани действия или състояния, то променената система трябва да може да бъде върната до предишното ѝ състояние.

Изпълнителят на промяната документира всички промени, които извършва в инфраструктурата. Ако е необходимо да се обновяват процедури и политики, внася предложение за промяна на съответната документация.

5.3.5. Затваряне на заявката

Процесът по извършването на промяна приключва след потвърждение от изпълняващия промяната за успешното/неуспешното изпълнение на заявката.

Ръководителят на промяната изготвя доклад за изпълнението и съобщава на заявителя за резултата от извършването на промяната.

Затваря се заявката в системата за управление на промените.

Преглед на резултатите от промяната се извършва на последващата редовна среща на консултативния съвет по промените с цел да се определят успехите, да се дефинират добри практики и да се разграничи наученото от съответната промяна.

5.4. Документиране на промените

Всички дейности, във връзка с изпълнението на заявките за извършване на промяна, се документират в съответната система за управление на промените със съответните изискуеми записи по качеството.

При необходимост се въвеждат необходимите записи за извършените промени в системи, регистри или бази данни.

Всяка изпълнена промяна се добавя към Дневника на промените в горепосочената система за последващи референции към нея.

5.5. Контрол на изпълнението

Оперативният контрол за изпълнението на промените в съответствие с подадената заявка за промяна се осъществява от ръководителя на съответната промяна.

Контролът се извършва чрез:

- проследяване дали заявката за промяна следва дефинирания процес за оценка, съобразен с изискванията на бизнеса;
- гарантиране, че промените следват процеса на одобрение;
- проверка за въвеждане на записи за промените в дневника за промените;
- следене за коректно докладване за статуса на съответната промяна.

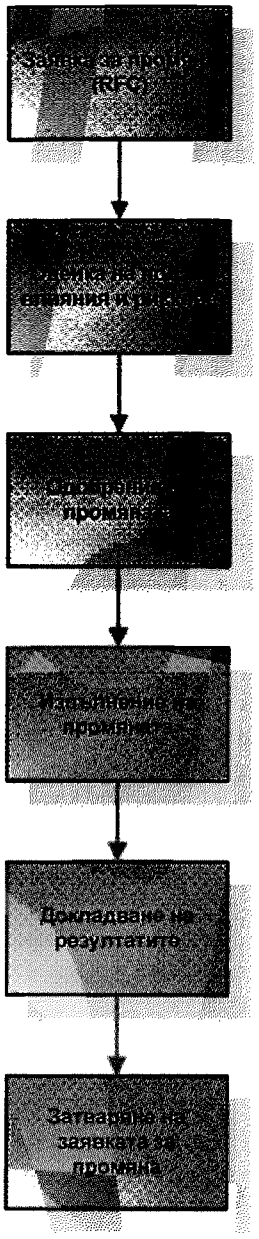
5.6. Управление на риска

Управлението на риска се извършва чрез:

- предварително тестване на промените в тестова среда преди внедряването им в продуктивната среда;
- създаване на планове за възстановяване след кризисни ситуации;
- осъществяване на строг контрол върху извършването на промените от страна на ръководителя на промените.

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

6. Блок схеми



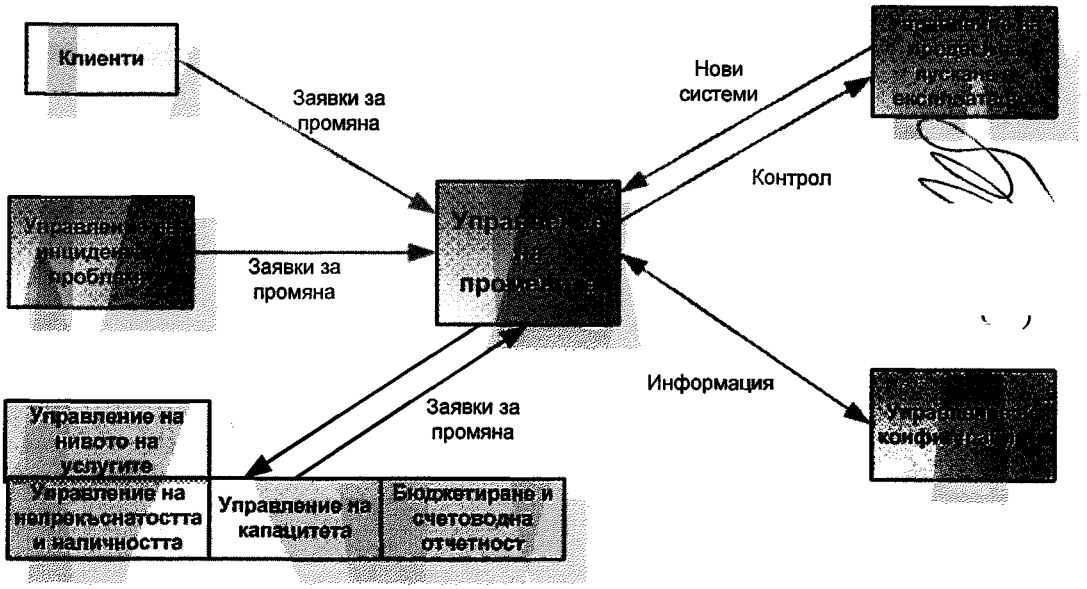
Фиг. 1 Фази на изпълнение на промяна

На следната диаграма са представени връзките на процеса за управление на промените с други процеси за управление:

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

За актуалната редакция и съдържание на процедурата проверете в *LODIS*.

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679



Фиг. 2 Връзки на процеса за управление на промените с други мениджмънт процеси

7. Термини и съкращения

Декларация за приложимост	Документ, описващ целите по контрола и механизмите за контрол, които се отнасят и са приложими към Системата за управление на сигурността на информацията.
Промяна	Всяко добавяне, модифициране или премахване на одобрен или поддържан хардуер, софтуер, мрежа, приложение, система и свързаната с тях документация.
Събитие	Всяко действие, което се случва извън нормалните оперативни процедури и което оказва реално или потенциално влияние върху стабилността и надеждността на инфраструктурата.
Консултативен съвет по промените	Група от специалисти, които могат да дават експертни съвети относно извършването на дадена промяна. Този съвет е съставен от представители от различни области на ИТ управлението и бизнеса. Съвета се свиква по предварително одобрен график или при необходимост от спешно вземане на решение за промяна.

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

Приоритет на промяната	Отнася се за това колко бързо и спешно трябва да бъде разгледана и изпълнена заявката за промяна. Приоритетите се степенуват както следва: (1) критичен, (2) висок, (3) среден, (4) нисък.
Критична промяна	Промяна, която трябва да бъде извършена незабавно и не може да бъде планирана за изпълнение в бъдещ период
Предварително одобрена промяна	Стандартна промяна, която се повтаря във времето и следва определен път.
График за извършване на промени	Списък, съдържащ всички одобрени за изпълнение промени и сроковете/датите за тяхното изпълнение.
Система за управление на качеството и информационната сигурност (СУКИС)	Организационната структура на *ЛИРЕКС.КОМ* в комплекс с регламентирания ред, процесите и ресурсите, необходими за управление качеството и информационната сигурност на предлагани продукти и услуги.
Сигурност на информацията (информационна сигурност)	Запазване на поверителност, цялостност и наличност на информацията.
Лирекс.ком	Дружествата Лирекс БГ, Лирекс БС, Лирекс Хай Тех, Беолик, Лирекс Скопие, Теза

8. Препратки към документи

ID на документа	*наименование на документа*
LPP001	Процедура: Подготовка, прегледи и сключване на договори
LQS Manual	Наръчник по качеството и информационната сигурност
LPP007	Процедура: Управление на конфигурацията

9. Оценки

Не се прилагат измервания.

10. Документирана информация

Записите, свързани с управлението на промените се съдържат в системата за управление на промените.

10.1. Форми и бланки

ID на формата	*наименование на формата*
LSB012-CHR	Заявка за извършване на промяна
LSB012-PCM	Матрица на предварително одобрените промени
LSB012-RMX	Матрица на ролите
LSB012-CHD	Дневник на промените

1. История на редакциите

версия	описание на промяната	автор	проверил	утвърдил	дата на влизане
2	Отстраняване на несъответствия от първия етап на одита по ISO/IEC 20000-1:2005	Б.Йорданов	Б.Янчев	Д.Илиева	15.02.2010
3	Въвеждане на изискванията на ISO/IEC 20000-1:2011	Б.Йораданов	П.Талева	Д.Илиева	17.04.2010
4	Актуализиране на документите от СУКИС	М.Йончева	Б.Янчев	Д.Илиева	05.08.2010

2. Предназначение

Процедурата определя изискванията за реда и начина за управление на Системата за управление на ИТ услугите, доставяни от дружествата Лирекс.ком на други организации или частни лица (външни ИТ услуги) в съответствие с декларираната политика по тяхното управление. Системата за управление на ИТ услугите в съответствие с ISO/IEC 20000-1 е неразделна част от интегрираната СУКИС в дружествата Лирекс.ком.

Процедурата има за цел постигането в максимална степен на изискванията на потребителите – организации или частни лица по отношение на съдържанието и нивото на предоставяните ИТ услуги и на изискванията на приложимите нормативни актове.

3. Приложимост

Процедурата се прилага при изпълнението на външните ИТ услуги, предоставяни от дружествата Лирекс.ком на други организации или частни лица.

Външните ИТ услуги, предоставяни от дружествата Лирекс.ком, са посочени в документ LSB-200-RES (Регистър на външните услуги).

4. Отговорности

4.1. Висше ръководство:

- осигуряват политиката за управление на ИТ услугите да съответства на целите на дружествата Лирекс.ком, да гарантира изпълнението на предоставяните ИТ услуги в съответствие с приложимите законови и други приети или договорени изисквания, да бъде периодично преглеждана за адекватност и актуализирана при необходимост с цел непрекъснато подобряване на дейността;
- осигуряват необходимите и достатъчни ресурси за изпълнение на договорените ИТ услуги;
- съвместно с ръководителите на функционалните звена определят целите по въведения ISO/IEC 20000-1 в СУКИС на дружествата Лирекс.ком;
- разработват стратегията за постигане на целите по ISO/IEC 20000-1 в СУКИС, като осигуряват необходимите кадрови и материални ресурси;
- определят правомощията и отговорностите на служителите за гарантиране, че процесите за управление на ИТ услуги са проектирани, планирани, изпълнявани и подобрявани в съответствие с политик ата и целите за управление на услугите;

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

- ежегодно правят преглед за съответствие на дефинираните цели с декларираните политики по въведеният ISO/IEC 20000-1 в СУКИС;
- съвместно с ръководителите на функционални звена анализират степента на постигане на определените цели по ISO/IEC 20000-1 и ги актуализират в зависимост от пазарните условия, законовите промени и изискванията и очакванията на клиентите.

4.2. Ръководители на функционални звена:

- планират необходимите и достатъчни ресурси за изпълнение на договорените ИТ услуги;
- организират взаимодействието и комуникацията с клиентите във връзка с исканите от тях ИТ услуги;
- организират и координират дейностите във връзка с прегледа на договорите и уточняване на изискванията на клиентите;
- организират документирането на дейностите във връзка с договорените ИТ услуги в съответствие с изискванията на приложимите в процеса процедури по СУКИС;
- гарантират, че активите, включително лицензите, използвани при доставянето на ИТ услугите, се управляват в съответствие с приложимите законови изисквания и други договорени задължения;
- информират служителите за важността на спазването на въведената политика, на изискванията на стандарта ISO/IEC 20000-1 и последствията от тяхното нарушаване, както и необходимостта от непрекъснато им подобряване;
- организират и координират всички дейности във връзка с изпълнение на целите по договорените ИТ услуги, като при необходимост възлагат на друг служител организацията и координацията на конкретна услуга;
- одобряват и утвърждават документите и записите във връзка с изпълнението на договорите за доставка на ИТ услуги;
- периодично отчитат и докладват за състоянието, постигнатите резултати, проблемите и предстоящите задачи по изпълнението на ИТ услугите от ръководените от тях звена;

4.3. Отговорник на ИТ услуга:

- изпълнява дейности съвместно с ръководителя на функционалното звено или по негово нареждане във връзка с прегледа на договора и уточняване на изискванията на клиентите;
- по нареждане от ръководителя на функционалното звено организира и координира дейностите във връзка с изпълнението на договорените ИТ услуги;
- по нареждане от ръководителя на функционалното звено комуникира с клиентите във връзка с исканите от тях обучения;
- отговаря за съставянето, правилното поддържане, съхранение и архивиране на всички записи в процеса на изпълнение на договора за доставка на ИТ услуги на клиента.
- обобщава резултатите от мненията и препоръките на клиентите за предоставяните им ИТ услуги.

4.4. Упълномощен представител на ръководството

- отговаря за координацията и управлението на всички външни ИТ услуги, предоставяни от дружествата Лирекс.ком;

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

- осигурява интегрирането на всички дейности по предоставянето на ИТ услуги във въведената СУКИС в дружествата Лирекс.ком;
- организира и участва съвместно с ръководителите на функционалните звена и отговорниците на услуги в изработването на документирани процедури и планове за управление на предоставяните ИТ услуги
- организира провеждането на Прегледи от ръководството на СУКИС, на които се обсъжда изпълнението на целите по управление на външните ИТ услуги по стандарта ISO/IEC 20000-1, тяхната ефективност, подобряване и приемането на нови цели.

5. Инициране на процеса за доставяне на ИТ услуга

5.1. Общи условия

Инициирането на процеса за доставяне на външни ИТ услуги и тяхното управление започва при:

- постъпило искане от клиент за доставяне на ИТ услуга, включена в Регистъра на външните ИТ услуги (LSB-200-RES);
- решение за участие в тръжна процедура за доставяне на ИТ услуга;

Документиране на постъпилите искания от клиенти се извършва в съответствие с процедура LPP001. В случай на запитване за услуга, която не е включена в Регистъра, решение за нейното разработване се приема от ръководството.

Управлението на процеса за доставяне на външни ИТ услуги се състои в:

- осигуряване на условия за пълно удовлетворяване изискванията на клиента в съответствие със сключения договор за доставяне на исканата ИТ услуга;
- приложението на единните принципи за осигуряване качеството и информационната сигурност на всички етапи от процеса на доставяне на ИТ услугата;
- изпълнение на дейностите, включени в Договора за доставяне на услугата, приложенията към него, споразумението за ниво на съответната услуга, както и свързания с нея План за управление на външната ИТ услуга.
- контрол за изпълнението на дейностите от всеки елемент на процеса в съответствие с изискванията на Договора, Плана за управление на услугата и на общосистемните процедури от СУКИС.

Процесът за управление на външните ИТ услуги, предоставяни от дружествата Лирекс.ком, се подразделя на следните под-процеси:

- подготовка, преглед и сключване на договори с клиенти за доставяне на ИТ услуги;
- доставяне, контрол, отчитане и подобрение на договорените ИТ услуги.

Извършваните дейности във всеки под-процес се определят в зависимост от съдържанието и обема на договорената ИТ услуга, изискванията на клиента, възможностите на дружеството и приложимите нормативни изисквания.

5.2. Подготовка и преглед на договора

Подготовката за прегледа и самия преглед на договора за доставяне на ИТ услуга се осъществява съгласно изискванията на процедура LPP001 „Подготовка, прегледи и сключване на договори" и на настоящата процедура.

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

В процеса на преглед на договора, ръководителят на функционалното звено, предоставящо услугата или определен от него служител изготвя и съгласува с клиента едно или няколко Споразумения за нивото на обслужване (SLA) за всяка конкретна ИТ услуга, като включва тези раздели и изисквания, които са приложими. Споразуменията могат да бъдат описани в отделен самостоятелен документ или да бъдат част от съответния договор за предоставяне на услуги.

Това споразумение може да включва някои или всички от следните елементи:

- кратко описание на услугата;
- период на валидност и/или механизъм за управление на промените в SLA;
- детайли за подобрение;
- кратко описание на комуникацията между заинтересованите страни, включително отчитането на услугата;
- данни за контакт на лица, упълномощени да действат в спешни случаи и да участват при разрешаване на възникнали конфликтни ситуации и проблеми, възстановяване или вземане на временни решения;
- работното време, неработни дни, критични периоди за бизнеса и осигуряване на извънредно работно време;
- планирани и договорени прекъсвания на работата, включително начин за предупреждаване и брой прекъсвания за даден период;
- отговорностите на клиента;
- отговорностите и задълженията на доставчика на услуги;
- насоки за въздействие и приоритет;
- процес за известяване и за поставяне на въпроса на по-високо ръководно ниво;
- процедури за оплаквания;
- цели на услугата;
- норматив за работа (горна и долна граница);
- детайли за финансово управление на високо ниво;
- действие, което се предприема в случай на прекъсване на услугата;
- експлоатационни услуги;
- речник с термини;
- поддържащи и свързани услуги.

Когато за изпълнението на договора за доставка на ИТ услуга е необходимо включването на подизпълнител, то неговият избор, комуникацията с него и периодичното му оценяване се извършват в съответствие с LPP101 „Закупуване на стоки и услуги". В договорите / споразуменията с всеки подизпълнител трябва да се включат необходимите изисквания към обхвата и управлението на дейността, която той предоставя. Споразуменията за нивото на услугата с подизпълнителите трябва да съответстват на SLA към клиентите на съответната доставяна услуга.

Всички уточнявания, споразумения и други условия, постигнати в контактите с клиентите и подизпълнителите в процеса на преглед на договора, се документират по подходящ начин и включват в Договор (съответно в приложенията към него и Споразуменията за нивата на обслужване). Организацията на документирането се създава от ръководителя на звеното или отговорника за услугата, който изпраща копие от съответните документи (в електронен или хартиен вид) на клиента и на евентуалните подизпълнители.

5.3. Заключителни дейности по прегледа и сключването на договора

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

Заключителните дейности по прегледа и сключване на Договора за доставяне на ИТ услуга се извършват в съответствие с процедура LPP001.

Договори от името на дружеството-доставчик се подписват от неговия управител. Одобреният от двете страни договор/споразумение с писменото удостоверяване от двете страни е свидетелство за приключване на процеса за преглед на договора и основание за иницииране на изпълнението му.

6. Изпълнение на договорените ИТ услуги

6.1. Общи условия

Изпълнението на договорените ИТ услуги, включени в Регистъра на външните услуги (LSB-200-RES), се осъществява в съответствие с изискванията на съответния договор, приложенията към него и SLA; плана за управление на услугата и на приложимите общосистемни процедури от СУКИС. Това включва дейности, свързани с:

- управление на човешките, техническите и информационните ресурси;
- определяне на отговорностите и ролите в процеса;
- разпределение и управление на определения бюджет;
- идентифицирането, оценката и управлението на рисковете за услугите;
- управление на процесите за управление на услуги;
- контрола и отчитането на дейностите по управление на услугите.

Организацията и координацията на всички дейности във връзка с изпълнение на договора за услуги се осъществява от ръководителя на съответното звено. За специализираните ИТ услуги, обвързани с лицензионни права или с други валидни договорни отношения с организации, носители на правата за тези услуги, той организира тези услуги в съответствие с договореностите с лицензодателите.

За документиране на дейностите отговорят длъжностните лица, реализиращи дейностите и отговорника за съответната услуга.

След сключване на договора за доставяне на определена ИТ услуга, ръководителят на функционалното звено, предоставящо тази услуга или определен от него служител подготвя План за управление на външната ИТ услуга. При планирането трябва да се отчитат политиката за управление на услугата, изискванията към конкретната ИТ услуга и на стандарта ISO / IEC 20000-1. Планът за управление на услугите трябва да съдържа или да включва препратки към:

- обхвата на предоставяната от доставчика ИТ услуга към клиента;
- изискванията, които трябва да бъдат постигнати от доставчика чрез управление на услугата, вкл. SLA;
- известните ограничения, които може да повлияят на доставяната ИТ услуга;
- задълженията, свързани с приложимите за съответната ИТ услуга политика, законовите и подзаконови изисквания, както и другите договорени задължения;
- рамката на правомощията, отговорностите и ропите в процеса на доставка на услугата;
- правомощията и отговорностите за плановете и процесите на управление и доставка на ИТ услугата;
- човешките, технически, информационни и финансови ресурси, необходими за постигане на поставените цели;

- взаимодействието с другите страни, участващи в проектирането и приемането на нови или променени услуги;
- взаимодействието между процесите на управление на ИТ услугата и тяхната интеграция с другите компоненти на системата на управление;
- подхода, който трябва да се избере при определяне, оценката, критериите за приемане и управление на рисковете за предоставяните ИТ услуги. Оценката се прави количествено в съответствие с процедура LSP200 „Управление на риска" или качествено по показатели, посочени за всяка услуга в съответния План за нейното управление;
- технологията, използвана при предоставянето на ИТ услугите;
- как ефективността на системата за управление на услугите и доставката на услугите се измерва, одитира, отчита и подобрява.

Модел на Плана за управление на външната ИТ услуга е показан в документ LPN002. Неговото конкретно съдържание зависи от спецификата на съответната ИТ услуга и условията на договора, приложенията към него, SLA, изисквания на клиента и др. При необходимост могат да се разработят отделни планове за управление на различните под-процеси при предоставянето на услуги, но те трябва да са в съответствие с Плана за управление на външната ИТ услуга.

Плановете за управление на външните ИТ услуги се преглеждат ежегодно и при необходимост се ревизират. При всяка съгласувана между страните промяна на условията по доставка на услугата, отразена в договора, приложенията към него, анекси, SLA и др., се съставя и одобрява нова редакция на Плана за управление на съответната услуга.

Планът за управление на външната ИТ услуга се изготвя и поддържа в електронен вид или на хартия.

Изготвените и утвърдени Планове за доставка на ИТ услуги са предназначени да организират работата на доставчика на ИТ услуга и не се предоставят на клиентите.

6.2. Внедряване и изпълнение на ИТ услугите към клиенти

Дружествата Лирекс.ком изпълняват ИТ услугите в съответствие с плановете им за управление в рамките на въведената Система за управление на услугите чрез дейности по:

- разпределението и управлението на бюджетите за тях;
- определяне на отговорностите и ролите в процеса;
- управление на човешките, техническите и информационните ресурси;
- идентифициране, оценка и управление на рисковете на услугите;
- наблюдение и докладване за изпълнението на дейностите по доставяне на услугите.

За всяка договорена ИТ услуга се планират и осигуряват необходимите и достатъчни ресурси за нейното изпълнение. Видовете ресурси и техния обем се конкретизират в съответния План за управление на услугата. Тези ресурси включват:

- **Персонал** – определят се необходимия брой служители и тяхната компетентност за изпълнение на съответната ИТ услуга. При необходимост се планират и провеждат обучения и се оценява тяхната ефективност в съответствие с процедура LRP001 „Квалификация и обучение" или се наемат нови служители в съответствие с процедура LRP002 „Набиране и подбор на персонал";
- **Хардуер** – определят се необходимите хардуерни ресурси по спецификация, обем, натоварване и др. Този хардуер е включен в Регистъра на информационните активи;

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

- **Софтуер** - определят се необходимите софтуерни ресурси по спецификация, права за използване, лицензии и др. Този софтуер е включен в Регистъра на информационните активи;
- **Финансови ресурси** – включват необходимите разходи за предоставяне на ИТ услуги. Определянето на необходимите финансови ресурси (бюджетиране на услугата) се извършва в съответствие с инструкция LPI005 "Бюджетиране и отчетност на външни ИТ услуги". При необходимост и когато бизнес условията изискват това, изготвените бюджети служат за основа при разясняването на клиентите на принципите на бюджетиране, съгласуването на съответните споразумения за нива на услугите и подготовка на договорите за тяхното предоставяне.
- **Ресурси на клиента** – зависят от вида на предоставяната услуга и включват документи, хардуер, софтуер или др. При необходимост от такива ресурси, те се описват в Плана за управление на съответната услуга и се управляват в съответствие с условията на договора с клиента.

7. Наблюдение и отчитане на ИТ услугите

Отговорниците на конкретната ИТ услуга извършват текущ контрол при нейното изпълнение и при отклонение на нормалната дейност предприемат незабавни мерки и при необходимост уведомяват ръководителя на съответното звено.

Вътрешен одит на доставчиците на ИТ услуги се планира и провежда в съответствие с процедурата LAP002 „Организация на вътрешния контрол (одити)" от СУКИС. При тези одити се оценява изпълнението на изискванията на стандарта ISO/IEC 20000-1, изпълнението на изискванията към съответната ИТ услуга и нейната ефективност и ефикасност. Констатираните несъответствия се регистрират и управляват в съответствие с процедурата LAP003 „Коригиращи и превантивни действия".

Отчети за предоставяните ИТ услуги се докладват на Прегледите от ръководството на СУКИС. Тези отчети съдържат:

- постигнати резултати при предоставянето на услугите спрямо заложените стойности на SLA;
- несъответствия при доставянето на услугата, например пробив на сигурността;
- характеристики за работното натоварване, например обем, оползотворяване на ресурсите и др.;
- докладване за работа след значими събития, например съществени инциденти и промени;
- информация за финансовите резултати – сравнение с планирания бюджет, причини за преразход (ако има);
- обратна връзка от клиентите;
- направени разходи спрямо планираните финансови ресурси;
- рисковете;
- настоящи и прогнозните човешки, технически, информация и финансови ресурси;
- текущите и прогнозните човешки и технически възможности.

Прегледите от ръководството на СУКИС се провеждат и документират в съответствие с изискванията на процедура LMP003 от СУКИС. На тези прегледи се прави оценка на изпълнението на предоставяните ИТ услуги към клиентите по отношение на приетите цели, на възможностите за

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

подобрение и необходимостта от промени на системата за управление на ИТ услугите, включително на политиката и целите. Входната информация за Прегледите трябва да включва:

- Обратна връзка от клиентите;
- Изпълнението и съответствието на услугите и процесите;
- Настоящи и прогнозни човешки, технически, информационни и финансови ресурси;
- Текущият и прогнозен човешки и технически капацитет;
- Рискове;
- Резултати и последващи действия от проведените одити;
- Резултати и последващи действия от предишни Прегледи от ръководството;
- Състояние на превантивните и коригиращите действия;
- Промени, които биха могли да повлияят на Системата за управление на услугите и на самите услугите;
- Възможностите за подобрения.

Оценка за ефикасността и ефективността на предоставяните ИТ услуги се прави от ръководителите на съответните функционалните звена на база на изпълнението на изискванията, отразени в договорите за съответните ИТ услуги, споразуменията за тяхното ниво и плановете им за управление, както и на изразходваните финансови ресурси за изпълнението им.

Констатираните на Прегледа несъответствия при доставянето на ИТ услуги се обсъждат и при необходимост се предприемат коригиращи действия в съответствие с процедурата LAP003. За решенията и коригиращите действия, приети на Прегледа от ръководството, отнасящи се до клиентите на ИТ услугите и до външните доставчици за тях, те се информират от отговорника за съответната услуга.

При прекратяване на предоставянето на конкретна ИТ услуга, ръководителите на звената или определените от тях отговорници на услугите, изготвят отчет за изразходваните ресурси по време на изпълнението на услугата. Изготвените отчети се представят на Прегледа от ръководството.

В зависимост от идентифицираните тенденции и организационни планове за развитие и бизнес климата в ИТ бранша, на Прегледите от ръководството се обсъжда формирането, актуализирането и разглеждането на базовите ресурси по реализиране на ИТ услугите.

Отчети за доставяните ИТ услуги се предоставят на клиентите съгласно условията на съответния договор, но не по-рядко от веднъж годишно. Конкретната периодичност е посочена в Плана за управление на съответната ИТ услуга.

7.1. Поддържане и подобряване на доставяните ИТ услуги

Ръководството на Лирекс.ком поддържа политика на непрекъснато подобряване на предоставяните IT услуги на клиентите, като:

- Събира и анализира данните за ИТ услугите към клиентите и управлява процесите по тяхното предоставяне;
- Установява цели за подобрение в качеството, разходите и използването на ресурсите за тези услуги;
- Консултира се с заинтересованите страни;
- Преглежда политиките по управление на услугите, процесите, процедурите и плановете;

- Оценява възможностите за подобрение на предоставяните ИТ услуги на базата на постигнатите резултати, степента на удовлетвореност на клиентите, прилагането на доказани добри практики и очакваната ефективност и ефикасност от подобренията.
- Взема предвид наличната информация за подобрения във всички процеси в организацията;
- Осигурява необходимите ресурси за извършване на приетите и планирани подобрения;
- Гарантира, че всички одобрени дейности се извършват с цел подобрения на услугите;
- Измерва, докладва и комуникира подобренията на ИТ услугите.

Ръководителите на функционалните звена на база оценката на възможните подобрения за изпълнение на изискванията, отразени в договорите за съответните ИТ услуги, констатираните несъответствия при проведените одити, рекламации от клиенти, предложенията на клиентите и на тенденциите за развитие на такива услуги изготвят План за управление на подобренията, който включва вида на подобренията и необходимите за това ресурси: човешки (нови хора, обучение и т.н.); нов хардуер, софтуер, разработване на нова ИТ услуга и др. и сроковете за изпълнението им. Подобренията в него са приоритизирани на основата на резултатите от изпълнението на услугите, предложенията на клиентите, на тенденциите за развитие и възможностите за изпълнението им.

Плановете за управление на подобренията може да бъдат оформени като самостоятелен документ или се включват в отчетите за съответната ИТ услуга.

Дружествата Лирекс.ком като доставчици на ИТ услуги изпълняват дейностите по изпълнение на подобренията, които включват:

- Определяне на цели за подобрения в една или повече направления като качество, себестойност, цена, производителност на ресурсите;
- Гарантиране, че одобрените подобрения; се прилагат;
- Преглед на политиките, плановете, процесите и процедурите за управление на услугите;
- Измерване на реализираните подобрения спрямо определените цели и когато целите не са постигнати, се предприемат необходимите действия;
- Отчитане на реализирани подобрения.

8. Планиране и въвеждане на нови или променени ИТ услуги

8.1. Общи изисквания

Процесът се инициира при нови ИТ услуги или при промени в съществуващите, които могат да имат голямо въздействие върху тях. Промяна в ИТ услугите се инициира по предложение на клиента, от доставчика на услугата или по решение от Прегледа на ръководството.

Разработването на нова ИТ услуга, предназначена за доставяне на външни клиенти, се извършват в съответствие с процедура LPP006 „Управление на програми и проекти". Оценяването, одобрението, планирането и прегледът на нови или променените услуги се извършва в съответствие с процедура LPP012 „Управление на промените". За решението за одобрение или отхвърляне на предложението за промяна се уведомяват неговите заявители. Ако това засяга промени в конфигурацията, свързана услугите, тя се управлява в съответствие с процедурата LPP007 „Управление на конфигурацията".

Резултатът от дейностите по планиране и проектиране на нови или променени ИТ услуги трябва да съответства на договорените изисквания за тези услуги и да се осигури ефективност на процеса.

8.2. Планиране на нови или променени ИТ услуги

При планирането трябва да се отчитат политиката за управление на ИТ услугите, изискванията към конкретната услуга и на стандарта ISO / IEC 20000-1. При планирането на услугите трябва да се има предвид:

- Правата и отговорностите за дейностите по проектиране, разработване и въвеждането на нови или променени ИТ услуги;
- Дейностите, които трябва да се извършат от доставчика на услугата, клиентите и другите страни за доставката на нова или променена услуга;
- Комуникацията със заинтересованите страни;
- Необходимите човешки, технически, информационни и финансови ресурси;
- Сроковете за планираните дейности;
- Идентифициране, оценка и управление на рисковете;
- Зависимостите от други услуги;
- Изпитванията, които се изискват за нови или променени услуги;
- Критериите за приемане на услуги;
- Очакваните измерими резултати от предоставянето на нови или променени ИТ услуги.

За ИТ услуги, които трябва да бъдат прекратени, доставчикът на услугата трябва да планира за отстраняването й. Планирането включва датата за прекратяване, архивирането, унищожаването или трансфера на данните, документацията и другите й компоненти. Компонентите на услугите може да включват инфраструктура и приложения със съответните лицензи.

Доставчикът на услуги трябва да идентифицира и другите страни, които може да бъдат ангажирани за предоставянето на компоненти за новите или променени услуги. Доставчикът на услуги трябва да се оцени техните възможности да отговорят на изискванията към конкретните услуги. Резултатите от оценката се регистрират.

8.3. Проектиране и разработване на нови или променени ИТ услуги

При проектирането и разработването трябва да се има предвид:

- Правата и отговорностите за дейностите по доставянето на нови или променени ИТ услуги;
- Дейностите, които трябва да се извършват от доставчика на услугата, клиента и другите страни при доставянето на нови или променени услуги;
- Изискванията за нов персонал или промени в него, включително изискванията за подходящо образование, обучение, умения и опит;
- Изискванията за финансови ресурси за доставка на нови или променени ИТ услуги;
- Необходимите нови технологии или промени в тях за осигуряване на новите или променените услуги;
- Нови планове и политики или промени в тях в съответствие със стандарта ISO / IEC 20000-1;
- Нови договори или други документирани споразумения или промени в тях, за да се приведат в съответствие с промените в експлоатационните изисквания за ИТ услугите;

- Необходимите промени в Системата за управление на ИТ услугите;
- Нови или променени Споразумения за нивото на услугите (SLA's);
- Актуализация на каталога на услугите;
- Промени в процедурите и другите документи, които ще бъдат използвани за доставка на нови или променени ИТ услуги.

Доставчикът на услугата трябва да осигури проектирането на новите или променени услуги да изпълнява изпълнение на тези услуги в съответствие с изискванията към тях.

8.4. Приемане на нови или променени услуги

В случая на одобрение на предложението за промяна на доставяната услуга, в зависимост от вида на промяната, определен за това служител съставя План за изпълнение и въвеждане на промяната. Планът включва дейностите и отговорностите, включително тези и на клиента и (при наличие) на външни доставчици / поддоставчици, комуникацията с тях, необходимите ресурси (материални и човешки, вкл. необходими обучения и квалификации), сроковете за изпълнение, критериите за приемане на промените и очакваните конкретни резултати след въвеждане на промяната, както и промените в документацията и договорните споразумения с клиента (вкл. SLA). Предварителни тестове се извършват в тестова среда съгласно изискванията на инструкция LSI431„Работа в тестова среда".

След изпълнение на планираните дейности по промяна на услугата, заинтересованите страни (клиент и външни доставчици – ако има) се уведомяват за резултатите и за произтичащите от това промени в договорните условия (вкл. SLA). След тяхното съгласуване и приемане, промяната на доставяната ИТ услуга се въвежда в конкретната работна среда, включва се в LSB-200-RES "Регистър на външните ИТ услуги" и се доставя на клиентите по реда на настоящата процедура.

За новата или променена ИТ услуга се изготвя и утвърждава нов или нова редакция на Плана за нейното управление.

8.5. Управление на конфигурацията на ИТ услугите

Управлението на конфигурацията при доставянето на ИТ услуги се извършва в съответствие с процедурата LPP007 "Управление на конфигурацията". Конфигурацията на всяка ИТ услуга включва всички материални ресурси като софтуер и свързаната с него системна документация; хардуер; компоненти за сигурност, например защитни стени; документацията, свързана с услугата, например SLAs, договори, процедури, както и поддържащите ИТ услугата съоръжения. Конфигурацията за всяка ИТ услуга се идентифицира в нейния План за управление. Той може да бъде самостоятелен документ или да бъде включен в Плана за управление на съответната услуга.

Елементите на конфигурацията на трябва да бъдат идентифицирани и включени в база данни (CMDB), която съдържа (ако е приложимо):

- Описание на елемента на конфигурацията;
- Връзките на елемента с другите елементи от конфигурацията;
- Връзките на елемента на конфигурацията с компонентите на услугата;
- Състоянието на елемента;
- Версията;
- Местоположението;
- Свързаните с елемента на конфигурацията искания за промяна;
- Свързаните с елемента на конфигурацията проблеми.

Базата данни на елементите на конфигурацията (CMDB) се поддържа актуална и промените в нея се контролират. Тя се проверява най-малко веднъж годишно и при установени несъответствия се предприемат необходимите действия, които се регистрират.За да се осигури целостта на системите, свързани с доставяните ИТ услуги, информацията за елементите на конфигурацията се съхранява в подходяща и сигурна среда, която да ги защитава от неоторизиран достъп, промяна или подправяне. Това включва документация, лицензна информация, софтуер и, когато е възможно, изображения на хардуерната конфигурация.

Всяка промяна в конфигурациите, свързана с предоставяните ИТ услуги (нова версия на услугата), се извършва в съответствие с процедура LPP012 "Управление на промените". Информацията от Базата данни на елементите на конфигурацията се използва при оценка на исканията за промени в услугите.

8.6. Управление на непрекъсваемостта и наличността на ИТ услугите

Изискванията за непрекъснатост и наличност на услугата се определят на основата на договора за услугата и споразуменията за тяхното ниво и в съответствие с процедура LSP900 „Непрекъсваемост на бизнес процесите". Изискванията трябва да включват права за достъп и време за реакция, а също така и непрекъснатото наличие на услугата.

Плановете за непрекъснатост и наличност на услугата се преглеждат поне веднъж годишно, за да се осигури спазване на изискванията при всички обстоятелства – от нормална работа до значителни прекъсвания на услугата. Плановете за непрекъснатост и наличност се изпитват отново при всяка значителна промяна на бизнес средата.

Достъпността на ИТ услугата се измерва и записва. При непланирана недостъпност на услугата (инцидент) се предприемат подходящи действия. Плановете за непрекъснатост на услугата, списъкът с лица за контакти и базата данни за управление на конфигурациите трябва да бъдат достъпни, когато нормалният достъп до офиса на доставчика на услугата е възпрепятстван. Планът за непрекъснатост на услугата трябва да включва начина за връщане към нормална работа.

Всички изпитвания за непрекъснатост трябва да бъдат записани, а неуспешните резултати от изпитвания трябва да се опишат в плановете за действие.

За осигуряване на договореното ниво на ИТ услугите се определят методи за планиране и наблюдение на капацитета на всяка услуга. Управлението на капацитета се прави в съответствие с процедура LSP702 „Планиране на капацитета".

9. Комуникация при доставяне на ИТ услуги

9.1. Заинтересовани страни при предоставянето на ИТ услуги

Заинтересованите страни при доставянето на ИТ услуги са техните доставчици, клиентите им и подизпълнителите/поддоставчиците (ако има такива). Подизпълнителите при доставката на ИТ услуги са вътрешни (от дружествата Лирекс.ком) и външни.

Дейността с вътрешните поддоставчици се осъществява и контролира в съответствие с процесите, въведени в интегрираната СУКИС.

За успешно изпълнение на договорените ИТ услуги, доставчикът сключва договори с външните поддоставчици. Тези договори трябва да съдържат или да включват позоваване на:

- Обхвата на услугите, които трябва да бъдат доставени;
- Зависимостите между услугите, процесите и страните по договора;

- Изискванията, които трябва да бъдат изпълнени от доставчика;
- Нивата на доставяните услуги;
- Взаимодействието между процесите за управление на услугите на страните по договора;
- Интегриране на дейностите на доставчика в рамките на Системата за управление на ИТ услугите; които трябва да бъдат доставени;
- Характеристики на работното натоварване;
- Договорените изключения и как те ще бъдат управлявани;
- Правомощията и отговорностите на страните по договора;
- Отчетността от доставчика и комуникацията с него;
- Условията за плащане;
- Дейностите и отговорностите при очаквано или предсрочно прекратяване на договора и прехвърлянето на задълженията по него към други страни.

За успешна комуникация с клиентите и външните поддоставчици, доставчикът на ИТ услугата поддържа база с данни с информация за тях и техни представители, оторизирани за оперативен контакт по време на доставка на услугата (име, адрес, телефон, електронна поща и др.). Тези данни се включват в Плана за управление на съответната ИТ услуга. Освен основният поддоставчик, който осигурява текущата доставка на съответната услуга, в Плана се включват и данни за резервен поддоставчик/ци, към които доставчикът на ИТ услуга се обръща, когато основният поддоставчик не може да изпълнява своите функции по договора.

Ежегодно, на съвместна среща с клиентите, се прави преглед на предоставяните им ИТ услуги съгласно сключените договори и споразуменията към тях (включително SLA), за да се гарантира, че техните потребности и задълженията по договорите се изпълняват. Прегледите се документират. При необходимост се правят съгласувани промени в услугите, които се въвеждат съгласно процедура LPP012 "Управление на промените". При необходимост се провеждат междинни срещи с клиентите за обсъждане на параметрите на доставяната услуга, като срещите се документират.

Изискванията към външните поддоставчици и тяхната периодично оценяване са определени в процедурата LPP101 "Закупуване на стоки и услуги".

9.2. Уреждане на рекламации

Подаване на рекламации от клиента става по установените канали за комуникация с клиентите или по реда на процедура LAP001 „Измерване степента на удовлетвореност на клиентите".

Обработка на получената рекламация става по начина, посочен в процедурата LAP003 „Коригиращи и превантивни действия". За предприетите действия по рекламацията клиентът се информира от УПР. Неуредените рекламации се ескалират към по-високо управленско ниво, ако проблемите не са разрешени в сроковете, уговорени с клиента.

Анализ на получените рекламации за ИТ услуги се представя на Прегледите от Ръководството на СУКИС. Резултатите от такива анализи, когато е подходящо, се използват за представяне на информация за подобряване на услугата.

Когато клиентът не е доволен от уреждането на неговата рекламация или има спор по изпълнението на договора за доставка на ИТ услугата, както и за всички въпроси, неуредени в този договор, се прилага българското гражданско и търговско право, като страните уреждат

отношенията си чрез споразумение. При непостигане на съгласие спорът се отнася за решаване пред компетентния съд.

9.3. Управление на инциденти и проблеми

Управление на инциденти и проблеми при доставката на ИТ услуги се извършва в съответствие с процедурата LSP800 „Управление на инциденти и проблеми".

Информация за инцидент се получава от системата за наблюдение на доставяната услуга, от клиентите по установените канали за комуникация или по начина, посочен в процедурата LSP420 „Service Desk". В процедурата е посочен начина на записване, задаване на приоритет, класифициране, обновяване, придвижване по йерархията, окончателно решение и официално приключване на всички инциденти.

Клиентът на ИТ услугата се информира от отговорника на съответната услуга или от отговорника на съответното звено за напредъка на докладвания от него инцидент или заявка за услуга и се предупреждава предварително, ако нивото на услугата не може да бъде постигнато.

Идентифицираните проблеми се записват. За промените, необходими за коригиране на основната причина на проблемите, трябва да бъде подадена информация към процеса за управление на промените. Ефикасността на решаването на проблем трябва се наблюдава, преглежда и отчита от ръководителя на звеното или от отговорника на услугата и се включва в периодичния отчет за нея. Набелязаните действия за подобрения по време на този процес трябва да бъдат записани и включени като входни елементи в плана за подобряване на услугата.

Информацията, свързана с известните грешки, решения на проблеми и базата данни за управление на конфигурациите е достъпна за целият персонал, включен в управлението на инциденти.

10. Управление на сигурността на информацията, свързана с ИТ услугите

Сигурността на информацията, свързана с предоставяните на клиентите ИТ услуги, се осигурява от процедурите и инструкциите на въведената Система за управление на качеството и информационната сигурност (СУКИС).

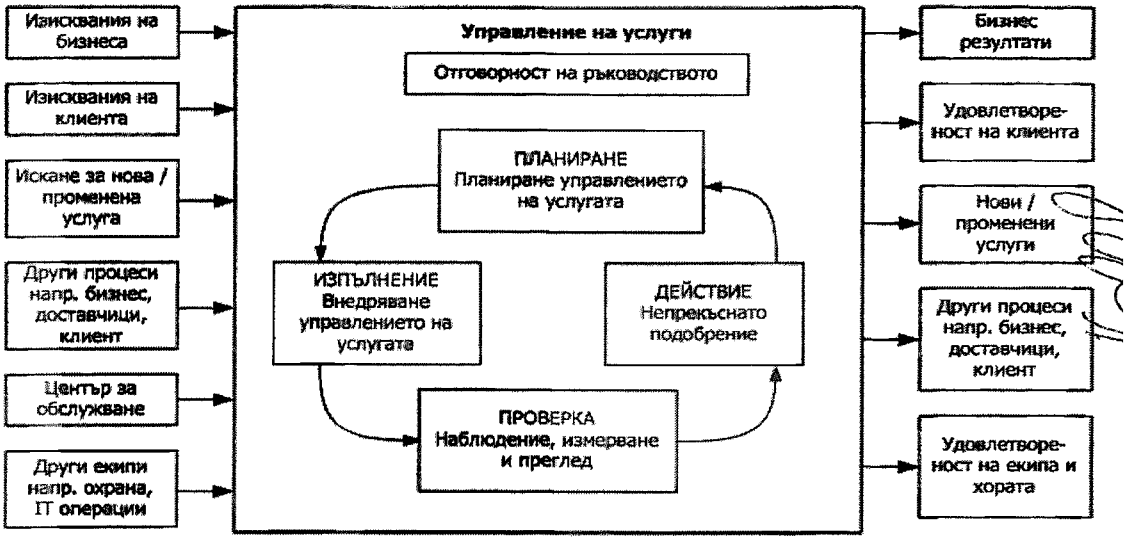
Информацията, свързана с личните данни и търговската дейност на клиентите и на поддоставчиците се събира и използва само във връзка с пълното и точно изпълнение на договорите за доставка на ИТ услуги, осигуряване на договорените SLA и на необходимото качество на обслужването.

Цялата информация, свързана с предоставяните на клиентите ИТ услуги, в зависимост от вида на носителя (в електронен вид или хартиен носител), се съхранява на определените за това места (на вътрешни електронни системи или в шкафове) и достъп до нея имат само ръководителят на звеното, доставящо услугата и служителите, участващи в нейното изпълнение. Достъпът на трети лица до тази информация се предоставя само при законови основания за това или при влезли в сила съдебни решения.

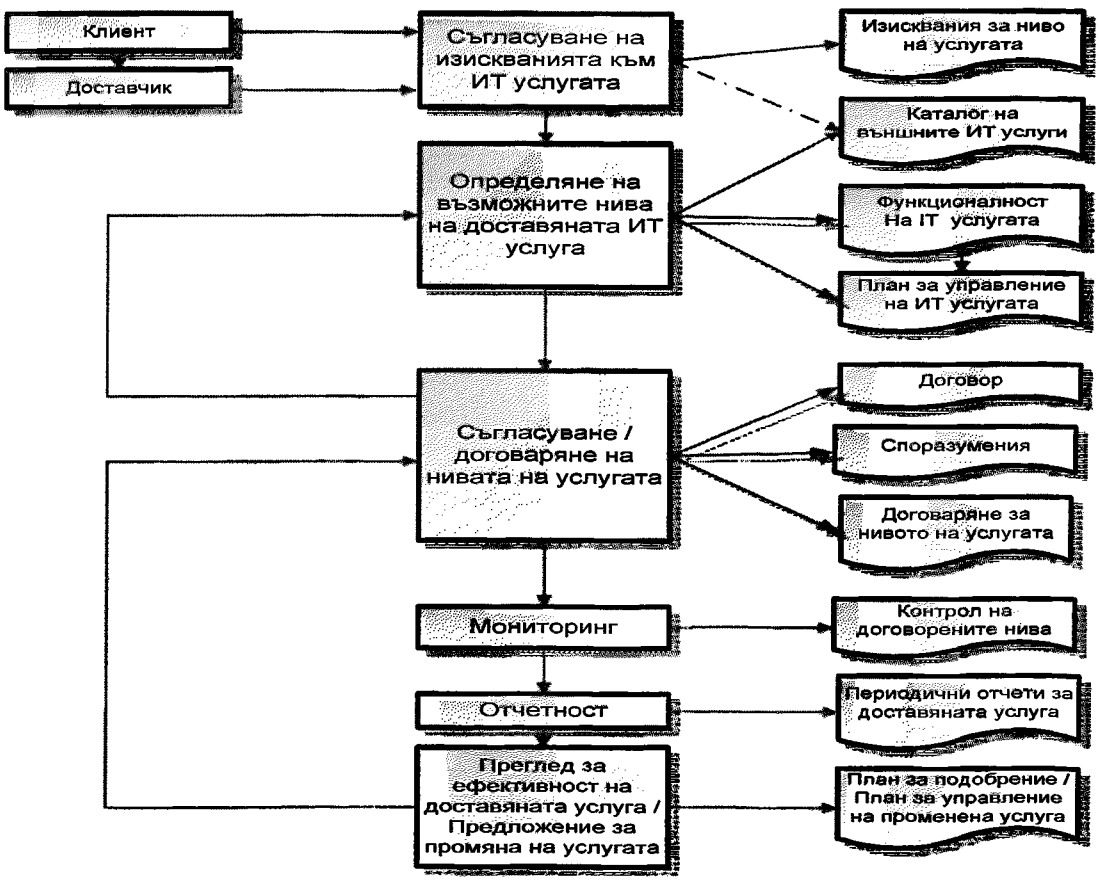
Унищожаване на излезли от употреба носители на информация, свързана с предоставяни ИТ услуги на клиенти, се унищожава по процедура LSP472 „Унищожаване на информация".

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

11. Блок схеми



Фигура 1



Фигура 2

За актуалната редакция и съдържание на процедурата проверете в *LODIS*.

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

12. Термини и съкращения

ИТ услуги	Услуги в областта на информационните технологии
Външни ИТ услуги	ИТ услуги, предоставяни от дружествата Лирекс.ком на други организации или частни лица
Клиент/Потребител	Юридическо или физическо лице, с което доставчикът сключва или има сключен договор или друго споразумение за доставяне на услуги
Доставчик	Дружеството, с което клиентът сключва или има сключен договор или друго споразумение за доставяне на услуги
Подизпълнител/ Поддоставчик	Юридическо или физическо лице, с което доставчикът има действащ договор или друго споразумение за изпълняване на отделни дейности от процеса на доставяне на услуги
Договор/ Споразумение	Документирана договореност за доставяне на услуги от доставчик на клиент, с точно определени изисквания, потвърдени от двете страни.
Преглед на договора	Дейности преди подписване на договора за удостоверяване, че всички изисквания на клиента са точно и еднозначно определени, документирани са и могат да се изпълнят.
Ръководител на функционално звено	Служител, в чиито правомощия и отговорности е правото да организира и управлява доставянето на ИТ услуги от ръководеното от него звено.
Отговорник на ИТ услуга	Служител, на когото е възложено да организира изпълнението на определена ИТ услуга
Споразумение/договор за ниво на обслужване - Service level agreement (SLA)	Самостоятелен документ или част от договора за доставка на ИТ услуга, който определя критериите за минимално допустими нива на обслужване
СУКИС	Система за управление на качеството и информационната сигурност
Лирекс.ком	Дружествата Лирекс БГ, Лирекс БС, Лирекс Хай Тех, Беолик, Лирекс Скопие, Теза

13. Препратки към документи

За актуалната редакция и съдържание на процедурата проверете в *LODIS*.

ID на документа	наименование на документа
LPP001	Подготовка, прегледи и сключване на договори
LMP003	Преглед на СУКИС от Ръководството
LSB-200-RES	Регистър на външните ИТ услуги
LSP200	Управление на риска
LPP501	Управление на Интернет услуги и продукти
LPP601	Организация и управление на сервизната дейност
LRP001	Квалификация и обучение
LRP002	Набиране и подбор на персонал
LPP101	Закупуване на стоки и услуги.
LPN002	План външна ИТ услуга
LPP007	Управление на конфигурацията
LAP002	Организация на вътрешния контрол (одити)
LAP003	Коригиращи и превантивни действия
LSP701	Управление на пускане в действие
LSP702	Планиране на капацитета
LSP900	Непрекъсваемост на бизнес процесите
LSP800	Управление на инциденти и проблеми
LSP420	Service Desk

14. Документирана информация

Документите и записите, свързани с предоставянето на ИТ се създават, утвърждават, съхраняват и унищожават съгласно въведената в Лирекс.ком Система за управление на качеството и информационната сигурност (СУКИС) в съответствие със стандартите ИСО 9001, ISO/IEC 27001 и ISO/IEC 20000-1.

Информацията, свързана с личните данни и търговската дейност на клиентите се събира и използва само във връзка с точното и навременно изпълнение на предоставяните им ИТ услугите и осигуряване на необходимото качество на обслужването.

14.1. Форми и бланки

ID на формата	*наименование на формата*
LPN002	План за управление за външна ИТ услуга

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

ЛИРЕКС.КОМ	Процедура: Организация и управление на мрежово сервизно обслужване (Cisco Support)	Версия 4
	LPP301	1 от 11

1. История на редакциите

версия	описание на промяната	автор	проверил	утвърдил	дата въвеждане
2	Въвеждане на изискванията на ISO/IEC 27001:2005	Пл. Петрова	Вл.Стоев	Д.Илиева	10.02.2009
3	Въвеждане на изискванията на ISO/IEC 20000-1:2005	Б.Йорданов	Вл.Стоев	Д.Илиева	06.04.2010
4	Актуализиране на документите от СУКИС	М.Йончева	Б.Корчев	Д.Илиева	16.08.2019

2. Предназначение

Процедурата определя общата схема за организация и управление на процесите за реализация на мрежово сервизно обслужване в *Лирекс.ком, звено Телекомуникационни услуги.*

3. Приложимост

Регламентираните в процедурата процеси и схемата за тяхната организация (взаимодействие, управление) са приложими при изпълнение на гаранционен и извънгаранционен сервиз на продукти и технологии. Изключения се допускат в случаите на специфични изисквания за управление на проекти, по регламентирания в процедури *LPP006* и *LPP013*.

Процедурата е задължителна за изпълнение от служителите на *Лирекс.ком*, които осъществяват сервизно поддържане на мрежови решения.

4. Отговорности

4.1. Управителят

- осигурява необходимите ресурси за реализация на мрежово сервизно обслужване;
- ангажира всички възможни фирмени ресурси за решаване на мрежови проблеми на клиентите;
- непосредствено контролира изпълнението на задължения за сервизно обслужване по важни проекти, към важни клиенти и по съществени за бизнес процесите на клиенти мрежови проблеми.

4.2. Ръководителят на звено Телекомуникационни услуги

- организира и контролира цялостната дейност за мрежово сервизно обслужване;
- докладва на прегледите на Ръководството за извършваното сервизно обслужване и възникналите проблеми;
- определя изпълняващия длъжността *администратор на* СЦ - ТКУ;
- планира обучението и повишаването на квалификацията на сервизните специалисти;
- прави предложения за превантивни и коригиращи действия относно мрежовото сервизно обслужване.

4.3. Изпълняващият длъжността *администратор на* СЦ - ТКУ

- оперативно ръководи дейността за сервизно поддържане на мрежови решения;

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

- контролира своевременното и качествено решаване на регистрирани сервизни случаи;
- организира и участва в регламентирания ескалационен процес;
- организира и ръководи сервизния склад за мрежово оборудване;
- контролира своевременната замяна на дефектирало оборудване по RMA процедура;
- прави предложения за допълнителни ресурси, необходими за реализация на мрежово сервизно поддържане;
- прави предложения за превантивни и коригиращи действия относно мрежовото сервизно обслужване.
- регистрира и води на отчет резервни части (устройства, модули, компоненти) за сервизно поддържане;
- организира и участва в дейностите за приложението на RMA процедурата за замяна на дефектирало оборудване;
- поддържа в актуално състояние регистрите за отчет и контрол на движението на резервни части и заменяно оборудване по RMA.

4.4. Сервизните специалисти

- регистрират в LCC (cc.lirex.bg) възникналия сервизен проблем;
- качествено и в срок решават възникнали мрежови проблеми;
- записват всички съществени данни и процеси при разрешаване на поет сервизен проблем, като своевременно отразяват всяка промяна на състоянието му в LCC системата и 'затварят' неговото досие там при разрешаване на сервизния проблем;
- правят предложения за превантивни и коригиращи действия на базата на практическия опит от решаването на възникнали проблеми.

5. Процедура

5.1. Общи принципи

Мрежово сервизно поддържане се извършва в случаите на:

- гаранционен сервиз на продуктите, закупени от дружеството или по договори за сервизно поддържане;
- извънгаранционен сервиз на продуктите и технологии по договори;
- поддържане на Интернет мрежата на *Лирекс.ком*.

Искания за сервизно поддържане от клиенти, които не са закупили продуктите от дружеството или нямат договор с дружеството, се разглеждат по общия ред за преглед и сключване на договор съгласно процедура *LPP001*, като се уведомява търговския директор или ръководителя на *Търговския отдел*.

Организацията на процесите за мрежово сервизно обслужване адаптира процедурите и стандартите на партньорите на *Лирекс.ком* в условията на организационната схема на дружеството и на българския пазар.

Преди началото на доставката на дадена ИТ услуга, ръководителят на функционалното звено, предоставящо тази услуга или определен от него служител подготвя **План за управление на външната ИТ услуга**. Този план съдържа информация в следните направления:

- обхвата на управление на предоставяната ИТ услуга;

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

- целите и изискванията, които трябва да бъдат постигнати чрез управление на услугата;
- процесите, които трябва да бъдат изпълнени при предоставянето на услугата;
- рамката на ролите и отговорностите на ръководството, включително висшестоящия отговорен собственик, собственика на процеса и управлението на доставчиците;
- ресурсите и бюджета, необходими за постигане на поставените цели;
- методи за регистрация и управление на инциденти и проблеми при предоставянето на услугата;
- взаимодействието между процесите на управление на услугата и начина, по който дейностите трябва да бъдат координирани;
- методи за регистрация и управление на инциденти и проблеми при предоставянето на услугата;
- подходящи методи за осигуряване на непрекъснатост и наличност на услугите;
- подхода, който трябва да се избере при определяне, оценка и управление на рисковете за постигане на поставените цели. Оценката на рисковете при доставка на ИТ услугата се прави количествено в съответствие с процедура LSP200 „Управление на риска" или качествено по показатели, посочени за всяка услуга в съответния План за нейното управление;
- въвеждане на промени в условията на предоставяните ИТ услуги;

Модел на Плана за управление на външната ИТ услуга е показан в документ LPN002. Неговото конкретно съдържание зависи от спецификата на съответната ИТ услуга и условията на договора, приложенията към него, SLA, изисквания на клиента и др. При необходимост могат да се разработят отделни планове за управление на различните подпроцеси при предоставянето на услуги, но те трябва да са в съответствие с Плана за управление на външната ИТ услуга.

При всяка съгласувана между страните промяна на условията по доставка на услугата, отразена в договора, приложенията към него, анекси, SLA и др., се съставя и одобрява нова редакция на Плана за управление на съответната услуга. Планът за управление на външната ИТ услуга се изготвя и поддържа в електронен вид или на хартия.

ЗАБЕЛЕЖКА: Изготвените и утвърдени Планове за доставка на ИТ услуги са предназначени да организират работата на доставчика на ИТ услуга и не се предоставят на клиентите.

Сервизно поддържане на продуктите и технологиите се извършва само от специалисти с адекватната квалификация и сертификация.

Мрежово сервизно обслужване се изпълнява от специализирано функционално звено *Сервизен Център* в структурата на звено *Телекомуникационни услуги.*

Функциите на звеното се изпълняват от специалисти, които работят във всички офиси на дружеството – централния и териториалните. Сервизните инженери от СЦ - ТКУ, които работят в офисите на територията на страната административно са подчинени и на ръководителите на съответните офиси.

За оперативна връзка и ефективно изпълнение на служебните си задължения, специалистите от СЦ - ТКУ ползват непрекъсната връзка по вътрешната Интернет мрежа на дружеството, със стационарни и мобилни телефонни средства.

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

Организацията на работа с клиентите в СЦ - ТКУ е на териториален принцип. Специалистите от СЦ - ТКУ, които работят в даден офис, отговарят за определена територия от страната (една или повече административни области).

Ръководителят на звено ТКУ организира и контролира цялостната дейност за мрежово сервизно обслужване.

Оперативното ръководство на мрежовото сервизно обслужване се осъществява от администратор на СЦ - ТКУ. Същият се определя от ръководителя на звено ТКУ.

За ефективно мрежово сервизно обслужване се поддържа в актуално състояние информация за инсталираното и/или поддържано мрежово оборудване (*Installed DB*).

Организацията на сервизното обслужване се основава на принципа за работа по възникнал проблем. Всяко съобщение за проблем от клиент се регистрира в LCC (*cc.lirex.bg)* и до приключване на работата по него се разглежда като *сервизен case*. Всеки сервизен case има уникален идентификатор. Със сервизния case се свързват реализуемите операции, техните изпълнители, приложимите ресурси (труд, резервни части, други).

Управлението на ресурсите на дружеството за решаване на възникнал проблем се основава на оценката за влиянието на функционалността на мрежовото оборудване върху бизнес операциите на клиента. За целта се прилага механизъм за категоризация на проблемите, респ. на регистрираните сервизни cases за решаването им, по приоритет. В основата на механизма е правилото, че колкото повече един проблем влияе на бизнес операциите на клиента, толкова повече внимание и ресурси се заделят за по-бързото му решаване. В детайли механизмът се разглежда в инструкция *LPI301*.

В изпълнение на декларираната политика на дружеството за осигуряване изискваното качество на предлаганото сервизно обслужване, се прилага механизъм за максимално пълно ангажиране на ресурсите за изпълнение на задълженията, наричан *ескалация на проблемите*. Същият се основава на правилото за своевременно ангажиране на длъжностни лица със съответни компетенции и правомощия.

В процеса на работата по сервизен case длъжностните лица (сервизни инженери) информират регулярно клиента за установеното състояние по проблема, предприетите действия и очакваните резултати от тях.

За ефективна комуникация на клиентите със СЦ - ТКУ се поддържат "горещ" телефон и e-mail адрес. Последните са адресирани към т.н. *Call Centre*, в който се дават денонощни дежурства от сервизни специалисти.

. Сервизното поддържане се основава на правилото за замяна на дефектирало Cisco оборудване с ново такова. За целта се прилага процедурата RMA, която работи по схемата "*заявка за замяна на хардуер по RMA → получаване на нов хардуер → износ на дефектиралия хардуер*" . За своевременно решаване на мрежовите проблеми на клиентите, в практическата дейност RMA процедурата се прилага гъвкаво. На клиентите се предоставя еквивалентно или с близки параметри и функционалности оборудване от поддържан резерв от оборотна техника.

Всички операции, изпълними при реализиране на сервизните дейности, се документират с подходящи записи по качеството. Записите се формират и поддържат съгласно изискванията на общосистемната процедура *LMP002*.

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

За оценка удовлетвореността на клиентите от предоставеното им сервизно обслужване, след приключване на всеки сервизен case се провежда анкетно проучване на тяхното мнение и оценка, съгласно процедура *LAP001.*

Ръководителят на звено ТКУ се запознава с резултатите и анализите на анкетните проучвания, и набелязва мерки за подобряване качеството на сервизната дейност, като за целта прилагат механизмите от процедура *LAP003.*

При изпълнение на сервизните операции се съблюдават изискванията на общосистемните за *СУКИС* процедури *LPP002, LPP003, LPP004* и *LAP004.*

5.2. Процеси

Мрежовото сервизно обслужване е организирано като съвкупност от процеси, с определени взаимовръзки между тях.

Създаването на информационната база за мрежовото сервизно поддържане е обект на процеса за информационно осигуряване, чиято връзка с другите процеси за реализиране на дейността е опосредствена – чрез БД ***Installed DB***.

Практическата дейност за сервизно обслужване се реализира като процес за *сервизно поддържане на мрежови решения*, включващ операциите от регистрация на възникнал мрежов проблем като сервизен case до намиране решение и приключване на работата по сервизния case. Редът за изпълнение на процеса се определя от инструкция *LPI301.* В тясна взаимовръзка с процеса протича и процесът за *ескалация на проблемите.* Дефинирането на ескалационния процес в контекста на мрежовото сервизно поддържане и редът за неговата реализация са описани в инструкция *LPI301.*

Планирането, отчетността и контролът на резервни части и оборотна техника, замяната на дефектирало оборудване по процедурата RMA са основни функции на процеса за *управление на резервни части*, регламентиран от инструкция *LPI302.* Взаимодействието с процеса се основава на заявки от сервизните инженери, изпълняващи задачи по сервизното поддържане. Операциите за документиране износа на дефектирало и вноса на ново оборудване по RMA и взаимодействието с отдел *Логистика* се определят в инструкция *LPI303.*

Функциите за цялостен контрол на реализуемото сервизно обслужване са обект на процеса за *контрол на сервизното обслужване.*

Схемата на процесите и взаимовръзките между тях са показани на *Фигура 1* от *Раздел 6* на процедурата.

5.3. Информационно осигуряване на Support

Организацията на мрежовия сервиз се основава на документирани задължения по договори за инсталирано оборудване и/или за сервизно поддържане. Това включва за всеки клиент:

- данни за клиента – наименование, адрес(и), телефонни и факс номера, mail – адреси, лице(а) за контакт;
- условия на сервизния договор – време за реакция, режим на поддържане (24 x 7, 5 x 8, друг), типа на сервиза (гаранционен, разширен гаранционен, извънгаранционен);
- инсталирано оборудване при клиент – за всяко устройство: p/n, s/n, версия на ОС, конфигурация, дата на инсталиране, местонахождение, други данни;
- топология на мрежата, схема(и) за управление;
- права за достъп, ако се изискват от клиента;

- данни за експлоатационната среда;
- характеристика на експлоатационния персонал;
- други данни, необходими за ефективно сервизно поддържане.

Изброените данни се съхраняват в БД ***Installed DB***.

Отговорен за документиране в БД ***Installed DB*** на задълженията по договори за инсталирано оборудване и/или за сервизно поддържане е водещият сделката.

В процеса на сервизното поддържане, данните в *Installed DB* се актуализират и допълват с информация за дефектирало и новоинсталирано оборудване, история на поддържаните конфигурации за всяко устройство, история за възникналите проблеми (No. на сервизни cases) за всяко устройство, данни за експлоатационната среда и персонал, други данни във връзка със сервизното обслужване.

Детайлното съдържание и структурата на данните в таблиците от *Installed DB* се определят от администратора на СЦ - МКТ.

Без да се абсолютизира, правило в организацията на сервизното обслужване е определянето на отговорен сервизен инженер за клиент или за обекти на клиент, ако последният има повече обекти с инсталирано оборудване. Това рефлектира в по-доброто познаване на обстановката, хората и условията за експлоатация. Наред със сервизното поддържане на мрежовото оборудване, отговорните сервизни инженери систематично работят за обучение на персонала на клиента.

Необходимата техническа и друга информация за изпълнение на мрежовото сервизно обслужване се осигурява с on-line достъп до информационните фондове на *партньорите на Лирекс.ком,* за което са осигурени и съответни права за достъп.

5.4. Контрол на сервизното обслужване

Контролът се осъществява на няколко нива:

- оперативен контрол за решаването на възникнали проблеми на клиентите, регистрирани като сервизни cases;
- контрол от висшестоящи длъжностни лица за съблюдаване времето за реакция и своевременно решаване на възникналите проблеми;
- контрол за наличностите от резервно оборудване;
- контрол за своевременна замяна на дефектирало оборудване с ново;
- контрол на фирмено ниво.

За оперативен контрол на сервизните cases се поддържа ***LCC***, в която се отразява статуса на всеки един case и отговорният(те) изпълнители – сервизни инженери. В записите се отразява всяка промяна в изпълнението на сервизен case. Записи в *LCC* се правят съгласно инструкция *LPI301.*

Отговорни за поддържането на ***LCC*** в актуално състояние са сервизните инженери.

Цялостният контрол на дейността в СЦ - МКТ се осъществява от неговия ръководител.

Резултат от ескалационния процес е непосредственото участие на висшестоящи длъжностни лица в решаването на възникнали мрежови проблеми, и по този начин – контрол за изпълнение на поети задължения за време на реакция и решаване на проблемите.

Отчетът на регистрацията и движението на наличностите от резервно оборудване се реализира с поддържането на регистър на резервните части. Редът за поддържане на регистъра се определя в инструкция *LPI302.*

Отговорен за отчета и регистрацията на резервното оборудване е администраторът на СЦ - ТКУ.

За контрол на своевременната замяна на дефектирало с ново оборудване по RMA процедурата се поддържа регистър за дефектирало мрежово оборудване ***Cisco_RMA.*** В записите на регистъра се отразява всяка една заявка за замяна на хардуер, доставката на новите устройства и експедицията на дефектиралите устройства. Редът за поддържане на регистъра се определя в инструкции *LPI302* и *LPI303.*

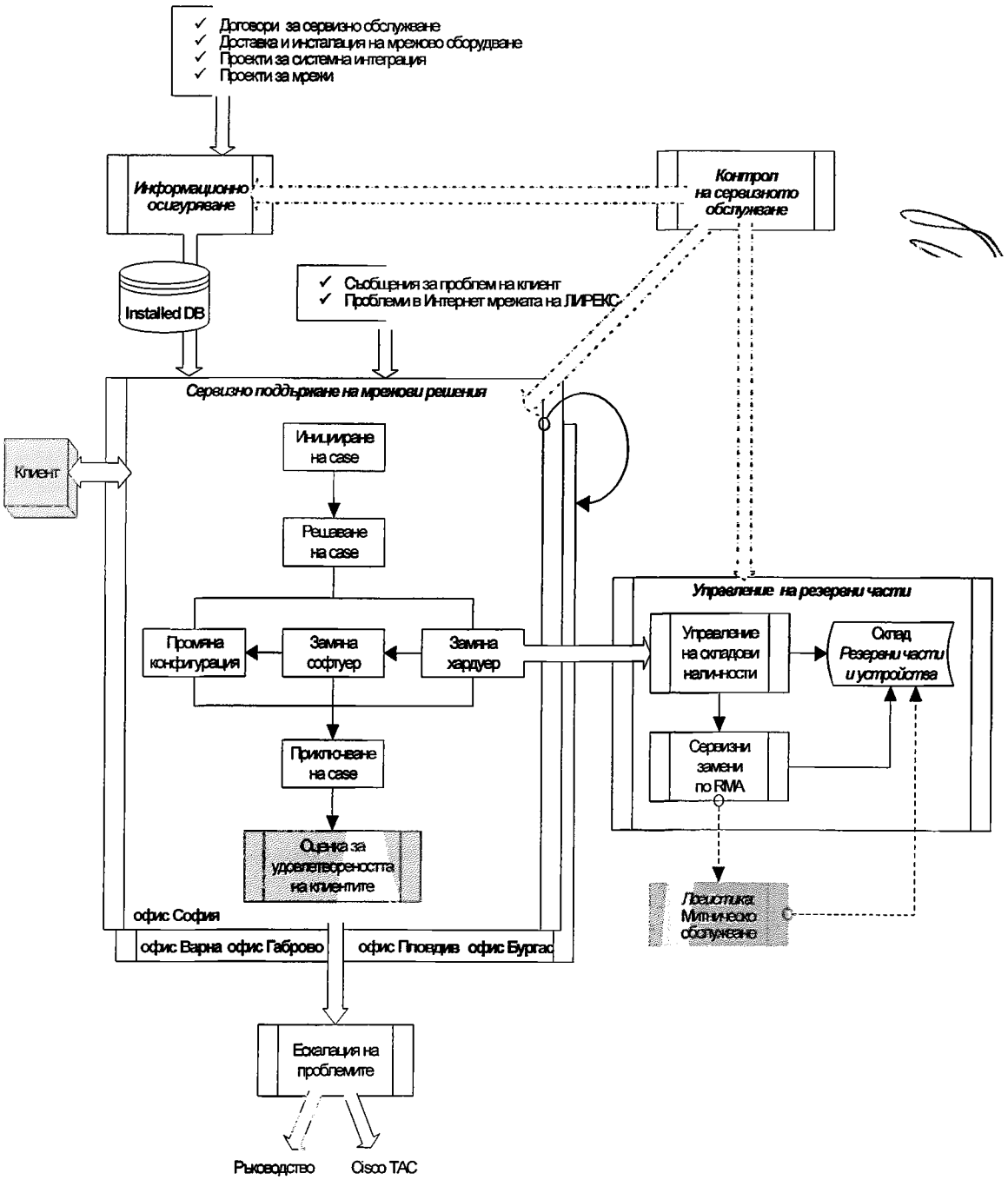
Отговорен за замените на оборудване по RMA процедурата е администраторът на СЦ - ТКУ.

6. Блок схеми

.....

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

Фигура 1. Схема на процесите за мрежово сервизно обслужване



7. Термини и съкращения

За актуалната редакция и съдържание на процедурата проверете в *LODIS*.

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

Ескалация на проблем	Политика на дружеството за своевременно уведомяване на съответни ръководни нива за възникнал проблем, с цел : • контрол за състоянието на работата по отстраняване на проблема; • ангажиране на необходимите за решаване на проблема ресурси; • участие на всички ръководни нива за осигуряване на декларираното ниво на качеството на продукти и услуги; • осведомяване на клиента за вземаните мерки за отстраняване на проблем;
Call Centre	Организационна форма за контакт със СЦ - ТКУ. Реализира се с 'горещ' телефон и e-mail адрес.
СЦ - ТКУ	Сервизен Център. Функционално звено в състава на звено Телекомуникационни услуги. Включва специалисти с необходимата квалификация. Специалистите от СЦ - ТКУ, които работят в офисите на територията на страната, административно са подчинени на ръководителите на офисите.
ТКУ	Телекомуникационни услуги
LCC	Автоматизирана информационна система за регистриране и проследяване на обслужването на сервизни проблеми – *cc.lirex.bg*
Installed DB	База данни с описание на инсталирано и/или поддържано от *Лирекс.ком* мрежово оборудване. За всяко устройство се поддържат данни за: • p/n и s/n; • компоненти (модули) и серийните им номера; • заредена операционна система (версия на ОС); • конфигурация; • данни за клиента; • други данни.
RMA	Return Materials Authorization. Процедура за замяна на (дефектирал) хардуер по предварително договорени сервизни условия.

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

СУКИС	Система за Управление на качеството и информационната сигурност на *Лирекс.ком.*
Сигурност на информацията (информационна сигурност)	Запазване на поверителност, цялостност и наличност на информацията.
Лирекс.ком	Дружествата Лирекс БГ, Лирекс БС, Лирекс Хай Тех, Беолик, Лирекс Скопие, Теза

8. Препратки към документи

ID на документа	наименование на документа
LMP002	Процедура: Управление на документи и записи за реализация на фирмените дейности
LMP003	Процедура: Преглед на СУКИС от Ръководството
LPP001	Процедура: Подготовка, преглед и сключване на договори
LPP002	Процедура: Идентификация и проследимост на продукти
LPP003	Процедура: Работа с продукти на клиент
LPP004	Процедура: Манипулиране, съхранение, опаковане и доставка на продукти
LPP006	Процедура: Управление на програми и проекти
LPP013	Процедура: Управление на Управление на външни ИТ услуги
LPI301	Инструкция: Сервизно поддържане на мрежови решения (Support)
LPI302	Инструкция: Управление на резервни части за Support
LPI303	Инструкция: Сервизни замени на продукти по RMA
LAP001	Процедура: Измерване степента на удовлетвореност на клиентите
LAP003	Процедура: Коригиращи и превантивни действия
LAP004	Процедура: Работа с продукти, несъответстващи на определените изисквания
LPN002	Модел: План за управление на външна ИТ услуга

9. Оценки

За изпълнени задължения и възникнали проблеми относно мрежово сервизно обслужване, ръководителят на звено ТКУ докладва на текущите прегледи от Ръководството съгласно процедура *LMP003* и *LMP013.* Оценката на ефективността и ефикасността на предоставяните услуги се прави на основа на изпълнението на договорните изисквания за съответната услуга, на SLA, както и изразходваните финансови ресурси за тяхното изпълнение

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

10. Документирана информация

Сигурността на записите, свързани с изпълняваните дейности се осигурява от процедурите и инструкциите на въведената Система за управление на качеството и информационната сигурност.

Информацията, свързана с личните данни и търговската дейност на клиентите се събира и използва само във връзка с точното и навременно изпълнение на техните заявки и осигуряване на необходимото качество на обслужването.

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

ЛИРЕКС.КОМ	Процедура: Измерване степента на удовлетвореност на клиентите	Версия 9
	LAP001	1 от 6

1. История на редакциите

версия	описание на промяната	автор	проверил	утвърдил	дата на въвеждане
7	Въвеждане на изискванията на ISO/IEC 20000-1:2005	Б.Йорданов	Р.Илиева	Д. Илиева	17.02.2010
8	Отразяване на препоръка от външен одит от 06.12.2012 г.	Б. Йорданов	Вл. Стоев	Д. Илиева	03.01.2013
9	Актуализиране на документите от СУКИС	М.Йончева	Вл. Стоев	Д. Илиева	15.07.2019

2. Предназначение

Процедурата определя реда, методите и средствата за измерване степента на удовлетвореност на клиентите от предоставените им продукти и услуги.

3. Приложимост

Приложима е при събиране и обработка на информация за удовлетвореността на клиентите от предоставени услуги и закупувани продукти, както и за търговското обслужване.

4. Отговорности

4.1. **Ръководителят на направление *Маркетинг***

- планира дейностите за проучване удовлетвореността на клиентите;
- организира разработване на анкетни карти за проучване удовлетвореността на клиентите от предоставяните продукти/услуги от съответното функционално звено със съдействието на управляващите процеси/дейности;
- анализира обработените данни от анкетни проучвания и обобщава резултатите;
- изготвя доклади въз основа на получените резултати и съгласувано с управляващите процесите/дейностите прави предложения пред висшето ръководство за коригиращи, превантивни и други действия.

4.2. **Управляващите функционални звена**

- съдействат при разработването на анкетни карти за проучване удовлетвореността на клиентите от предоставяните продукти/услуги от ръководеното функционално звено;
- анализират случаите за рекламация и неудовлетворителни оценки от страна на клиентите, вземат решение за последващи действия, включително и коригиращи/превантивни действия, съгласно процедура *LAP003 Коригиращи действия;*
- организират събирането на необходимата за процеса на анкетиране контактна информация за клиентите (име на компания, лице за контакт, телефон, e-mail адрес) на звеното и предаването ѝ на организатора от отдел *Маркетинг*;
- съдействат в процеса за анкетиране на клиентите.

4.3. **Отдел *Маркетинг***

- организира процеса за събиране на контактна информация за клиентите на отделните функционални звена, поддържа актуален списък на клиентите според

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

предоставените от функционалните звена данни и отразява в него попълването на анкетна карта;

- организира процеса за анкетиране на клиентите;
- получава, класифицира, съхранява и обработва попълнените анкетни карти;
- следи и обобщава информацията за референции, рекламации и предложения, получени от клиенти на продуктите и услугите на дружествата Лирекс.ком за включване в докладите за оценка на клиентската удовлетвореност;
- следи резултатите от проучването за лоялност на клиентите на сайта на Cisco и ги включва в доклади за удовлетвореността на клиентите на Cisco.

5. Процедура

5.1. Приложими оценки

За оценка удовлетвореността на клиентите от предоставяните услуги или закупувани продукти и съпровождащото покупката обслужване при използване на анкети се прилага 5 – степенна скала, както следва:

Оценка		*интерпретация*
бал	*Качествена*	
1	Най-ниска степен на оценка (съгласие, одобрение и т.н.)	Според въпроса
2	Ниска степен на оценка (съгласие, одобрение и т.н.)	Според въпроса
3	Неутрална степен на оценка (съгласие, одобрение и т.н.)	Според въпроса
4	Висока степен на оценка (съгласие, одобрение и т.н.)	Според въпроса
5	Най-висока степен на оценка (съгласие, одобрение и т.н.)	Според въпроса
n/a	Без мнение	Клиентът не може да оцени съответния показател.

Допълнителна оценка за удовлетвореността на клиентите се прави на базата на отговорите на „отворени" въпроси, както и от препоръки и коментари, получени от тях.

5.2. Събиране на информация

Информация за удовлетвореността на клиентите се събира от попълнените анкети, референции, рекламации или отзиви, получени по пощата, e-mail, телефон или факс.

Съдържанието на отделните анкети се определя съвместно с ръководителите на функционалните звена, като задаваните въпроси са в зависимост от приложимата форма и целта на провежданата анкета.

Прилагат се следните форми за анкетиране:

- попълване на web –форми,
- попълване на документални бланки за анкетиране.

Анкетиране на клиентите се провежда периодично или след провеждане на мероприятие (семинар, изложение, друго), съгласно правилата от *Таблица* 1.

За контакти с клиентите се използват данните за тях във функционалните звена, които имат взаимоотношения с тях и се систематизират в база данни в *Маркетинг*.

5.3. **Обработка на резултатите**

Събраните данни периодично се обработват и обобщават от служители в отдел *Маркетинг.*

5.4. **Анализи и обобщения**

В края на всяка година получените данни се анализират и обобщават от ръководителя на отдел *Маркетинг* в писмен доклад за оценка удовлетвореността на клиентите, който се докладва при преглед от Ръководството, съгласно изискванията на процедура *LMP003 Преглед на СУКИС от Ръководството.*

5.5. **Реакция в случаи на неудовлетворителни оценки и рекламации**

В случай на неудовлетворителна оценка в анкетна карта или рекламация от страна на клиент на стоки или услуги, предоставени от дружествата Лирекс.ком, получилият анкетната карта или приелият рекламацията служител уведомява съответните длъжностни лица съгласно *Таблица* 1 с цел вземане на отношение и предприемане на превантивни или коригиращи действия.

За получени неудовлетворителни оценки и рекламации, на първото мениджърско събиране ръководителите на съответните дейности/процеси докладват за всеки конкретен случай, както и за резултатите от анализа и предприетите мерки по този повод.

След изпращане годишната анкета на Cisco Systems ежеседмично се следят резултатите от проучването за лоялност на клиентите и при всеки постъпил случай на "high risk" и "trapped" се информира съответния Акаунт мениджър и Търговския директор. Акаунт мениджърът проучва причините, довели до тези резултати и определя мерките, които трябва да се предприемат. Те се отразяват на бланка Cisco-CSAT-YYYY.

5.6. **Информация за устойчивата удовлетвореност на клиентите**

За получаване на информация за удовлетвореността на клиентите, които вече са ползвали услугите на дружеството и са внедрили негови проекти, след приключване на работата по определен проект и предаването му на клиента, ръководството на дружеството може да възложи на УПР да събере информация за устойчивата удовлетвореност и за нагласите на клиентите за бъдещо сътрудничество с дружеството.

УПР с помощта на служители, които не са работили за дадения клиент, провеждат анкети, интервюта, посещения при клиента и др. След това УПР изготвя доклад, който съдържа информация и анализи за мнението на клиента по изпълнението на проекта, степента на неговата удовлетвореност, качеството на гаранционното обслужване, взаимоотношенията изпълнител - клиент, предложенията и препоръките на клиента за подобряване на работата, както и нагласите му за продължаване на сътрудничеството с изпълнителя.

Докладът се предава на ръководството за сведение и се архивира към документацията на проекта.

6. Блок схеми

Не се прилага блок – схема.

7. Термини и съкращения

Анкета	Метод на проучване, посредством който набор от въпроси се предоставя на определен брой хора с цел да се получат отговори на тези въпроси.

Анкетна карта	Форма за събиране на първични данни. Състои се от набор въпроси, зададени към клиента, на които той трябва да даде отговор.
Управляващ дейност/процес	Служител, в чиито правомощия и отговорности е дефинирано правото да управлява съответен процес/функционална дейност.
Упълномощен представител на ръководството (УПР)	Упълномощен от ръководството на Лирекс.ком ръководен служител, отговарящ за контрола по приложимостта и развитието на СУКИС.
Сигурност на информацията (информационна сигурност)	Запазване на поверителност, цялостност и наличност на информацията. [ISO/IEC 17799-1:2005]
СУКИС	Система за управление на качеството и информационната сигурност в дружествата Лирекс.ком.
Лирекс.ком	Дружествата Лирекс БГ, Лирекс БС, Лирекс Хай Тех, Беолик, Лирекс Скопие, Теза

8. Препратки към документи

ID на документа	*наименование на документа*
LMP003	Процедура: Преглед на СУКИС от Ръководството
LAP003	Процедура: Коригиращи действия

9. Оценки

Не се правят измервания за оценка

10. Документирана информация

Информацията, свързана с личните данни и търговската дейност на клиентите се събира и използва само във връзка с измерване степента на удовлетвореност на клиентите от предоставените им продукти и услуги.

Сигурността на събираната информация се осигурява от процедурите и инструкциите на въведената Система за управление на качеството и информационната сигурност.

Анкетни карти	*симв.наименование*	съгласно приложимия подход за анкетиране
	индексация/регистрация	по конвенции
	е-фонд активен	по съгласуваност между ръководителите дейности / процеси и ръководителя на *Маркетинг и Реклама*
	достъп	само от сътрудниците, които обработват анкетите

ЛИРЕКС.КОМ	Процедура: Измерване степента на удовлетвореност на клиентите	Версия 9
	LAP001	5 от 6

	съхранение	6 месеца след обработката им; сътрудник от *Маркетинг*, който обработва анкетите
	doc-фонд активен	фонд Анкетни карти
	достъп	само от сътрудниците, които обработват анкетите
	съхранение	6 месеца след обработката им; сътрудник от *Маркетинг*, който обработва анкетите

Доклад за оценка удовлетвореността на клиентите от предоставяните стоки и услуги от дружествата Лирекс.ком	*сима наименование*	***SSReport-yyyymm***, където yyyy – година, mm –месец на изготвяне на доклада
	индексация/регистрация	yyyy – година, mm –месец на изготвяне на доклада
	e-фонд активен	***Lomis/Satisfactory Survey/***
	достъп	W,U – ръководител *Маркетинг и Реклама*; R -свободен
	съхранение	за календарната година; администратор *LOMIS*
	архивен	архивен ***Lomis/Satisfactory Survey/***
	достъп	само R -свободен
	съхранение	3 години; администратор *LOMIS*
	doc-фонд	архив на СУКИС
	достъп	с разрешение на висшето ръководство
	съхранение	3 години; администратор СУКИС

Доклад за оценка удовлетвореността на клиентите от гаранционен ремонт	*сима наименование*	оценка удовлетвореността на клиентите от гаранционен ремонт
	индексация/регистрация	
	e-фонд активен	\Lomis\Satisfactory Survey\Reports\HP Warranty Support Reports\
	достъп	W,U – ръководител *Маркетинг*; R -свободен
	съхранение	за календарната година; администратор *LOMIS*
	архивен	архивен ***\Lomis\Satisfactory Survey***

За актуалната редакция и съдържание на процедурата проверете в *LODIS*.

	достъп	само R -свободен
	съхранение	3 години; администратор *LOMIS*

Таблица за отразяване на мерките в случаите на "high risk", "trapped" или ниска оценка на удовлетвореността от клиентите (Cisco-CSAT-YYYY)	*сист.наименование*	мерки в случаите на "high risk", "trapped" или ниска оценка на удовлетвореността от клиентите
	в-фонд активен	http://eportal.lirex.com/LOMIS/Audits/CISCO/Forms/AllItems.aspx
	достъп	W,U – ръководител *Маркетинг*; R -свободен
	съхранение	за календарната година; администратор *LOMIS*
	архивен	архивен *Lomis*\
	съхранение	3 години; администратор *LOMIS*

Формите за попълване на анкетни карти са в електронен вид и се поддържат на Интернет - адреси http://index.bg/anketa/lirex/lirexhitech-trade.php и http://index.bg/anketa/lirex/lirexhitech-service.php; или според процедурите за дейността на съответните функционални звена. При необходимост, същите могат да бъдат предоставени за попълване на клиента във вид на хартиено копие.

Резултатите от попълнените анкетни карти се събират автоматично в електронен вид и се поддържат на Интернет - адрес според процедурите за дейността на съответните функционални звена.

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

1. История на редакциите

версия	описание на промяната	автор	проверил	утвърдил	дата въвеждане
3	Отразяване на промени във връзка с направени забележки и препоръки от одит на адекватност на документите от СУК за сертификация по AQAP 2110	М.Цолов	Д. Кънчев	Д. Илиева	14.03.2005
4	Въвеждане на изискванията на ISO/IEC 27001:2005	Б. Йорданов	Д. Кънчев	Д. Илиева	11.02.2009
5	Актуализиране на документите от СУКИС	М. Йончева	Вл. Стоев	Д. Илиева	16.07.2019

2. Предназначение

Процедурата определя реда за управление на материали и продукти, които не отговарят на определени изисквания.

3. Приложимост

Процедурата се прилага относно:

- закупувани материали и продукти, независимо от естеството на извършвания входящ контрол по силата на договори с доставчиците и последващото им приложение;
- продукти със срок за годност;
- продукти, за които несъответствието е открито на етапите за разработване или внедряване при провеждане на тестове в съответствие с план за проект/програма;
- продукти, за които несъответствието е установено след продажба/предоставяне на клиент.

Изискванията на процедурата се отразяват в установения ред за изпълнение на дейностите/процесите с отчитане на тяхната специфика и предмета на дейност.

Като несъответствие не се разглежда отклонение от определените изисквания в резултат от неправомерни действия на клиент при транспортиране, манипулиране, съхранение и експлоатация.

4. Отговорности

4.1. Отговорници по процеси

(управляващи дейност/процес/звено, ръководители проект/програма, директори)

- за всеки конкретен случай разпореждат проверка за несъответствие на продукт, предоставен на клиент;
- определят реда за маркиране и съхранение на продукти с установени несъответствия;
- определят последващите действия относно продукти с несъответствия;
- правят предложения за коригиращи и превантивни действия за по-ефективна и ефикасна работа с продукти с установени несъответствия;
- изготвят анализи за установените случаи на продукти с несъответствие в ръководените направления на дейност;

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

- контролират подчинените си служители за правилно експлоатиране на продукти с несъответствие.

4.2. Всеки служител

- уведомява съответния отговорен мениджър за установено несъответствие в продукт;
- съхранява продукти с несъответствия съгласно получените разпореждания;
- изпълнява разпорежданията за работа с продукти с несъответствия;
- по разпореждане, документира несъответствието на продукт по установения разпоредения ред.

4.3. Завеждащият склад

- ежемесечно проверява наличните в склада продукти със срок на годност за валидност на срока им;
- за налични в склада продукти с изтекъл срок за годност уведомява търговския директор и изпълнява неговите разпореждания;
- поддържа и съхранява документите относно продуктите с установени несъответствия.

5. Процедура

5.1. Установяване на несъответствие

Несъответствие на продукт на специфицирани изисквания може да се установи:

- в процеса на осъществявания регламентиран входящ контрол при получаване от доставчик;
- при проверка на функционалните характеристики на продукт от специалисти на дружеството в процеса на окомплектоване и системна интеграция, при провеждане на тестове и други изследвания;
- при периодичната месечна проверка за срока на годност на стоките в склада;
- при инсталация от клиента или от специалисти на дружеството на продукти, за които не е осъществен фактически входящ контрол;
- от клиента, когато в процеса на експлоатация са открити несъответствия, които е било невъзможно да се установят на по-ранен етап.

5.2. Документиране на установено несъответствие при/от клиент - рекламации

В случаите на установено несъответствие от клиент, за което той уведомява дружеството съгласно условията на сключения договор, отговорният мениджър или търговският директор разпорежда проверка от специалист(и) на дружеството с необходимата квалификация. Проверката се извършва съгласно :

- регламентирания ред за функционални тестове;
- предвидения специфичен ред в споразумението с клиента или в плана за качество на проект.

За извършената проверка при клиента, с цел установяване на несъответствие, осъществилият същата специалист(и) от дружеството съставя(т) констативен протокол, който се подписва и от представител на клиента. Протоколът се докладва на разпоредилия проверката, който определя и последващите действия.

Всички документални записи (в оригинал или като копие) за установено несъответствие при/от клиент (рекламация) и за документиране на разпоредени последващи операции се окомплектоват и съхраняват.

Отговорност за окомплектоване на документите за рекламация носи ръководителят, разпоредил проверката по рекламация.

5.3. Действия относно продукт с несъответствие

За несъответствие на продукт, установилият го служител на дружеството уведомява съответния ръководител.

Всеки продукт с установено несъответствие се маркира по подходящ начин, "изолира" за ползване и съхраняване, съгласно разпорежданията на отговорния ръководител, до вземане на решение за неговата приложимост. Маркиране се осъществява по установения в практиката начин с цветни етикети, надписи или други, определени от управляващите дейности/процеси/звена. За изпълнението на маркировката отговорният ръководител определя служителя, който да я извърши.

Решение за последващите действия относно продукт с установени несъответствия взема съответният отговорен мениджър.

Преценката на отговорния мениджър се основава на:

- допустимия диапазон на отклоненията от параметрите на продукта;
- възможна промяна на функционалностите;
- алтернативно приложение;
- цената и времето за преработка, ремонт или възстановяване.

Възможни разпореждания за действие са:

- провеждане на допълнителни функционални тестове;
- ползване с установеното несъответствие;
- ремонт, преработка;
- връщане на доставчик;
- замяна с аналогичен продукт;
- настройка на функционалности;
- унищожаване.

За взетото решение относно действията с продукт, несъответстващ на изискванията, отговорният мениджър уведомява:

- доставчика, по съгласувания за целта ред;
- клиента, на когото е предоставен продукта;
- търговските звена на дружеството;
- функционалните звена или екипи, на които се възлагат допълнителни задачи по отношение на продукта.

При целесъобразност и необходимост, след анализ на причините за установено несъответствие, отговорният мениджър прави предложения за коригиращи действия и/или оценка на риска.

5.4. Анализ на несъответствията

Всяко несъответствие се класифицира в зависимост от причината за неговото възникване:

- проектни решения,

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

- фабрични дефекти,
- недостатъци на доставчика,
- пропуски в установения ред за работа с продукти в дружеството,
- недостатъчна квалификация на персонала на дружеството,
- други.

Анализите на установени несъответствия на продукти на определените изисквания се докладват и обсъждат на прегледите на ръководството, съгласно процедура *LMP003 Преглед на СУКИС от Ръководството.*

6. Блок схеми

За процедурата не се прилага блок-схема.

7. Термини и съкращения

Клиент	Юридическо или физическо лице, което сключва споразумение/договор за доставка на продукт или услуга.
Продукт	Технически средства и устройства, стандартен и базов софтуер, дистрибутивен материал за софтуер, или други компоненти и елементи, които се интегрират в разработвани и тествани от дружествата продукти или се доставят на клиентите по спецификация.
Продукт с несъответствие	Продукт, който не отговаря на предварително определени изисквания за технически характеристики, функционалности, срок за годност, други специфични изисквания.
Отговорен мениджър (ръководител)	Ръководен служител, в чиито правомощия е вземане на решение относно последваща работа с продукт, за който е установено несъответствие. Управляващ дейност/процес/организационно звено, ръководител на програма/проект, директор.
Управляващ дейност/процес	Служител, в чиито правомощия и отговорности е дефинирано правото да управлява съответен процес/функционална дейност.
Формален (входящ) контрол	Контрол на закупен продукт относно: • цялостност на опаковка и маркировки; • външни белези за нарушаване на цялостност и търговски вид; • съответствие на продуктови и серийни номера; • пълнота и коректност на съпровождащи закупуването документи; • съответствие на изискванията за окомплектованост, ако се разопакова стоката. Не включва проверка за функционалност.
Фактически контрол	Контрол на продукт (стока) за окомплектованост и за изпълнение на функционалности, в съответствие с техническа спецификация.
Система за управление на качеството и информационната сигурност (СУКИС)	Организационната структура на *ЛИРЕКС.КОМ* в комплекс с регламентирания ред, процесите и ресурсите, необходими за управление качеството и информационната сигурност на предлагани продукти и услуги.
Сигурност на информацията (информационна сигурност)	Запазване на поверителност, цялостност и наличност на информацията.

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

Упълномощен Представител на Ръководството (УПР)	Упълномощен от Ръководството на *ЛИРЕКС.КОМ* ръководен служител, отговарящ за контрола по приложимостта и развитието на *СУКИС.*

8. Препратки към документи

ID на документа	*наименование на документа*
LMP003	Процедура: Прегледи на СУКИС от Ръководството
LAP003	Процедура: Коригиращи действия. Непрекъснато подобрение.

9. Оценки

Изготвят се ежегодни отчети за целите на прегледите от ръководството.

10. Документирана информация

Сигурността на информацията, свързана с изпълняваните дейности се осигурява от процедурите и инструкциите на въведената Система за управление на качеството и информационната сигурност.

Изготвяните протоколи за установени несъответствия на продукт при/от клиент може да се съхраняват, в зависимост от случая, и в информационните фондове на сервизните центрове, в досиетата на проекти, в досиетата на клиенти.

Документи по рекламации	*симв.наименование*		
	индексация		по дата на регистрация и наименование на клиент
	дос-фонд	*активен*	дело "*Документи за рекламации*";
		достъп	
		съхранение	деловодител; 3 календарни години;
		архивен	"*Документи за рекламации*";
		достъп	с разрешение на директор
		съхранение	деловодител; безсрочно

Анализи на продукти с несъответствие	*симв.наименование*		
	индексация		по дата на изготвения документ
	дос-фонд	*активен*	*\LOMIS\Nonconforming\Nonconforming Products*
		достъп	

За актуалната редакция и съдържание на процедурата проверете в *LODIS*.

		съхранение	администратор *LOMIS;* 1 календарна година
		архивен	*\LOMIS Archiv\Nonconforming\Nonconforming Products*
		достъп	
		съхранение	администратор *LOMIS;* безсрочно
	doc-фонд	*активен*	архив на СУКИС
		достъп	с разрешение на УПР
		съхранение	администратор на СУКИС; 1 календарна година;
		архивен	архив на СУКИС
		достъп	с разрешение на УПР
		съхранение	администратор на СУКИС; безсрочно

10.1. Форми и бланки

ID на формата	*наименование на формата*
L-ADM-002-TSP	Протокол за техническо състояние

ЛИРЕКС.КОМ	Политики и управление на информационната сигурност	Версия 4
	LSP001	1 от 9

1. История на редакциите

версия	описание на промяната	автор	проверил	утвърдил	дата въвеждане
2	Отстраняване на несъответствията от предварителния одит по ISO/IEC 27001:2005	Б.Йорданов	Б.Янчев	Д.Илиева	16.03.2000
3	Въвеждане на изискванията на ISO/IEC 27001:2013	Б.Йорданов	Б.Янчев	*Д.Илиева*	09.03.2015
4	Актуализиране на документите от СУКИС	М.Йончева	Р.Радев	Д.Илиева	27.08.2019

2. Предназначение

Документът има за цел да определи политиките (цялостните намерения и насоки на дейност) за създаване, внедряване, поддържане и непрекъснато подобряване на Системата за управление на информационната сигурност (СУИС) в контекста на дружествата Лирекс.ком и в съответствие с изискванията на ISO/IEC 27001:2013.

3. Приложимост

Политиките се прилагат при управлението на Системата за управление на информационната сигурност в рамките на СУКИС в дружествата Лирекс.ком и са задължителни за всички служители в тях.

4. Отговорности

Пълномощията и отговорностите на управленските органи и позиции за определяне на политиките (цялостните намерения и насоки на дейност) на дружествата Лирекс.ком, насочени към осигуряване и поддържане на сигурността на информацията, в съответствие с изискванията на изпълняваните дейности, стандарта ISO/IEC 27001и приложимите законови и други нормативни актове, като част от внедрената СУКИС в дружествата Лирекс.ком, са регламентирани в съответните процедури и включват:

- **Съвет по качеството и информационна сигурност –** изпълнява главната функция по ръководството и контрола на Системата по качеството и информационната сигурност в дружествата Лирекс.ком. Състои се от управителите и мениджърите/ръководителите на функционалните направления. Приема доклада за оценка на информационните рискове и се свиква за обсъждане на възникнали въпроси или инциденти, свързани с информационната сигурност.
- **УПР по Системата за управление на качеството и информационната сигурност** - Организира разработването на политиките, процедурите и инструкциите от СУКИС по отношение на сигурността на информацията. Отговаря за документацията и записите и вътрешния контрол. Докладва на прегледи от ръководството за състоянието на СУКИС и предлага мероприятия за нейното развитие и усъвършенстване.

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

- **Ръководител по информационната сигурност (РИС) -** отговаря целия персонал да бъде напълно информиран по отношение на задълженията и отговорностите, включени в процедурите и инструкциите по отношение на информационната сигурност. Организира провеждането и документирането на периодичните проверки и тестове за сигурност на системите. Докладва на Прегледите от ръководството за състоянието на информационната сигурност в Лирекс.ком.
- **Ръководители на функционални звена -** носят отговорност по отношение на данните и другите информационни ресурси, използвани при дейностите, които се осъществяват под тяхното наблюдение и контрол, за да се гарантира, че те са адекватно защитени, а също така се спазват приложимите указания, процедури и механизми при изпълнението на съответните дейности. Притежават правомощия за инициатива за промени по отношение на действащата СУИС в дружествата Лирекс.ком.
- **Системен администратор –** отговаря за инсталацията, конфигурацията и администрирането на инфраструктурата на публични ключове, както и за регистрацията и създаването на удостоверения; отговаря за ежедневната работа на системата за издаване на удостоверения, като извършва редовно процедури по архивиране, създаване на резервни копия на информация и възстановяване информационни системи.
- **Всички служители -** служителите, вкл. временно наетите, посетителите, доставчици и подизпълнители, са длъжни да спазват указанията, процедурите и механизмите за информационна сигурност и активно да участват в опазването на информационните активи/ресурси на Лирекс.ком. Те не трябва да имат достъп и да боравят с информационните активи без да имат съответните пълномощия и са длъжни да докладват за нарушения по отношение на сигурността на Ръководителя по информационна сигурност.

5. Външен и вътрешен контекст

Външният и вътрешен контекст (средата) е в зависимост от основните дейности, които дружествата Лирекс.ком изпълняват:

- **Лирекс БГ –** изграждане и поддръжка на големи интегрирани информационни проекти с национално значение в държавни институции, сектора на отбраната и вътрешната сигурност. Предлага услуги, които покриват всички етапи от жизнения цикъл на проектите, изискващи специални мерки за сигурност.
- **Лирекс БС –** извършва одити на ИТ системи, изпълнява консултантски услуги и интегрирани информационни и комуникационни решения, съобразени с изискванията и конкретните потребности на различни корпоративни клиенти. Осъществява аутсорсинг на ИТ приложения, мониторинг и поддръжка на ИТ инфраструктурата на държавната и общинска администрация и на корпоративни клиенти.
- **Лирекс Хай Тех –** осъществява продажби и доставки на компютърно, комуникационно и мрежово оборудване, офис техника, консумативи и стандартен софтуер. Продуктите могат да бъдат поръчани освен в офисите на дружеството и чрез електронен магазин. Предлага гаранционно и извънгаранционно обслужване в сервизните си центрове и на обекти на клиента.

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

- **Лирекс Скопие** – предоставя всички услуги от портфолиото на дружествата Лирекс.ком на територията на Република Македония.
- **ТЕЗА** – извършва услуги за професионални обучения, доставка и инсталиране на специализирани приложни програми. Притежава лицензия за център за професионално обучение (ЦПО) от Националната агенция за професионално образование и обучение (НАПОО). Разполага с напълно оборудван компютърен учебен център.

5.1. Външен контекст

Външният контекст е средата, която съществува извън границите на дружествата Лирекс.ком и оказва потенциално въздействие върху тяхното функциониране и развитие и в която те се стремят да постигнат своите цели. Външната среда обхваща следните:

- **Политически и правни фактори** – държавната финансова, кредитна, данъчна и митническа политика; мерките по защита личните данни и правата на потребителите; патентното законодателство; законодателството за защита на околната среда; антимонополното законодателство; приложимите законови регулации и ограничения; междудържавните отношения със страните, където дружествата Лирекс.ком развиват дейност, както и политическите и икономически условия в тези държави.
- **Икономически фактори** – макроикономическият климат, който като цяло определя възможността дружествата Лирекс.ком да постигнат своите финансови цели. Влияние оказват и темповете на общото икономическо развитие, валутните курсове, кредитната и застрахователна политика и др.
- **Технологични фактори** - дружествата Лирекс.ком развиват дейност в компютърните и комуникационните технологии, които се развиват ускорено и постоянно се обновяват. Средата е силно конкурентна и това изисква от дружествата да следят последните постижения и изпреварващо да прилагат нововъведенията в своята работа, за да имат пазарен успех.

5.2. Вътрешен контекст

Вътрешната среда, в която дружествата Лирекс.ком работят и която влияе на възможността да се изпълнят поставените цели от СУИС, включва следните основни фактори:

- **Организационни** – обхващат функционалните, йерархичните, длъжностните и др. структури на дружествата. В тях са въведени отговорностите, задачите и пълномощията на персонала от всички нива по отношение на дейностите, касаещи качеството, информационната сигурност, безопасността при работа и опазването на околната среда в съответствие с изискванията на въведените стандарти в интегрираната СУКИС.
- **Социални** – включват служителите, условията на труда и работната среда. По отношение на човешкия потенциал като основен фактор на една организация в Лирекс.ком са въведени сериозни изисквания при подбора, наемането и повишаването на квалификацията. Всички служители са мотивирани непрекъснато да повишават своите познания и умения, за да отговорят на динамичните изисквания на изпълняваните дейности. Сертифицирането на въведената в Лирекс.ком СУКИС

по ISO 45001 и ISO 14001 показва сериозните социални ангажимента на ръководствата на дружествата към работната и околната среда.

- **Технически** – в дружествата Лирекс.ком се използва съвременно техническо и информационно оборудване и свързаните с него обща инфраструктура, ноу-хау и технологии. Въведените в дружествата изисквания за сигурност на информационните технологии осигуряват сигурна и защитена комуникация вътре в дружествата и извън тях по комутируеми канали.

Вътрешната среда на дружествата Лирекс.ком включва и ценностите, на които са подчинени всички аспекти на организация на работата и управлението в дружествата Лирекс.ком в съответствие със стандартите ISO 9001, ISO/IEC 27001, ISO/IEC 20000-1, ISO 14001 и ISO 45001 и са отразени в Наръчника на СУКИС (LQS Manual).

6. Заинтересовани страни и техните изисквания към ИС

6.1. Заинтересовани страни

Заинтересованите страни, които имат отношение към Системата за управление на сигурността на информацията на дружествата Лирекс.ком са:

- **Клиентите** – при доставянето на стоки и услуги на индивидуалните и корпоративни клиенти е необходима информация, свързана с личните данни и търговската дейност на клиентите. Тя се събира и използва само от служителите, ангажирани в съответната сделка или проект във връзка с точното им и навременно изпълнение. Задълженията за опазване от страна на Лирекс.ком на чувствителната информация се включва в договорите и в споразумения за поверителност с клиентите.
- **Служителите на дружествата** в дружествата Лирекс.ком - при комуникацията с клиентите, те имат достъп до информация, чувствителна за клиентите (лични данни, търговска тайна, ноу-хау и др.). Ползването на такава информация и данни се осъществява само в рамките на изпълнението на договорите. За работа с класифицирана информация, свързана с изпълнение на проекти на клиентите, се допускат само специалисти от дружествата с валидни сертификати за достъп по Закона за защита на класифицираната информация и по стандартите на НАТО (NATO Secret).
- **Доставчиците** – институции, организации или лица, които осигуряват необходимите стоки и услуги на дружествата Лирекс.ком за осъществяване на цялостната им дейност. В споразуменията с тях, при необходимост, се включват изисквания за сигурност на информацията. За контакти с отделните доставчици са определени различни лица или екипи, с цел ефективна комуникация при възникване на проблем.
- **Държавни и контролни органи** - структури на държавната и общинската администрация. Имат законови правомощия за определен достъп до лични и търговски данни на дружествата Лирекс.ком и клиентите, както и задължения за спазване на изискванията за конфиденциалност на получената информация.
- **Сертифициращи, браншови или други неправителствени организации** - представляват отделни професионални или граждански сдружения и изпълняват различни функции по отношение на дейността на дружествата Лирекс.ком в

съответствие с договорни или други приложими изисквания, които включват задължение за опазване на получената конфиденциална информация.

6.2. Изисквания на заинтересованите страни

В своята дейност дружествата Лирекс.ком се стремят да удовлетворят изискванията на всички заинтересовани страни във връзка с информационната сигурност чрез спазване на правните, законовите, нормативните и договорните изисквания по отношение на:

- защита на търговската информация (съдържанието на търговските договори и досиетата на сделките с клиенти и доставчици; данните, предоставяни от клиентите по търговските взаимоотношения и във връзка със сключените договори);
- опазване на работната документация и техническите архиви (параметрите и структурата на техническите, комуникационните и програмните системи, изградени по договори) на дружествата Лирекс.ком;
- защита на правата върху интелектуалната собственост (авторски права, използване на лицензиран софтуер, други лицензи и патенти);
- защита и конфиденциалност на личната информация;
- други договорни задължения на дружествата Лирекс.ком за информационна сигурност.

Лирекс.ком може да изпълнява своите цели и да има добра корпоративна репутация само ако поддържа коректни отношения и диалог със заинтересованите страни. Съзнавайки това, служителите на дружествата се задължават да спазват строго търговските тайни и поверителността на информацията, предоставени от деловите му партньори в съвместната им работа.

Към подизпълнителите, които дружествата Лирекс.ком ангажират в своите дейности, се предявяват същите задължения, като в договорите или споразумения за поверителност с тях се включват приложимите изисквания за информационна сигурност.

Необходимите външни документи за изпълнение на изискванията за информационна сигурност са включени в Регистър на нормативните актове (RegisterLegInfoSecurity.doc), който периодично се актуализира, като в него, при необходимост, се включват и новите документи, приложими за дейностите на дружествата Лирекс.ком.

До актуалното съдържание на всички нормативни и поднормативни актове (наредби, правилници, постановления и др.) се осигурява достъп в правните информационни системи в Интернет, за които се поддържа абонамент.

7. Система за управление на информационната сигурност

7.1. Обхват на Системата за управление на информационната сигурност

Обхватът на Системата за управление на информационната сигурност (СУИС) в дружествата Лирекс.ком е определен от техния външен и вътрешен контекст; от разбирането на

изискванията на заинтересованите страни и взаимовръзките между дейностите, изпълнявани от дружествата и другите организации.

СУИС се прилага по отношение на:

- **Средства за управление и контрол** – включват цялото оборудване и необходимата за неговото функциониране инфраструктура, като:
  - компютърни системи от всички класове – сървъри, работни станции, преносими компютри;
  - офис оборудване – принтери, копирна техника, факсове и телефони;
  - структурни кабелни системи и активно мрежово оборудване;
  - интранет и интернет оборудване;
  - климатични инсталации за компютърното оборудване;
  - охранителни системи на сгради и помещения;
  - необходимите за нормално обезпечаване на дейността сградни инсталации;
  - сгради и помещения, предназначени за персонала и оборудването.
- **Данни и информация** - обхващат неструктурирани данни и обработена информация, като:
  - файлове и досиета с данни, независимо от формата на съхранение и обмен;
  - информацията, получена след обработка на данни, независимо от формата им на съхранение и представяне.
- **Софтуер** – включва закупен от външни доставчици лицензиран софтуер и самостоятелно разработени програми като:
  - операционни системи и системен софтуер;
  - приложен софтуер.
- **Документи на хартиен носител** – включително документацията на Системата за управление на качеството и информационната сигурност, наръчници за потребителите, договори, указания и процедури.
- **Лица и организации** – служители, доставчици, консултанти, клиенти или други организации, имащи достъп до данни, информация и информационните системи на Лирекс.ком.

7.2. Системата за управление на информационната сигурност в СУКИС

За актуалната редакция и съдържание на процедурата проверете в *LODIS*.

Системата за управление на информационната сигурност (СУИС) в дружествата Лирекс.ком е включена в интегрираната Система за управление на качеството и информационната сигурност (СУКИС) в съответствие със стандартите ISO 9001, ISO/IEC 27001, ISO/IEC 20000-1, ISO 14001, ISO 45001.

Водещата роля и ангажираността на ръководството на Лирекс.ком за създаване, внедряване, поддържане и непрекъснато да подобрява системата за управление на информационната сигурност (СУИС) в рамките на интегрираната СУКИС е отразена в документа LQS Manual.doc.

Основният принцип при управление на информационната сигурност е прилагането на ефективен контрол, който е измерим със стандартите за сигурност и изискванията за съответствие, които са приложими за дружествата Лирекс.ком. Контролът е насочен към постигане на следните изисквания:

- **Поверителност** - Свойството информацията да не се предоставя или разкрива пред неупълномощени лица, служители или процеси.
- **Цялост** - Свойството за опазване на точността и целостта на активи.
- **Наличност** - Свойството за достъпност и използваемост на информацията при заявка от упълномощено лице.

8. Политики за информационна сигурност

8.1. Обща политика за информационната сигурност

Управлението на информационната сигурност в дружествата Лирекс.ком се извършва в съответствие с определената и одобрена от ръководството на Лирекс.ком обща политика в тази област, която:

- е в съответствие с предмета на дейност на дружествата и с краткосрочните и дългосрочни цели на въведената в Лирекс.ком интегрирана СУКИС;
- съдържа ангажименти за изпълнение на всички приложими законови и други договорни изисквания, свързани със сигурността на информацията в дружествата;
- съдейства за непрекъснатото повишаване на ефективността и ефикасността на СУИС.

Политиката по ИС е обявена и разбрана от всички служители на дружествата Лирекс.ком и е на разположение на клиентите, доставчиците и другите заинтересовани страни.

8.2. Общата политика има за цел:

- да осигури непрекъснато функциониране на бизнес процесите в дружествата Лирекс.ком;
- минимизиране на степента на загуби или вреди, причинени от пробиви в сигурността;
- да осигури запазването на конфиденциалността, целостта и наличността на информацията.

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

8.3. Политики за информационната сигурност

В съответствие с общата политика и в изпълнение на изискванията на стандарта ISO/ IEC 27001, ръководството на Лирекс.ком е одобрило набор от политики, които са включени в следните документи от Системата за управление на информационната сигурност:

LSI412	Политика за сигурност в среда на Активна Директория
LSI471	Политики за управление на сменяеми носители
LSI481	Политика за обмен на електронна поща
LSI482	Политика за употреба на виртуални частни мрежи
LSI602	Политика и изисквания към използването на компютърни средства
LSI603	Политика и изисквания към паролите
LSI605	Политика за използване на IP телефония
LSI606	Политика за защита на отдалечен порт за диагностика и конфигуриране
LSI621	Политика за работа чрез отдалечен достъп
LSI622	Политика за използване на безжичен достъп до защитена Интернет зона
LSI704	Политика за криптиране

9. Контрол и преразглеждане

Изпълнението на политиките, включително дейностите на дружествата Лирекс.ком по осигуряване и поддържане на сигурността на информацията в съответствие с изискванията на стандарта ISO/IEC 27001 и приложимите законови и други нормативни актове се контролира, обсъжда и при необходимост преразглежда най-малко веднъж годишно на прегледите от ръководството на СУИС в рамките на СУКИС.

10. Вътрешен и външен обмен на информация

Висшето ръководство на дружествата Лирекс.ком осъзнава, че функционирането на СУИС е зависимо от ефективния вътрешен и външен обмен на информация и е въвело подходящи процеси за обмен на информация, които са описани в документацията на СУКИС.

Процесът на комуникация включва обмена на информация между хората в дружествата, самата информация, получателите на информация и средата, в която я получават.

Определени и оповестени са отговорните длъжностни лица за получаване, документиране и даване на отговор на съответните искания от външни заинтересовани страни, което включва:

- комуникацията при инциденти с информационната сигурност с компетентните органи и организации се извършва от Ръководителя по информационната сигурност;

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

- комуникацията с оторизираните органи по сертификацията на системата по информационната сигурност се осъществява от УПР по СУКИС.

Информация от външните заинтересовани страни, свързани с дейността на дружествата Лирекс.ком се събира чрез кореспонденция, постъпили сигнали, преки контакти, информация от различни медии и др. При необходимост за оповестяване на информация или събития, свързани с дейността на дружествата, след нареждане на ръководството, тя се оповестява на вътрешната интранет система на дружествата Лирекс.ком.

11. Санкции и дисциплинарен процес

При преднамерено и умишлено неспазване на принципите и изискванията на въведените политики или на процедурите и инструкциите за осигуряване и поддържане на сигурността на информацията в дружествата Лирекс.ком се налагат по съответния ред дисциплинарни наказания от Управителите на дружествата на провинилите се служители в съответствие Кодекса на труда, другото приложимо законодателство или се инициира съдебна процедура в зависимост от тежестта на нарушението.

Лирекс.ком	Процедура: Управление на риска	Версия 5
	LSP200	1 от 10

1. История на редакциите

версия	описание на промяната	автор	проверил	утвърдил	дата въвеждане
3	Отразяване на забележките от пресертификационния одит по ISO/IEC 27001:2005	Б.Йорданов	Б.Янчев	Д.Илиева	10.05.2012
4	Въвеждане на изискванията на ISO/IEC 27001:2013	Б.Йорданов	Б.Янчев	*Д.Илиева*	27.02.2015
5	Актуализиране на документите от СУКИС	М.Йончева	П.Димков	Д. Илиева	15.08.2019

2. Предназначение

Процедурата има за цел да осигури и поддържа ефективно управление на риска за информационната сигурност за постигане на целите на въведената СУИС в дружествата Лирекс.ком.

3. Приложимост

Процедурата се прилага при управлението (вкл. идентифициране, оценяване, третиране, приемане, докладване и наблюдение) на риска за информационната сигурност в дейността на дружествата Лирекс.ком.

4. Отговорности

4.1. Висше ръководство

- контролира цялата дейност по управление на риска, като одобрява процедурите и инструкциите от СУКИС;
- одобрява извършената оценка на риска, като утвърждава Протокола за неговата оценка;
- разрешава промените (придобиването или отписването) на активите, включени в СУКИС, с цел намаляване на риска за информационната сигурност.

4.2. Мениджърите/Ръководителите на функционални направления/Управляващи съответната дейност:

- участват в разработването на процедурите и инструкциите от СУКИС по отношение на информационната сигурност;
- предлагат закупуване или отписване на активи, свързано с необходимостта за правилното и безопасно функциониране на направленията/дейностите, които управляват;
- отговарят за организацията на правилното използване на активите, които се намират в ръководените от тях направления/дейности по отношение на сигурността на информацията;
- предлагат на Управителя да наложи по съответния ред дисциплинарни наказания на служителите, които нарушават настоящата процедура или да инициира съдебна процедура в зависимост от нарушението;
- участват в оценката на значимостта на активите и техния риск за информационната сигурност.

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

4.3. УПР по Системата за управление:

- организира дейността на Системата за управление на информационната сигурност като част от Системата за управление на качеството и информационната сигурност Лирекс.ком;
- организира разработването на процедурите и инструкциите от СУКИС по отношение на сигурността на информацията;
- участва в оценката на значимостта на активите и техния риск за информационната сигурност;
- организира изготвянето на отчетите за състоянието на сигурността на информацията като част от отчетите на СУКИС в Лирекс.ком.

4.4. Ръководителят по информационна сигурност:

- организира и контролира цялостната дейност по управление на риска по отношение на сигурността на информацията;
- участва в разработването на процедурите и инструкциите от СУКИС, свързани с информационната сигурност;
- предлага закупуване или отписване на активи, свързано с необходимостта за правилното и безопасно функциониране на СУКИС по отношение на информационната сигурност в Лирекс.ком;
- контролира своевременното вписване на новите активи в съответните регистри и тяхното отписване при изваждането им от употреба;
- определя отговорници за съответните активи, като контролира изпълнението на задълженията им;
- изготвя отчетите, свързани със сигурността на информацията и оценката на риска като част от отчетите на СУКИС в Лирекс.ком;
- предлага на Управителя да наложи по съответния ред дисциплинарни наказания на служителите, които нарушават настоящата процедура или инициира съдебна процедура в зависимост от нарушението;
- организира изпълнението на предписаните превантивни и коригиращи действия от проведени вътрешни и външни одити на СУКИС.

4.5. Служителят по сигурността на класифицираната информация:

- поддържа Плана за физическата сигурност на класифицираната информация в актуално състояние;
- прилага мерките, предвидени в Плана за физическата сигурност на класифицираната информация;
- участва в дейностите по оценка на риска на активите, свързани с обработката и съхранението на класифицираната информация.

4.6. Отговорникът на актив:

- изпълнява изискванията на всички процедури и инструкции по отношение на сигурността на информацията и свързани с активите, за които отговаря или има разрешен достъп;
- при забелязване на инциденти със сигурността на информацията, свързани с активите, след изясняване на проблема и евентуалната причина, незабавно информира Ръководителя по информационна сигурност;
- участва в дейностите по оценка на риска на активите, свързани с обработката и съхранението на класифицираната информация.

5. Процедура

5.1. Общи изисквания

Управлението на риска за информационната сигурност е съобразено с дейностите на дружествата Лирекс.ком, както и с техните външни и вътрешни аспекти и има за цел:

- системата за управление на информационната сигурност да постигне желаните резултати;
- да се предотвратят или намалят нежеланите ефекти от проявата на рисковете, свързани със сигурността на информацията;
- да се постигне непрекъснато подобряване на СУКИС.

Дейностите по управлението на риска и оценка на ефикасността им се отразяват от РИС в ежегодните доклади по сигурността на информацията в дружествата Лирекс.ком

5.2. Оценяване на риска, свързан с управление на качеството и околната среда

Оценката на риска, свързан с управление на качеството и околната среда се извършва посредством SWOT анализ.

5.3. Оценяване на риска за информационната сигурност

В дружествата Лирекс.ком е въведен процес на оценяване на риска за информационната сигурност, който:

- определя контекста и критериите за риска, които включват както критериите за оценяване, така и тези за приемането на риска за информационната сигурност в Лирекс.ком;
- осигурява последвалите оценявания на риска да дават повторяеми и сравними резултати;
- в процеса на оценяване идентифицира рисковете за информационната сигурност, свързан със загуба на поверителността, целостта и наличността на информацията в обхвата на СУСИ и идентифицира собствениците на риск;
- анализира рисковете за информационната сигурност, като оценява потенциалните последствия от осъществяването на рисковете в зависимост от контекста и вероятността тези рискове да се случат и определя нивата на риска;
- оценява рисковете за информационната сигурност като сравнява резултатите от анализа на риска с установените критерии за риск и определя приоритетите за въздействие върху рисковете.

Оценяването на риска е свързано с идентифициране на информационните активи и тяхното значение за обработването, съхраняване и обмена на информация, както и с приложимите законови и други договорни изисквания за информационната сигурност в зависимост от определения вътрешен и външен контекст на Лирекс.нет.

Документацията на процеса за оценяване на риска за информационната сигурност се съхранява съгласно изискванията на СУКИС.

5.4. Идентифициране на информационните активи

В оценката на риска за информационната сигурност се включват тези активи (информационни системи или други активи), при които са възможни последствия като загуба на поверителност, на цялостност и наличност на информацията; както и потенциални щети, пропуснати ползи или неблагоприятно влияние върху бизнеса вследствие на инцидент, свързан с тях.

За целите на оценката на риска, активите може да бъдат групирани по:

- дейности (информационни системи, процеси);
- вид на информационните активи (т.е. хардуер, софтуер, бази данни, записи с информация);
- хора (т.е. персонал, клиенти, доставчици и др.);
- инфраструктура (сгради, офиси, съоръжения).

Идентифицирането на активите, свързани със сигурността на информацията по отношение на вида им, мястото и техните отговорници, се извършва в съответствие с процедура LSP100 "Управление на активите".

5.5. Идентифициране на заплахите и уязвимостите за активите

Примерен списък на заплахите за сигурността на активите в обхвата на СУКИС на Лирекс.ком, по отношение на сигурността на информацията и уязвимостите, които могат да бъдат използвани от тях, е показан в **LSB-200-TRT.**

Списъкът не е изчерпателен и за определени активи при необходимост може да се идентифицират други заплахи и/или уязвимости.

5.6. Приложение на избраната методика за оценка на риска

В избраната методика рисковете за информационната сигурност са функция на:

- вероятността от появата на възможната заплаха, която може да застраши съответните активи и
- влиянието на значимостта на активите и свързаните с тях уязвимости и потенциални нежелани въздействия върху сигурността на информацията, както и съществуващите или планирани защити, които трябва да намалят тежестта на нежеланите въздействия.

За оценка на риска за сигурността на информацията, свързана с дейността на Лирекс.ком, се използва следната формула, която свързва експертните оценки за вероятността за поява на конкретна заплаха с влиянието на значимостта на активите и свързаните с тях уязвимости:

Риск = Вероятност Х Влияние

При определяне на вероятността за появата на определена заплаха се взема предвид следното:

- привлекателността на актива, свързан със заплахата за преднамерена човешка намеса;
- лесното получаване на облаги от преднамерената човешка намеса;
- техническите възможности на реализация на заплахата от преднамерена човешка заплаха;
- периодът от време, в което активът се използва и има нужда от защита.

Вероятността се оценява в съответствие с **Таблица 1:**

Вероятност	*Честота*	*Оценка*
Минимална	До 2 пъти за 5 годишен период.	0,5
Много ниска	2-3 пъти за 5 годишен период.	1
Ниска	До 1 път годишно.	2

Вероятност	Честота	Оценка
Средна	До 2 пъти годишно.	3
Висока	До 1 път месечно.	4
Много висока	Повече от 1 път месечно.	5
Изключително висока	Няколко пъти в рамките на седмица или ден.	6

Влиянието на свързаните с активите уязвимости (технически и нетехнически) се оценява, като се отчита значимостта на съответния актив за сигурността на информацията (определя се от възможните последствия, свързани със загубата на поверителност, цялостност и наличност на информацията при инцидент или от пропуснатите ползи; потенциалните щети или неблагоприятното влияние върху бизнеса). Влиянието се определя експертно и се използват качествени критерии. При определяне на критериите за уязвимост се отчитат всички въведени мерки за защита на оценявания актив, както и адекватността на тези мерки.

Критериите се оценяват в съответствие с **Таблица 2**:

Ниво на влияние	Въздействие върху активите	Оценка
Пренебрежимо	Трудно забележимо влияние.	0,5
Незначително	Не са необходими усилия или средства, за да се възстановят или поправят щетите.	1
Значително	Реални щети, необходимо е усилие/средства, за да се възстанови или поправи.	2
Увреждащо	Щети на репутация или конфиденциалност. Значителни разходи на усилие и/или средства, за да се възстанови или поправи.	3
Сериозно	Продължително отпадане на актив/услуга и/или загуба на свързаност. Компрометирани големи обеми от данни или услуги.	4
Изключително	Отпадане на част от бизнес процес. Невъзможност да се възстанови актив/услуга.	5

За оценката на риска е необходимо съответният актив (или група от активи), като се отчита присъщата му уязвимост, да се съпостави с възможната за него заплаха и отговарящата й уязвимост (от **LSB200-TRT** или друга възможна заплаха).

Заплахите могат да бъдат:

- форсмажорни събития;
- организационни проблеми;
- човешки грешки;
- технически грешки;

- преднамерени, злоумишлени деяния.

Заплахите могат да бъдат случайни или предумишлени. И случайните и предумишлените източници на заплаха трябва да бъдат отчетени и да бъде оценена вероятността за тяхната поява.

Ако за един актив са възможни няколко заплахи или няколко уязвимости, свързани с определена заплаха, то рискът се оценява поотделно за всеки отделен случай. Списъкът със заплахи в LSB200-TRT не е изчерпателен и за определени активи при необходимост може да се идентифицират други заплахи или уязвимости.

Наличието на уязвимост само по себе си не причинява вреда, а трябва да има налична заплаха, която да я използва. При уязвимост, на която не съответства заплаха, не се изисква прилагането на защита, но тя трябва да бъде разпозната и да се наблюдава за промени. Трябва да се отчете, че неправилно въведените, нефункциониращите или неправилно използваните защити могат сами по себе си да бъдат уязвимост.

Нивото на риска се изчислява по скалата на **Таблица 3:**

Ниво на риск	Стойности
нулево	по-малко от 1
ниско	от 1 до 3
средно	от 4 до 6
високо	от 7 до 14
критично високо	от 15 до 19
изключително високо	от 20 до 30

Резултатите от оценката на риска се нанасят в Протокол за оценка на риска (LSB-200-RAR).

Процесът на управление на риска е цикличен процес. Крайният етап се явява начало на нов цикъл на оценка на риска. Новият цикъл се провежда, когато:

а) остатъчният риск не удовлетворява ръководството на дружествата;

б) са настъпили съществени изменения в структурата на активите или са въведени нови информационни системи или активи;

в) е регистриран сериозен инцидент, свързан с информационната сигурност;

г) има промени в приложимата законова или друга нормативна база, променени договорни задължения или промени в социалния климат;

д) изтече една година от предишната оценка на риска.

5.7. Оценка и приемане на риска

Началната оценка за рисковете се прави от работна група под ръководството на Ръководителя по информационна сигурност.

Входящите данни за оценката на риска се получават от отговорниците на активите или техните потребители; от специалистите, които планират активите и ги поддържат, както и от хора, отговорни за охраната на сградите и офисите на дружествата. Друг източник на информация за

оценка на рисковете, са приложимите за дейността на Лирекс.ком законови и други нормативни актове.

Оценката на риска за активите (информационни системи или други активи), които са включени в обхвата на Системата за управление на качеството и информационната сигурност на Лирекс.ком, по отношение на сигурността на информацията, се прави по методиката, посочена в т. 5.5. Ако за един актив са възможни няколко заплахи или няколко уязвимости, свързани с определена заплаха, то рискът се оценява поотделно за всеки отделен случай. За приемливи рискове на активите, свързани със сигурността на информацията, се приемат тези със стойност до 6 включително (средно ниво на риска). Резултатите от оценката на риска се нанасят в Протокол за оценка на риска (LSB-200-RAR). Съветът по сигурност на информацията го разглежда, обсъжда и след приемането му, предлага протокола за одобрение на Управителя на дружествата Лирекс.ком.

Въведените защитни мерки (механизми за контрол), които да бъдат използвани за намаляване на оценените рискове до приемливото ниво, както и мерките, които да не позволяват приемливия риск (със стойност 6) да се увеличи, се включват в Плана за третиране на риска (LSB-200-RTP). За изпълнение на защитните мерки се определя отговорник, изпълнител, както и срок за изпълнение и необходимите ресурси. Въпреки, че 6 е в границите на приемливото (средно) ниво на риск, той се контролира, за да не се допусне неговото нарастване. Планът за третиране на риска се предоставя на собствениците на рисковете за одобрение и след това се утвърждава от Управителя.

За активите с оценка на риска над средно ниво се въвеждат нови мерки за защита и се прави повторна оценка на риска след прилагането на съответната мярка. Този цикъл се повтаря, докато се получат приемливи стойности на остатъчния риск за съответния актив. Нова оценка се прави и когато настъпят съществени изменения в структурата на активите или са въведени нови информационни системи или активи. Предишните оценки на риска се архивират.

При всяка оценка на риска трябва да се използват еднакви критерии и стойности за съответната заплаха или уязвимост, за да има възпризводимост и повторяемост на резултатите.

5.8. Избор на защити, прилагане, проверка и оценка на ефективността

При установяване на риск над приемливия, трябва да се предприемат ефективни и икономични мерки за неговото снижаване и оценка дали резултативният риск е в приемливи граници.

При идентифициране на риск над приемливия, се предприема едно от следните действия:

а) ликвидиране на риска (например, чрез отстраняване на причиняващите го обстоятелства);

б) намаляване на риска (например, чрез използване на допълнителни защитни средства);

в) приемане на риска и разработване на план за действия в обстановка на риск;

г) преадресиране на риска (например, чрез сключване на договор с друга организация за изпълняване на съответната дейност с приемлив риск или за съответната застраховка).

Защитите (механизмите за контрол), въведени след прегледа на анализа на риска, трябва да бъдат подходящи за допълнение на вече съществуващите, за да се избегне излишното дублиране на защити. Проверява се дали избраните защити са съвместими със съществуващите и планираните защити, т.е. избраните и съществуващите защити трябва да бъдат съвместими, тъй като защитата, която не функционира правилно, е източник на възможна уязвимост.

Когато се установи, че вече съществуващите защити не изпълняват своите функции, Ръководителят по информационна сигурност прави аргументирано предложение на Съвета по сигурност на информацията съответната защита да бъде премахната, заменена с друга по-подходяща или да бъде усъвършенствана.

Оценката на ефективността за предприетите защитни мерки за привеждане на рисковете до приемливи нива за Лирекс.ком, се провежда при повторния анализ на рисковете на база получените стойности за тях, като се сравнява планираният остатъчен риск от Плана за третиране на риска с реално отчетения. Ако резултантният риск е по-малък или равен на планирания остатъчен риск, се приема, че мярката е ефективна. В случай на прилагане на неефективна мярка се прави допълнителен анализ за причините за неефективността и се докладва на Съвета по сигурност на информацията.

Пример: *Планиран остатъчен риск след прилагане на защитни мерки – 6. Прави се повторна оценка на риска и се установява, че рискът, след прилагането на мярката, е спаднал до 4.* ***Резултантен*** *риск* ***4*** *е по-малко от* ***планирания остатъчен*** *риск* ***6,*** *от което считаме, че приложените мерки са* ***ефективни****.*

6. Блок схеми

Не се прилага блок-схема за този документ.

7. Термини и съкращения

СУКИС	Система за управление на качеството и информационната сигурност в Лирекс.ком.
СУИС	Система за управление на информационната сигурност в Лирекс.ком.
РИС	Ръководител по информационната сигурност:
Информационна сигурност (сигурност на информацията)	Запазване на поверителност, цялостност и наличност на информацията.
Събитие, свързано със сигурността на информацията	Идентифицирана проява на състояние в система, услуга или мрежа, показваща възможно нарушаване на политиката по сигурност на информацията, пробив на защити или неизвестна до момента ситуация, засягаща сигурността.
Информационен актив	Материалните и нематериалните активи, свързани с информация, които имат полезна стойност за организацията.
Наличност на информацията	Свойството за достъпност и използваемост на информацията при заявка от упълномощено лице.

Поверителност на информацията	Свойството на информацията да не се предоставя или разкрива пред неупълномощени лица, служители или процеси.
Цялост на информацията	Свойството за опазване на точността и целостта на активите.
Заплаха	Потенциална причина за нежелан инцидент, който може да навреди на система или организация.
Уязвимост	Слабост на актив или група активи, която може да бъде използвана от една или повече заплахи.
Риск	Комбинация от вероятността на дадено събитие и неговото последствие.
Анализ на риска	Систематично използване на информация с цел да се идентифицират източниците и да се прецени рискът.
Преценяване на риска	Цялостен процес на анализ и оценяване на риска.
Оценяване (оценка) на риска	Процес на сравняване на оценения риск с дадени критерии за риск, за да се определи неговата значимост.
Остатъчен риск	Рискът, който остава след въздействието върху риска.
Приемане на риска	Решение да се приеме рискът.
Управление на риска	Координирани действия за насочване и контролиране на организацията по отношение на риска.
Риск за сигурността	Фактическо състояние, което създава заплахи за уязвяване на един или няколко информационни актива, което да предизвика тяхното повреждане или унищожаване.
Въздействие върху риска	Процес на подбор и прилагане на мерки с цел изменение на риска.
Собственик на риска	Лице (физическо или юридическо), имащо отговорност и пълномощия да управлява риска.
Лирекс.ком	Дружествата Лирекс БГ, Лирекс БС, Лирекс Хай Тех, Беолик, Лирекс Скопие, Теза

8. Препратки към документи

ID на документа	наименование на документа
LSP100	Процедура: Управление на активите
LSP001	Процедура: Политика и управление на информационната сигурност
LRI002	Инструкция: План за физическата сигурност на националната класифицирана информация
LQS Manual	Наръчник на СУКИС

9. Оценки

На годишния преглед от Ръководството на СУКИС се разглежда и обсъжда доклад от Ръководителя по информационна сигурност с включени актуалната оценка на риска и на ефективността на приложените мерки, както и План за третиране на рисковете с оценка над базовото ниво.

10. Документирана информация

ID на формата	наименование на формата
LSB-200-RAR	Протокол за оценка на риска
LSB-200-TRT	Заплахи
LSB-200-RTP	План за третиране на риска

ЛИРЕКС.КОМ	Непрекъсваемост на бизнес процесите	Версия 4
	LSP900	1 от 17

1. История на редакциите

версия	*описание на промяната*	*автор*	*проверил*	*утвърдил*	*дата въвеждане*
2	Описание на непрекъсваемостта на Външните ИТ услуги	Б.Янчев	Б.Йорданов	Д.Илиева	19.02.2010
3	Отразяване на промени свързани с ISO27001:2013	Б.Янчев	Б.Йорданов	***Д.Илиева***	06.03.2015
4	Актуализиране на документите от СУКИС	П.Димков	Р.Радев	Д.Илиева	28.08.2019

2. Предназначение

Процедурата има за цел да опише планираните дейности за адресиране на заплахите и потенциалните уязвимости свързани със бедствия и аварии и риска който те водят към Лирекс.ком.

Целта на процедурата за управление на непрекъсваемост на бизнес процесите е да гарантира, че всички заплахи със значимо влияние над бизнеса са разгледани и е планирано отстраняването или намаляването на тяхното влияние върху бизнеса на Лирекс.ком.

3. Приложимост

Процедурата се прилага от всички служители в съответствие с изпълнение на изискванията на ISO 27001:2013 за управление на непрекъсваемостта на бизнес процесите.

4. Предпоставки за непрекъсваемост на бизнес процесите

Възстановяването на даден бизнес процес от претърпяно бедствие или авария може да бъде труден и мъчителен процес, който не във всички случаи би довел до стопроцентов положителен резултат. Колкото по-добре са планирани техниките за осигуряване на непрекъсваемост, толкова по-бързо и пълно биха се възстановили бизнес процесите в Лирекс.ком.

Един от начините за подобряване непрекъсваемостта на работата и осигуряване на възможност за възстановяване на дейностите на информационните системи в Лирекс.ком в случаи на природни бедствия е чрез изграждане на резервирани центрове, разделени географски от централните ИТ мощности по такъв начин, че едно и също събитие(бедствие, авария, ИТ злополука), да не може да повлияе на основния и резервния център едновременно.

Целта на центровете за възстановяване след срив е да осуети прекъсванията на обичайните работни процеси в Лирекс.ком и да предпази тези от тях, които са критични за осигуряване на непрекъсваемост на предлаганите услуги, от отрицателните въздействия на сериозни аварии, бедствия, пробиви във сигурността или от други заплахи.

Проактивната оценка на рисковете, правилното им управление чрез прилагане на защитни мерки и периодичен контрол елиминира или драстично намаля рисковете и от там възможността от случване на неблагоприятни за бизнес процесите аварии.

За създаването на центрове за резервиране на основни информационни системи в Лирекс.ком се извърши специализирано изследване, което включва:

- Проучване на информационните системи внедрени в Лирекс.ком и оценката на следните фактори:
  - RTO - Времето, необходимо за да се възстанови достъпността на дадена услуга след съществено прекъсване (бедствие или авария)
  - RPO - Момент във времето, към който трябва да бъдат възстановени данните в системата
  - SLA – договорени нива за наличност
- Изградена е поддържаща инфраструктура за възстановяване след срив и аварии
- хардуерно и софтуерно обезпечаване на информационните системи в случай на срив
- разработена е схема за поддръжка на инфраструктурата и информационните системи за възстановяване след срив и аварии

5. Приоритети за защита

Ръководството на Лирекс.ком определя следните приоритети за защита от бедствия и аварии:

- ERP системи
- CCM - Телефония
- E-mail (Exchange)
- Active Directory
- VPN

В допълнение се включват и:

- Сървъри – хардуер и софтуер
- Техническа документация.

6. Възможни аварии със сериозни негативни последствия върху бизнес процесите

След анализ на бизнес процесите и възможните аварии и бедствия бяха дефинирани следните аварии със сериозни негативни последици:

- Продължително спиране на ел. захранване
- Отказ на система ERP
- Отказ на телефония
- Отказ на E-mail (Exchange)

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

- Отказ на Active Directory
- Отказ на VPN
- Природни стихии и бедствия възпрепятстващи персонала от явяване на работа в работните помещения

Приложения списък не е изчерпателен, а дефинира само системите със сериозни негативни последици. За всяка една услуга описана в LSB-100-RIS са дефинирани схемата и пътищата за възстановяване след срив и аварии.

7. Комуникации

За коректната комуникация в случай на бедствия и аварии са необходими надеждни комуникации. Наличните комуникационни канали са:

- IP телефони използваща
  - Стандартни гласови канали през БТК
  - IP свързаност
  - VoIP трънкове
  - Оптична свързаност с ТТК
  - Интернет свързаност и използване на Cisco IP Communicator
- Мобилни телефони
  - GSM апарати
  - Мобилни gateway
- Електронна поща
- Комуникатори тип messenger
  - Skype
  - Viber

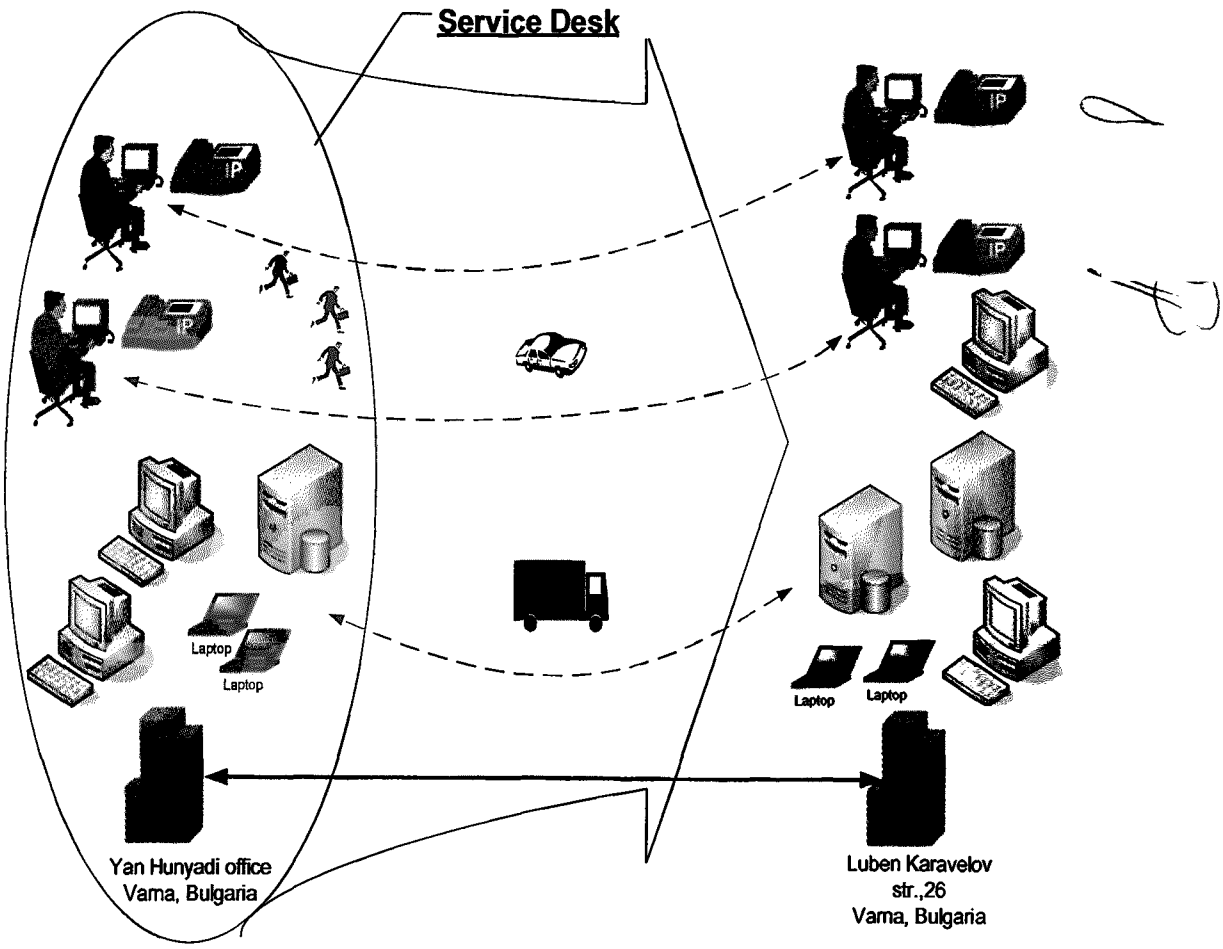
Лицата ангажирани в процеса по осигуряване на Непрекъсваемост на бизнес процесите са дефинирани в LSB900-BCT: "Членове на екипа за гарантиране на непрекъсваемост на бизнес процесите".

Техните основни контакти и поне един резервен контакт са налични в offline копието на GAL което всеки един от тях редовно синхронизира от Lirex GAL в MS Exchange, чрез MS Outlook и ръчна синхронизация на мобилния си телефон

8. Планирана схема за релокация на ресурси

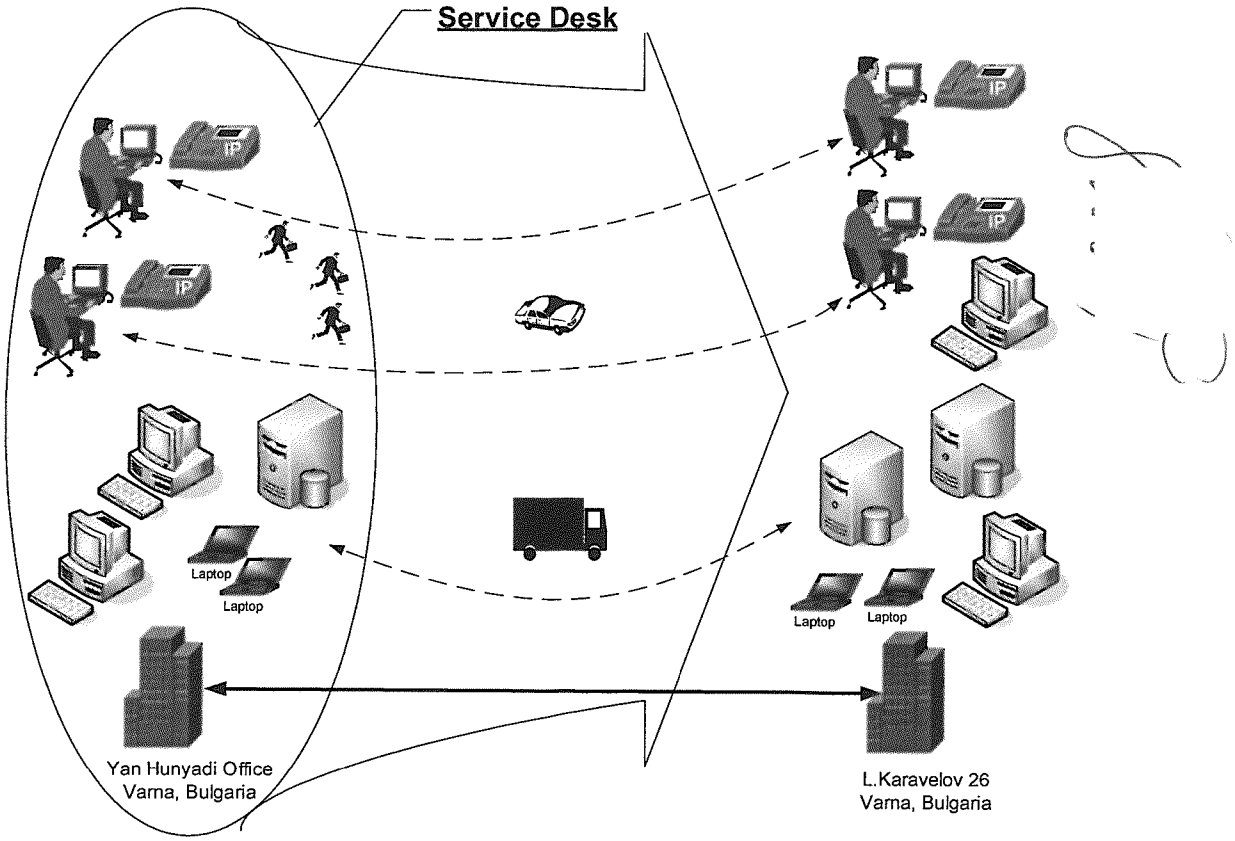
чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

Реалокация на екип по поддръжка на инфраструктурата



9. Непрекъснатост на външни услуги

9.1. Аутсорсинг услуги



Центровете за поддръжка на Аутсорсинг услуги и техните резервни центрове са описани в следната таблица:

Центрове за поддръжка на Външни ИТ услуги	
Основен Център	*Резервен Център*
Варна	Девня
Девня	Варна
Габрово	Варна
София	Варна

9.2. Сервизни услуги

Схемата за непрекъсваемост на сервизните услуги следва таблицата:

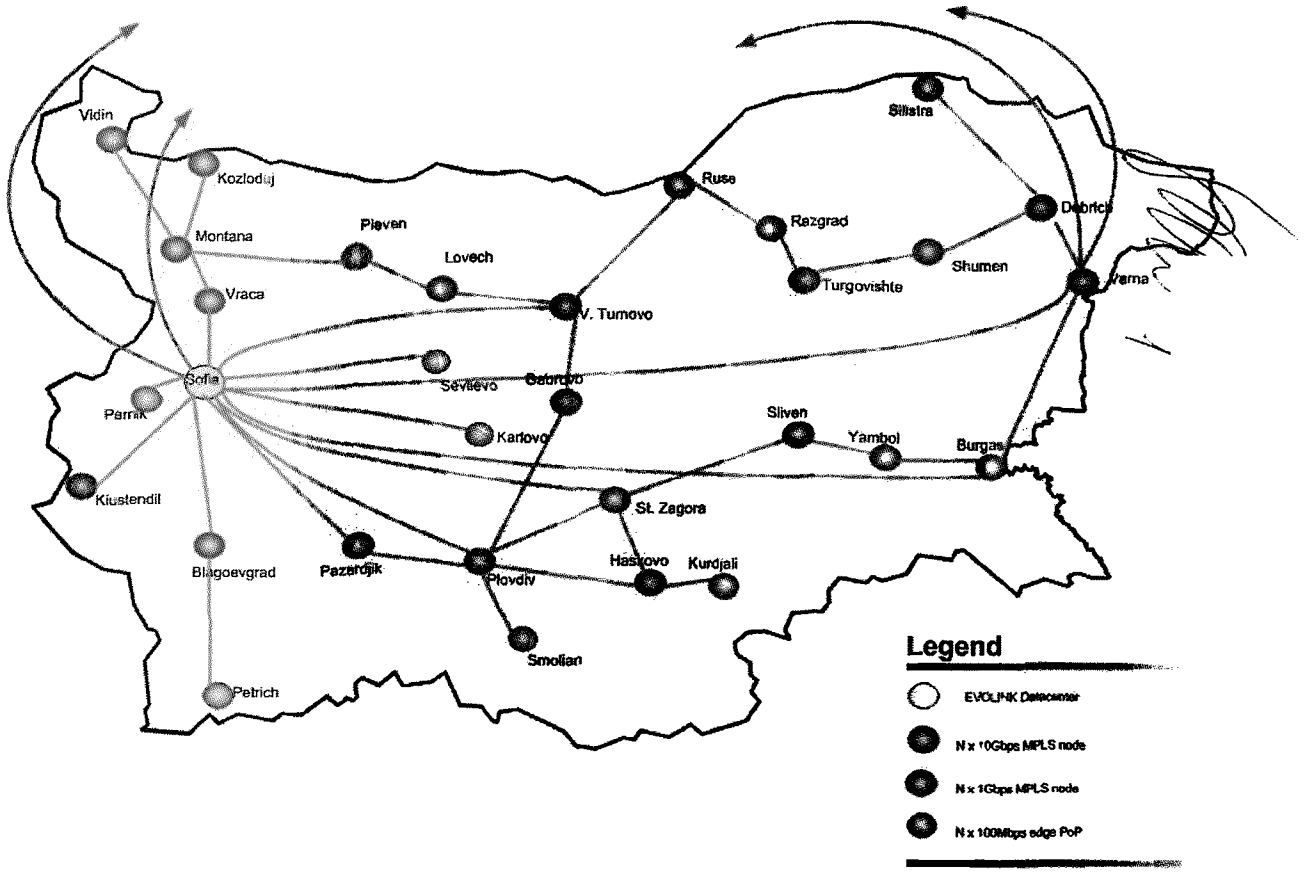
чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

Офис	Основен Резервен Офис	Втори резервен офис
Офис бл.302	офис бл.9	офис бл.54А
Офис бл.306	офис бл.54А	офис бл.9
Офис бл.9	офис бл.302	офис бл.54А
офис Козлодуй	Офис бл.302	Офис Габрово
Офис Габрово	Офис Стара Загора	Офис Русе
Офис Пловдив	Офис бл.302	Офис Стара Загора
Офис Бургас	Офис Варна	Офис Стара Загора
Офис Варна	Офис Русе	Офис Бургас
Офис Русе	Офис Варна	Офис Габрово
Офис Стара Загора	Офис Габрово	Офис Пловдив
Офис Плевен	Офис Габрово	Офис бл.306

9.3. Интернет услуги

Графично представяне на мрежата:

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679



Всички опорни възли в мрежата са свързани с повече от една връзка към мрежата.

Техническите възли в основните за компанията населени места – София, Пловдив, Бургас и Варна са свързани чрез три трасета към националната мрежа.

Международна свързаност

Международната Интернет свързаност се осигурява чрез директна свързаност към два международни оператора, като всяка от връзките се терминира в различен технически възел на мрежата на Лирекс Нет.

Чрез всяка от международните връзки може да се осигурява Интернет капацитет до всяка точка от мрежата на Лирекс нет.

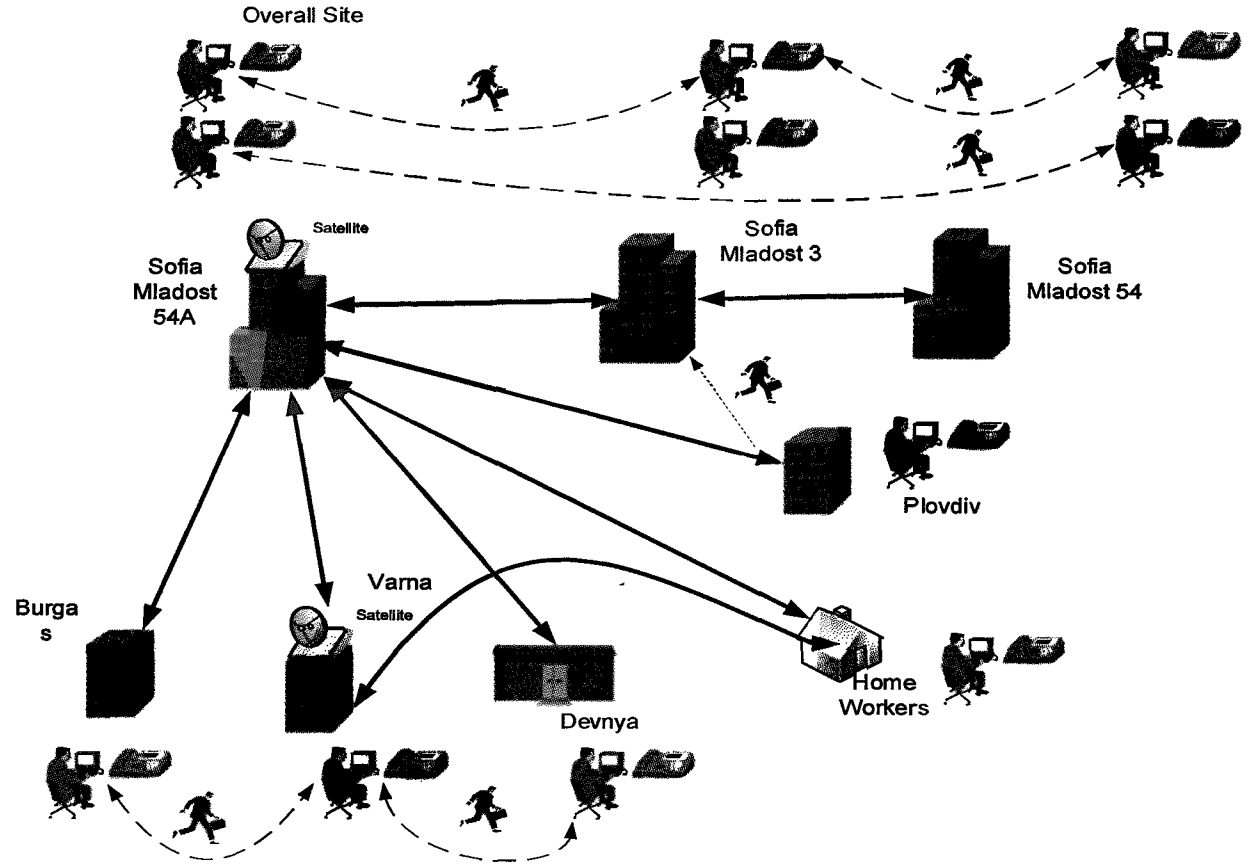
Доставчик на международна Интернет свързаност	Тип на услугата	Точка на свързване с мрежата на Лирекс нет	Тип на връзката	Резервираност
Rom Telecom	Global IP Transit	VRN2, гр. Варна	Nx 1Gbps	Да. Защитено резервирно трасе на доставчика до глобалната му мрежа.
Telia Sonera Internationa Carrier	Global IP Transit	SOF2, гр. София	Nx 1Gbps	Да. Защитено резервирно трасе на доставчика до глобалната му мрежа.

9.4. Резервираност на технически възли

Град	Основен технически възел	Резервираност на захранването	Резервираност на мрежовата свързаност	Резервен технически възел	Резервираност на захранването	Резервираност на мрежовата свързаност
София	SOF2 – ул. Акад. Г. Бончев, бл. 25А	2N – APC UPS, Diesel Generator	Множество директни оптични връзки, Множество MAN връзки	SOF1 – жк. Младост 1, бл. 9	UPS, Mobile Diesel Genrator	Директна оптична връзка до SOF2, MAN връзки
Пловдив	PLD1 - бул. "Христо Ботев" № 92В,	UPS, Mobile Diesel Genrator	Множество директни оптични връзки, Множество MAN връзки	ул. "Райко Даскалов" № 68	UPS	MAH връзки до PLD1
Варна	VRN2 – Христо Ботев 92В	UPS, Mobile Diesel Genrator	Множество директни оптични връзки, Множество MAN връзки	VRN1 – ул. Л. Каравелов 26	UPS	Директна оптична връзка до VRN2, MAN връзки
Бургас	BGS1 -	UPS, Mobile Diesel Genrator	Множество директни оптични връзки,	BGS2 – хл. България	UPS	Директна оптична връзка до BGS1,

Град	Основен технически възел	Резервираност на захранването	Резервираност на мрежовата свързаност	Резервен технически възел	Резервираност на захранването	Резервираност на мрежовата свързаност
			Множество MAN връзки			MAN връзки

9.5. Схема за релокация на персонала



10. Възстановяване след сривове и аварии

10.1. Процеси по планирането на възстановяването след аварии и сривове

- Поддръжка от висшето ръководство и участието му в процеса
- Планиране и документиране на процесите по възстановяване
- Одобрение от ръководството и обнародване на плана
- Тестове, поддръжка и ревизии на планирането

- Обучение
- Контролиране и одитиране
- Осигуряване на архиви
- Наличието на резервен център – Disaster Recovery Center
- Планиране на възстановяването след срив
- Анализ на въздействието върху ежедневните операции

10.2. RTO & RPO

За определяне на целите на сценариите за възстановяване след срив се ползва класификацията на съществените прекъсвания и свързаните с тях загуби на данни и показателите за възстановимост на системите:

- **Recovery Time Objective (RTO):** Времето, необходимо за да се възстанови достъпността на дадена услуга след съществено прекъсване (бедствие или авария). Обхваща периода от момента на обявяване на бедствено положение до активирането на резервната система, ако такава е налична. При липсата на резервна система, периодът се удължава до момента, в който се възстанови достъпността на услугата, предоставяна от основната система.
- **Recovery Point Objective (RPO):** Момент във времето, към който ще бъдат възстановени данните в системата. Покрива периода назад във времето от обявяване на бедствено положение до момента, към който имаме данни с ненарушен интегритет. Колкото по-малък е този период, толкова по-малки загуби на данни ще претърпи организацията.

Описание на конкретните RTO и RPO могат да бъдат намерени в регистъра на вътрешните системи – LSB100-RIS.

Схемата за архивиране и възстановяване съобразно дефинираните RTO & RPO може да бъде намерена в LSP440 - Процедура: „Архивиране и възстановяване на информацията" и LSB440-BUS - Спецификация на архивите.

Виртуализация и нейната наличност може да бъде намерени в LSP420 Хелпдеск процедура и LSP431 - Работа в тестова среда

Детайли относно наличността на архивите и мониторинг на дейностите по архивиране могат да бъдат намерени в „Lirex.comBackupChecklist" - Чеклист на архивите

Детайли за инфраструктурата в център за възстановяване могат да бъдат намерени в LSP300 - Управление на физическата сигурност на инфраструктурата

10.3. Максимална продължителност на прекъсване за различните режими на работа и гарантирана достъпност на услугата или системата

SLA (%)	24x7		24x6		14x5	
	за месец	за година	за месец	за година	за месец	за година
99	7,3 ч.	3,7 дни	6,3 ч.	3,1 дни	3,0 ч.	1,5 дни
99,5	3,7 ч.	1,8 дни	3,1 ч.	1,6 дни	1,5 ч.	18,3 ч.
99,8	1,5 ч.	17,5 ч.	1,3 ч.	15,0 ч.	36,6 мин.	7,3 ч.
99,9	43,8 мин.	8,8 ч.	37,6 мин.	7,5 ч.	18,3 мин.	3,7 ч.
99,99	4,4 мин	52,6 мин.	3,8 мин.	45,1 мин.	1,8 мин.	21,9 мин.
99,999	26,3 сек.	5,3 мин.	22,6 сек.	4,5 мин.	11,0 сек.	2,2 мин.
99,9997	7,9 сек.	1,6 мин.	6,8 сек.	1,4 мин.	3,3 сек.	39,4 сек.

Времетраенето на прекъсванията е дефинирано за отделен случай. За изискванията към незначителните прекъсвания значение имат и допълнителни показатели (брой и продължителност на отделните прекъсвания). Тези показатели оформят общата допустима продължителност на прекъсванията за определен период от време – например, месец или година.

Посочените лимити за прекъсвания са максимално допустимата продължителност за съответната система и категория. Например, определено е, че максимално допустимото съществено прекъсване за критична за бизнеса система е 8 часа. Всяко прекъсване в такава система за повече от 10 минути, без значение каква е причината за него, следва да бъде третирано като съществено прекъсване.

Посоченото времетраене не е абсолютна величина, а трябва да се отчита дали инцидентът е възникнал през работното време или не. Сравнително малко са системите, които трябва да работят непрекъснато и често пъти се изисква висока степен на достъпност само в рамките на работното време

Описание на конкретните SLA и времена за работа на системата (Window of Service) могат да бъдат намерени в регистъра на вътрешните системи – LSB100-RIS.

11. Сигурност на информацията

Сигурността на информацията в процеса на осигуряване на непрекъснатост на дейностите касае е от особено значение, тъй като в момента на опитите на една организация да се справя с

кризисни ситуации контролите въведени от СУКИС могат да бъдат прескочени волно или неволно от персонала.

В някой случаи някои от контролите няма да бъдат налични и е възможно да се появят потенциални уязвимости.

От тази гледна точка при засягане на единични услуги от авария, бедствие или срив след възстановяването им следва да се проведе повторен анализ на риска за тях, както и Penetration test, като най-реалистичен подход за проверка на системи и услуги.

Ако са засегнати повече от 2 критични услуги или при определяне от екипа на значително събитие се извършва повторна цялостна оценка на риска и тя се представя на ръководството.

В случай на отпадане на услуги по контрол на крайните клиентски машини или самите машини Хелпдеск звеното и ръководителя по информационна сигурност следва да проверят за наличието на отклонение от конфигурацията.

В процеса на планира и възстановяване всички политики за сигурност описание или реферирани в LSP001 следва да се спазват стриктно и безусловно.

В случай че дадена политика не може да бъде спазена за възстановяване на система/услуга или бизнес процес то това трябва да премине през одобрение от Ръководител по информационна сигурност, който ако касае критична система трябва да го синхронизира с висшето ръководство на Лирекс.ком.

Правилата на СУКИС за документиране, осигуряване на записи и проследи мост важат с пълна сила и за процесите по възстановяване след срив и аварии.

Контрола по отношение на информационната сигурност е възложен на ръководителя по информационна сигурност

След срив на дадена система паролите на административен достъп следва да бъдат сменени, тъй като срива може да бъде опит за скриване на атака към тези специфични акаунти. Препоръчва се смяната и на паролите на ключовите потребители.

Одитните следи трябва да бъдат внимателно анализирани от ръководителя по информационна сигурност и от ръководителя на ИТ звеното.

Процеса по извършваме на детайлна проверка за причините на срив или авария се адресира чрез така наречения - Root Cause Analysis. Процеса по анализа включва експерти в дадената ИТ област и експерти в областта на анализ на бизнес процесите.

RCA процеса е свързан с дейностите на Хелпдеск звеното. Детайли за RCA се описват в шаблона LSB420-RCA.

12. Рамка за планиране на непрекъснатостта на дейността

Процеса по планиране и документиране на процесите по възстановяване включва следните аспекти на непрекъснатост на дейностите

- Поддръжка от висшето ръководство и участието му в процеса
- Одобрение от ръководството и обнародване на плана
- Референции към процеси, процедури и учения
- Планиране и документиране на процесите по възстановяване
- Тестове, поддръжка и ревизии на планирането
- Анализ на риска
- Обучение
- Контролиране и одитиране
- Осигуряване на архиви
- Наличието на резервен център – Disaster Recovery Center
- Анализ на въздействието върху ежедневните операции

Планирането на процесите по възстановяване касае множество аспекти на функциониране на бизнеса на Лирекс.ком. Свързан е с множеството системи и активи в Лирекс.ком и с мерките за защитата им. От тази гледна точка множество документи и процеси са свързани с методологията за планиране на непрекъснатостта на дейността. Част от тях са:

- Политика за Информационна Сигурност – LSP001
- Управление на активи – LSP100
- Управление на риска – LSP200
- Каталог на услугите – LSB100-RIS
- Политика за архивиране и възстановяване – LSP440
- Хелпдеск процедури, в това число и мониторинг на инфраструктурата.

13. Проверяване, поддържане и повторно оценяване на плановете за непрекъснатост на дейността

Процеса по възстановяване след срив и аварии и осигуряване на непрекъснатост на дейността на Лирекс.ком се проверява регулярно.

Назначените проверки са:

- Планови одити
- Планирани действия – съгласно LSB900-BCP "План за непрекъсваемост на бизнес процесите" – Изготвя се от Ръководителя на ИТ звеното
- Симулации на аварии
- Тестово възстановяване на системи и услуги

В случай на възникване на инциденти с влияние върху бизнес процесите Ръководителя по Информационна сигурност алармира екипа по оценка на бизнес процесите и собствениците на услугите които са афектиране. В случай не не-ефективни мерки за защита или потенциални

възможности за подобряване на плана за действия се прави оценка на въздействието, риска и се прилагат.

Всяка една проверка съдържа оценка на действията и подобряване на процедурите и процесите.

Информационната сигурност и оценката на риска е неразделна част от гореописаните процеси. Оценката на риска е описана в детайли в LSP200 – Управление на риска, а регистъра на рисковете се поддържа в Интранет Портал на Лирекс.ком.

14. Отказоустойчивост /Redundancy/

За гарантиране на отказоустойчивост и възможност за възстановяване при сривове и аварии се използват следните технологии:

- Високо скоростна и надеждна свързаност
- Надеждни хранилища за данни
  - RAID 1, 5 или по-надежден базиран на технологии за дискови масиви
  - Споделени дискови масиви работещи както по FiverChannel така и по iSCSI
  - Преносими медии
- Надеждна сървърна инфраструктура
  - Хардуерни платформи базирани на intel и AMD
  - Достатъчно процесорна мощ и ресурси като памет и мрежови интерефейс –в детайли идентифицирани в план за управление на капацитета
  - Виртуализация и независимост
- Архиви
  - Архиви на лентови и дискови системи
  - Контролиране на архивните копия съхранявани отдалечено

Основните приоритети към отказоустойчивост са защита на данните, тяхната конфиденциалност, наличност и цялостност/Confidentiality, Availability, Integrity/.

Основните приоритети за защита на услуги и тяхната планирана отказоустойчивост са:

- Виртуализация и независимост от хардуерната платформа, използване на споделен дисков масив, 2 независими оптични пътя до дисков масив, 2 отказоустойчиви

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

FiberChannel switch-ове, 2 мрежови комутатора, архиви на ниво виртуална машина и на ниво бази данни.

- Услуги използващи тази отказоустойчивост са
  - ERP системи
  - CCM – Телефония – използва виртуална инфраструктура
  - Active Directory
- Услуги използващи други средства за отказоустойчивост са
  - E-mail (Exchange) – виртуализация, отказоустойчивост на ниво Exchange, RAID5 за защита на данни, 2 независими мрежови комутатора
  - VPN – използва 3 независими устройства (2 в София и 1 във Варна), които използват различни домейн контролери за автентикация и DNS сървъри на тях.

Описание на необходимите SLA и времена за работа на системата(Window of Service) откъдето произтича и необходимостта от осигуряване на отказоустойчивост могат да бъдат намерени в регистъра на вътрешните системи – LSB100-RIS

15. Блок схеми

Не се прилагат блок схеми.

16. Термини и съкращения

ИС	Информационни Системи
DRC	Виж Disaster Recovery Center
Disaster Recovery Center	Център за възстановяване след аварии
Recovery Time Objective (RTO)	Времето, необходимо за да се възстанови достъпността на дадена услуга след съществено прекъсване (бедствие или авария)
Recovery Point Objective (RPO)	Момент във времето, към който ще бъдат възстановени данните в системата
BM	Виртуална Машина
Business Continuity Planning (BCP)	Концепция, използвана за създаване и валидиране на логистичен план за частично и цялостно възстановяване на организация след срив в системата или природно бедствие.

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

Backup	Процес на резервиране, при който се прави копие на данни, така че те да могат да се използват за възстановяване на системата след загуба на данни или несъстоятелност.
RAID	Процедура на логическо обединяване на два или повече „твърди“ диска в масив, с цел постигане на по-голяма производителност и по-голям капацитет за съхранение на данни.
HVAC	„Отопление, вентилация и климатична инсталация". Климатична инсталация за контрол и регулация на големи индустриални и офис сгради, където влажността и температурата са от изключително значение.
Лирекс.ком	Дружествата Лирекс БГ, Лирекс БС, Лирекс Хай Тех, Беолик, Лирекс Скопие, Теза
GAL	Global Address List – списък с контактите и детайли за служители на Лирекс.ком свързани с електронна поща, позиция, телефони, йерархия, офис, web site в Лирекс и много други
Offline GAL	GAL което е наличен и при отпадане на централната сървърна инфраструктура и/или свързаността. Поддържа се от MS Outlook и всички устройства които комуникират с MS Exchange 2007.

17. Препратки към документи

ID на документа	*наименование на документа*
LSP200	Процедура: “Управление на риска”
LSP100	Процедура ”Управление на активите”
LSP001	Процедура ”Политика и управление на информационната сигурност”
LSP440	Процедура: „Архивиране и възстановяване на информацията”
LSP300	Процедура: „Управление на физическата сигурност на инфраструктурата”
LSI431	Инструкция: „Работа в тестова среда
LSI901	Инструкция: „Действия при бедствия или аварии”

18. Оценки

За актуалната редакция и съдържание на процедурата проверете в *LODIS*.

Оценките, свързани с изпълнението на дейностите по настоящия документ, се представят на Годишния преглед от ръководството.

19. Документирана информация

ID на формата	*наименование на формата*
LSB900-BCP-YYYY	План за непрекъсваемост на бизнес процесите
LSB900-BCT	Членове на екипа за гарантиране на непрекъсваемост на бизнес процесите
LSB-100-RIS	Каталог на услугите

ЛИРЕКС.КОМ	Управление на капацитета	Версия 4
	LSP702	1 от 19

1. История на редакциите

версия	описание на промяната	автор	проверил	утвърдил	дата въвеждане
2	Въвеждане на изискванията на ISO/IEC 20000:2005	Св.Манев	Б.Янчев	Д.Илиева	17.02.2010
3	Отразяване на промени свързани с ISO27001:2013	Б.Янчев	Б.Йорданов	*Д.Илиева*	06.03.2015
4	Актуализиране на документите от СУКИС	Д.Василев	Р.Радев	Д.Илиева	28.08.2019

2. Предназначение

Процедурата има за цел да въведе изисквания към сигурността и правилното използване на информационните ресурси, като определя правилата за използването им и прогнозира бъдещите изисквания по отношение на техния капацитет, за да се гарантира изискваната производителност на информационните системи и наличност на услугите в дружествата Лирекс.ком и при техните клиенти.

3. Приложимост

Процедурата е задължителна за всички служители, които имат и носят отговорност за планиране, внедряване и поддръжката на системите на дружествата Лирекс.ком, свързани с корпоративната мрежа, съхраняващи информация за тези дружества или служещи като средство за предоставяне на услуги на клиенти

4. Отговорности

4.1. Управителят:

- одобрява вътрешнофирмената политика за управление на капацитета и налага по съответния ред дисциплинарни наказания на служителите, които нарушават настоящата инструкция;
- извършва преглед и съгласува годишните планове за управление на капацитета във вътрешно-фирмен аспект и за функционалните направления, предоставящи външни ИТ услуги.

4.2. Ръководител на направление/ИТ мениджър:

- Изготвя и води годишен план за управление на капацитета, съобразно политиката и изискванията към планирането и управление на капацитета, посочени в текущия документ;
- На годишния преглед на Ръководството представя и съгласува изготвените планове за управление на капацитета;

- Отговара за обезпечаването на необходимия капацитет на системи и услуги за осигуряване на ефективно и качествено функциониране в съответствие с изискванията на СУКИС.

4.3. Отговорник на предоставяната услуга

- Отговаря за реализацията и контрола на управлението на капацитета за всяка конкретна предоставяна на клиент външна ИТ услуга.
- Съгласува особеностите по планиране и реализиране управлението на капацитета за конкретнта ИТ услуга с Ръководителя на съответното направление.

5. Политика и изисквания към планирането и управлението на капацитета

5.1. Обща цел за управление и планиране на капацитета

Основната цел на управление на капацитета е да се осигури ценово ефективен ИТ капацитет така, че винаги да съществува и да е подходящ за текущите и бъдещи идентифицирани бизнес нужди на дружествата Лирекс.ком.

5.2. Основни ползи от управлението на капацитета

- Повишена ефективност.
- Намаляване на рисковете.
- По-точни прогнози.
- Полезна стойност към жизнения цикъл на приложенията.

5.3. Критични фактори за успеха при планиране на капацитета

- Точни бизнес прогнози.
- Знания за ИТ стратегиите и плановете и че тези планове са точни.
- Едно разбиране за текущите и бъдещи технологии.
- Разбирането да се демонстрира ефективност по отношение на цена.
- Взаимодействието с други ефективни процеси по управление на услугите.
- Възможността да се планира и внедрява подходящия ИТ капацитет, който отговаря на бизнес нуждите.

6. Планиране и управление на капацитета

На вътрешно-фирмено ниво планирането и управлението на капацитета се извършва на годишна база чрез изготвяне на план за управление на капацитета на ресурсите на вътрешните системи (LSP702-SCP), описани в Регистъра на вътрешните услуги LSB-100-RIS. За съставяне на вътрешно-фирмения план за управление на капацитета на системите се ползва посочената в LSB-100-RIS информация за текущия капацитет на системите.

Планът се изготвя от ИТ мениджъра и се съгласува с Ръководителя по Информационна Сигурност.

За цялостното управление на капацитета на всяка една типова услуга, на годишна база или извънредно по искане на Ръководството, съгласно приложената бланка LSP702-SCP, се изготвя общ план за управление на капацитета, който се води от ръководителя на направлението, отговарящ за предоставяне на конкретния тип услуга. Като обща отправна точка в процеса на изготвяне на този план се ползват препоръките от преходната точка в документа – *„Политика и изисквания към планирането и управлението на капацитета"*.

Целта на изготвяне на общия план за управление на типовата услуга е да се гарантира, че доставчика на услугата разполага с достатъчно капацитет да посрещне текущото и договорено за в бъдеще търсене, породено от потребностите на бизнеса и клиентите.

В изготвянето на общия план за управление на услугата се взимат предвид следните аспекти:

- текущите и прогнозни изисквания за капацитета и експлоатационните характеристики;
- определените срокове, прагове и разходи за подобрения и оптимизиране на услугата;
- оценката на ефекта от очакваните подобрения и оптимизиране на услугата, потенциалните заявки за промяна, нови технологии и техники свързани с капацитета;
- данните и процесите, които да дадат възможност за прогнозен анализ;
- прогнозното въздействие от външни промени (например законодателни).

Като част от общия план за управление на капацитета на всяка типова услуга, ръководителят на направлението, пряко отговорен за предоставянето й, определя измерителите или метриките за количествено измерване на ресурсите, ангажирани в реализирането на услугата.

Управлението на капацитета за конкретна услуга предоставяна на конкретен клиент, въз основа на сключен договор и/или SLA, се изпълнява текущо в плана за управление на конкретната услуга, съобразно препоръките на процедура LPP013 „Управление на външни ИТ услуги" и съобразно утвърдения модел LPN002 „План за управление на външна ИТ услуга".

Реализацията и контрола се възлагат на отговорника на предоставяната ИТ услуга от ръководителя на съответното направление.

Процедурите, методите и техниките за измерване и наблюдение на характеристиките на капацитета за типовите услуги се прилагат при управлението на капацитета за всяка конкретна предоставяна услуга.

Количественото измерване на ресурсите необходими за поддържане на услугата се извършва регулярно, като се документира със съответните записи по качеството.

При приключването на изпълнението на дадена услуга или минимум на годишна база се извършва отчитане на изразходвания капацитет за съответната услуга с цел да се анализира и определи ефикасността на използването на капацитета и да се направи по-точно планиране на бъдещия капацитет, съобразено с тенденциите за растеж и изискванията на клиентите. Резултатите от отчитането на използвания капацитет по услуги се включват в годишния доклад на всяко от направленията.

Веднъж годишно или при внедряване на нова услуга се прави цялостен анализ и оценка на капацитета на определен ресурс или ресурси. Като резултат от анализа може да се достигне до следните два момента:

- оптимизиране на текущия ресурс;
- добавяне и увеличаване на общия максимален капацитет на ресурса.

7. Основни принципи при управлението на капацитета

7.1. Ключови индикатори за управление на производителността

7.1.1. Предвиждане на ресурсите

- Предвиждане за ресурсните изисквания за производителност във времето.
- Точни предвиждания за тенденцията в натоварването на ресурсите.
- Включване на бизнес плана в процеса на планиране на капацитета.
- *Технологии*
- Способността за наблюдаване производителността и пропускливостта на всички услуги и компоненти по подходящ начин.
- Внедряването на нови технологии в действие нарушавайки бизнес изискванията (време, цена и функционалност).
- Използването на по-стари технологии да не застрашава общото удовлетворяване (SLA) на услугата, дължащо се на проблем с поддръжката или производителността.
- *Ценова ефикасност*
- Едно намаляване при паническо купуване.
- Без значение за капацитета, което не може да се оправдае с езика на бизнеса.
- Точно предвиждане на планираните разходи.

7.1.2. Планиране и въвеждане на подходящи ИТ капацитети, за да удовлетворят бизнес нуждите

- Намаляване на инцидентите дължащи се на лоша производителност.
- Намаляване на загубата на бизнес, дължащ се на недостатъчен капацитет.
- Въвеждане на нови услуги, които да удовлетворяват изискванията за ниво на услугата (SLR).

7.2. Възможни проблеми при управление на капацитета

- Надвишаване на очакванията.
- Влияние от доставчика.
- Липса на информация.
- Сложност на усилията в разпределена среда.
- Сложност при проектирането и изпълнението на мониторинга.

7.3. Инструменти за управление на капацитета

- Инструменти за мониторинг.

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

- База данни за управление на капацитета (CDB).
- План за капацитета.
- Връзки към CDB.
- Инструменти за моделиране на трендовете.
- Инструментариум за предвиждания.
- Инструменти за настройки.

7.4. Входове и изходи при управление на капацитета

7.4.1. Входове:

- Технология.
- SLA, SLR и Каталог на услугите.
- Бизнес план и стратегия.
- ИС/ИТ план и стратегия.
- Бизнес изисквания и обеми.
- Оперативен план.
- Развитие и планове и програми за развитие.
- По нататъшен план за промени.
- Инциденти и проблеми.
- Преглед на услугите.
- SLA нарушения.
- Финансови планове.
- Бюджети.

7.4.2. Изходи:

- План за капацитета.
- База данни за управление на капацитета (CDB).
- Базова линия и профили.
- Гранични стойности и аларми.
- Доклади за капацитета (регулярни, специални и изключения).
- SLA и SLR препоръки.
- Остойностяване и препоръки за таксуване.
- Про-активни промени и подобрения за услугите.
- Ревизиране на оперативния план.
- Ефективни прегледи.
- Доклади от одити.

7.4.3. Дейности:

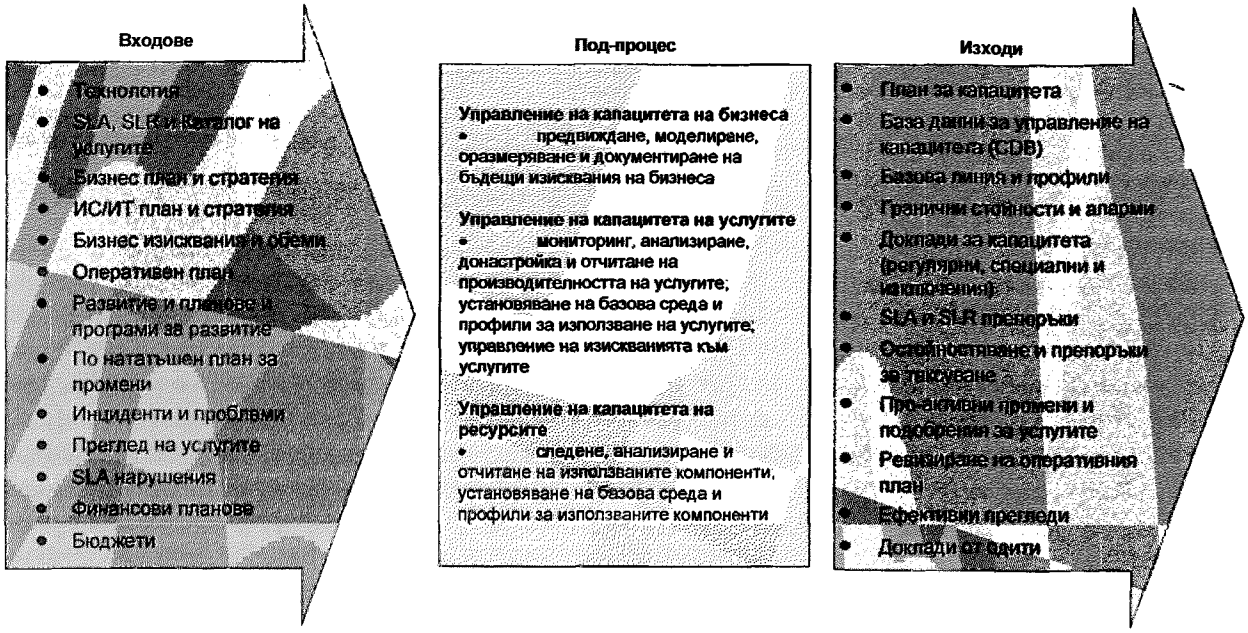
- Мониторинг.
- Анализи.
- Настройки.
- Внедрявания.
- Съхраняване на данните от управление на капацитета.
- Управление на търсенето.

За актуалната редакция и съдържание на процедурата проверете в *LODIS*.

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

- Моделиране.
- Оразмеряване на приложение.
- Продуктивност на плана за капацитета.

Диаграма за входовете и изходите при управление на капацитета



7.4.4. Описание на входа и изхода при управление на капацитета

Интерфейс	Описание
Технология (**Technology**)	Технологията влияе при управление на капацитета по два начина. Първия, технологичните подобрения позволяват управлението на капацитета да се обнови до по-голям капацитет, по-бързи ресурси и така да се предпази или реши от проблеми с капацитета. По същото време, технологията дава възможности да се мотивират желания за нови услуги и нови характеристики, които могат да намалят влиянието на капацитета. Управлението на капацитета трябва непрекъснато да оценява възможностите за технологични подобрения. Управлението на капацитета трябва също да валидира, че всяка заявка за промяна на конфигурацията правилно се адресира и към оценка на капацитета.

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

Интерфейс	Описание
Споразумение за ниво на услугите, изисквания за услугите и каталог на услугите **(SLAs, SLRs and Service Catalog)**	Споразумението за ниво на услугите и изискванията им дефинира договорената услуга, според сключения контракт. Управлението на капацитета трябва да прегледа всяко предложено споразумение, за да се осигури, че дефинираните метрики могат да се наблюдават и могат да се постигнат по най-ефективния начин. Каталога на услугите, впоследствие определя договорения график и наличните услуги.
Бизнес планове и стратегия **(Business plans and strategy)**	Управлението на капацитета се изисква, за да се оценят бизнес плановете и стратегията и да се определят прогнозите за капацитета.
ИС/ИТ планове и стратегии **(IS/IT plans and strategy)**	ИС /ИТ отдела често определят стратегическите цели като миграция към нова архитектура, ново средство или въвеждане на нова технология. Управление на капацитета е отговорен за оценка на тези планове и произлиза прогноза за капацитета
Бизнес изискания и обеми **(Business requirements and volumes)**	Тези входове определят текущите нужди на бизнеса. Управлението на капацитета е отговорен за внедряване на мониторинг на записите с текущото използване, от което трябва да произлезе трендлинията, от която да се предвиди бъдещото нарастване.
Оперативни планове **(Operational schedules)**	Оперативните планове са едновременно важни за проверка за споразуменията за услугите и за балансиране на търсенето. Оперативните планове трябва да включват часовете, които една услуга се предлага също както и договорката за планирани профилактики. Баланса на търсенето използва оперативните планове, когато търси възможност да мигрира дейностите извън пиковите часове.

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

Интерфейс	Описание
Развитие и планове и програми за развитие **(Deployment and development plans and programs)**	Плановете за развитие, по подобие на бизнес и ИТ планове, трябва да направят прогноза за бъдещите изисквания за капацитета.
Бъдещи планове за промени в конфигурацията **(Forward Schedule of Change)**	Бъдещи планове за промени в конфигурацията са всички планирани промени, услугите, които ще бъдат повлияни, както и договореното време определено за планирана профилактика. Управлението на капацитета е отговорно за оценка на всяка заявка за промяна по конфигурацията така, че да се провери дали има достатъчен или да препоръча промяна на RFC, който ще преодолее предвидения проблем с капацитета.
Инциденти и проблеми **(Incidents and Problems)**	Инцидентите и проблемите са обратна връзка в процеса на управление на капацитета, когато ескалират към него, за да се изследват. В допълнение може да се каже, че управлението на инцидентите и проблемите ще използват базата данни за управление на капацитета, когато анализират инцидентите и проблемите.
Прегледи на услугите **(Service reviews)**	Управлението на нивото на услугата трябва да извършва периодично прегледи за договорените параметри на услугите, договорените оперативни параметри и вътрешни споразумения. Тези прегледи изискват подпомагане на процеса на управление на капацитета, за да се оцени дали са съгласно изискванията, с малки пропуски и нарушения.
Нарушаване на споразуменията за услугата **(SLA breaches)**	Нарушаването на споразуменията за услугата са един вход към управлението на капацитета, защото всеки трябва да бъде записан и оценен. Базирайки се на тази оценка, управлението на капацитета е отговорен за дефиниране на подходящи подобрения на инфраструктурата.
Финансови планове **(Financial plans)**	Финансовите планове са един вход към управление на капацитета, защото тези планове ще включват бъдещи промени по инфраструктурата препоръчани от други отдели в компанията.

Интерфейс	Описание
Бюджети **(Budgets)**	Бюджетите ограничават обхвата на подобренията, които процеса на управление на капацитета може да оправдае в годишния план на капацитета.
Бизнес процес на управление на капацитета **(Business Capacity Management)**	Този под процес е отговорен за осигуряване, че бъдещите бизнес изисквания за ИТ услугите се смятат за планирани и внедрени постепенно в времето. Това може да се постигне чрез използване на съществуващите данни за текущото натоварване на ресурси от различните услуги, за да се види тренда, да се направи прогноза или модел за бъдещи изисквания. Тези бъдещи изисквания идват от бизнес плана описващ новите функции, подобрения и разрастването на услугите, плановете за развитие и т.н.
Управление на капацитета на услугата **(Service Capacity Management)**	Фокусът на този подпроцес е управлението на производителността в действителност - на оперативната ИТ услуга използвана от клиента. Той е отговорен за осигуряване, че производителността на всяка услуга, както и детайлите в целите са в договорените параметри на услугите и техните изисквания се наблюдават и измерват, а техните събрани данни се записват, анализират и докладват. Ако е необходимо също трябва да се предприемат действия, за да се осигури, че производителността на услугите отговаря на бизнес изискванията. Това се осъществява от персонала със знанията на всички области от технологията използвана в предоставянето на услугата от край до край и често включва търсенето на съвети от специалисти въвлечени в управлението на капацитета на ресурсите.
Управление на капацитета на услугата **(Resource Capacity Management)**	Фокусът на този подпроцес е управлението на индивидуалните компоненти на ИТ инфраструктурата. Той е отговорен за осигуряване, че всички компоненти в ИТ инфраструктурата, които имат ограничен ресурс се наблюдават и замерват и че събраните данни се записват, анализират и докладват. Ако е необходимо също трябва да се предприемат действия да се измерят наличните ресурси, за да се осигури ИТ услугите, които те поддържат, посрещат бизнес изискванията. За да се постигне тази задача, процеса по управление на капацитета се подпомага от хора със специални познания в тази област и технологии.
Планиране на капацитета **(Capacity plan)**	Планирането на капацитета е годишна прогноза за разходите необходими за поддържане на инфраструктурния капацитет. Той трябва да осчетоводи разходите необходими за постигненето на планирания бизнес и ИТ растежа.

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

Интерфейс	Описание
Базата данни за капацитета **(CDB)**	Базата данни за капацитета е свързана към базата данни на управление на конфигурацията, за да поддържа всички процеси по управление на услугата. За мониторинга на метриките и граничните стойности използвани за оценка на споразумението, параметрите на услугата се записват в CDB, за да поддържат SLA прегледите за изпълнение. Данните за остойностяване се пазят тук в базата данни на капацитета, за да поддържат планирането на капацитета. Управлението на инцидентите и управлението на проблемите използват CDB за преглеждане на производителността и метриките на капацитета, докато се изследват инцидентите и проблемите. Управлението на капацитета използва тези метрики за моделиране на производителността, когато се оценява заявките за промени на конфигурацията и когато се планират бъдещите разходи.
Базова линия и профили **(Baselines and profiles)**	След мониторинг на метриките се натрупват в CDB за период от седмици, така става възможно да се оцени един нормален образец на ресурса и използване на капацитета. Тези „нормални" стойности след това стават база за сравнение за заявката за промяна в конфигурацията и растежа на бизнеса
Гранични стойности и аларми **(Thresholds and alarms)**	Управлението на капацитета трябва да бъде про-активен процес в колкото се може по широка област. Граничните стойности се дефинират едновременно, за да проверят как се удовлетворяват договорените параметри на споразумението и активните дефинирани аларми. Управлението на капацитета трябва да даде обратна връзка към автоматичните инциденти за Service Desk–а, за да се предупредят за предстоящ проблем с капацитета. Например, една аларма настроена да се активира при 90% на капацитета, който е достигнат, за да предупреди Service Desk–а преди да се изконсумира останалия капацитет. И това ще позволи Service Desk–а да предприеме предварителни действия, за да се предпази услугата от пропадане.
Доклади за капацитета **Capacity reports (regular, ad hoc and exception)**	Докладите за капацитета се използват от процеса по управление на капацитета в планирането, при инциденти, проблеми и управление на капацитета, при изследване на инциденти и проблеми и при достъпност, капацитет и процеса на управление до договаряне на параметрите на услугата, когато се изследват удовлетвореност и заплахи.

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

Интерфейс	Описание
SLA and SLR recommendations	Управлението на капацитета е отговорен за оценяване на услугите и преценяване на постижимите параметри на услугата. Управлението на капацитета трябва да направи препоръки едновременно за измерител на всяка метрика дефинирана в предложението и възможността да се изпълни успешно.
Остойностяване и препоръки за таксуване **(Costing and charging recommendations)**	Управлението на капацитета е отговорен за оценка на себестойността на доставената услуга. Таксуването й може да се използва едновременно за възстановяване на тези разходите, както и да бъдат начин за влияние на търсенето.
Про-активни промени и подобрения за услугите **(Proactive changes and service improvements)**	Управлението на капацитета е отговорно едновременно за препоръчителните промени по конфигурацията, за да се адресират проблемите, очакван растеж и даване на препоръки за промени преди растежа да доведе до проблеми.
Ревизиране оперативния план **(Revised operational schedules)**	Управлението на капацитета може да предложи ръководство за структурирането на планове за батч задачи, архиви и други повтарящи се задачи, за да се минимизират проблемите с капацитета.
Ефективни прегледи **(Effectiveness reviews)**	Процеса на управление на капацитета трябва да се преглежда за ефективност и ефикасност на регулярен период от време, за да се осигури че: • той осигурява необходимия изход в необходимото време за подходящата аудитория; • техните дейности са ценово ефективни.
Доклади от одита **(Audit reports)**	Периодични одити трябва да се извършват, за да се осигури, че метриките събрани в базата данни свързана с управлението на капацитета не са нито прекомерни, нито са разпилени, за да се смятат за неадекватни стойности.

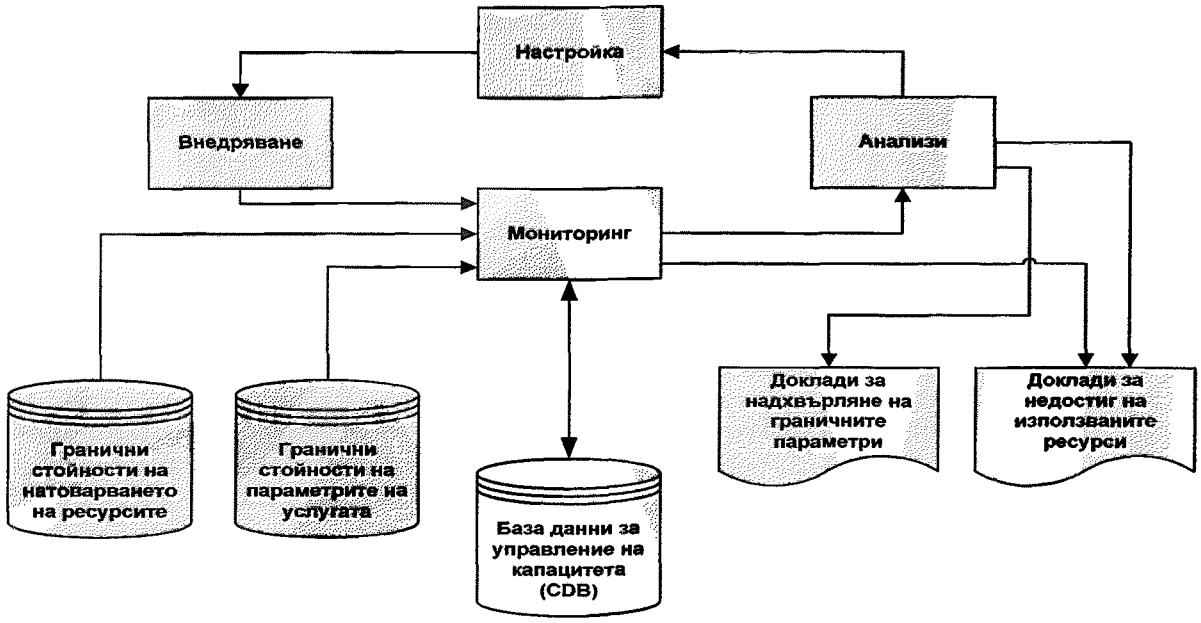
чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

8. Последователност в процеса по управление на капацитета

Управлението на капацитета не е прост процес от последователности. Дейностите в управлението на капацитета са илюстрирани във фигурата непосредствено по-долу. Тези дейности са повтарящи се, т.е. циклични. В допълнение управлението на капацитета има няколко дейности при поискване, които се появяват спорадично. Тези дейности са илюстрирани в диаграмата от последователности.

8.1.1. Процес на управление на капацитета – диаграма с последователност от повтарящи се дейности



8.1.2. Описание на повтарящите се дейностти

Страна	Описание
Внедряване (**Implementation**)	Едно проследяване трябва да бъде предприето, за да се осигури, че ресурсите, които обслужват жизнено важните за бизнеса функции и всички услуги покрити от SLA се наблюдават. Където има налични пропуски в мониторинга и когато и да са направени промени в конфигурацията, всеки компонент трябва да се оценява и наблюдава по най-ефективния ценови начин. Всички внедрявания трябва да се управляват от процеса по управление на капацитета.
Мониторинг (**Monitoring**)	Мониторинга трябва да се внедри през RFC (заявка за промяна) и после остава активен докато един бъдещ RFC оторизира отмяната.

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

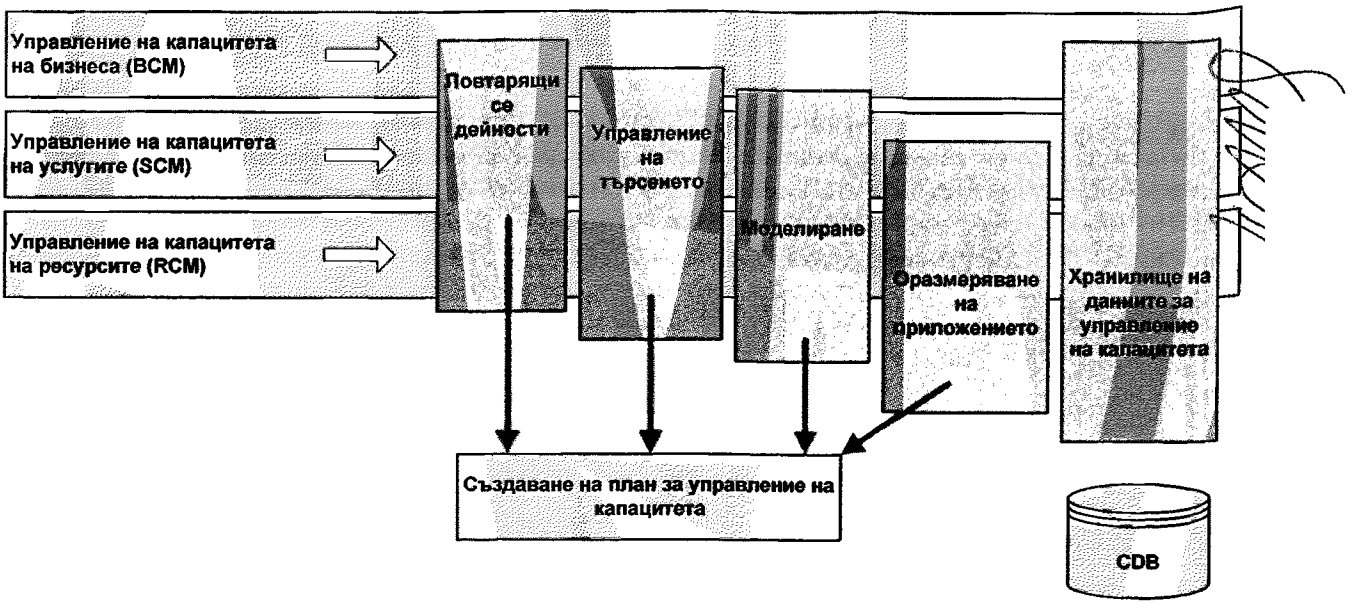
Страна	Описание
Анализи (**Analysis**)	Анализите трябва да се правят про-активно, за да се изследва тренда и да се предусещат проблеми. Анализите се стартират и в момент, когато се е появил проблем, които се ескалира към групата отговорна за управлението на капацитета.
Настройка (**Tuning**)	Оптимизирането на ресурсите ще се получи, когато един анализ установи слабост. Усилията за донастройка трябва да се координират с надеждност и процеса за продължаване на ИТ услугата, за да се осигури, че няма насрещно въздействие. Всички усилия за настройки трябва да се оценят срещу критериите установени от процеса за управление на капацитета.
Гранични стойности на натоварването на ресурсите (**Resource utilization thresholds**)	Граничните стойности на натоварването на ресурсите са предварителни стойности. Намерението е да се наблюдава капацитета или натоварването на ресурсите и автоматично да се генерира инцидент, когато наблюдаваните гранични стойности са застрашени. Тези гранични стойности трябва да се настроят достатъчно ниско, така че Service Desk –а може да отработи инцидента и да предприеме действие за предотвратяването на инцидента от повлияване на услугата доставяна на потребителите. Трябва също да се погрижи за настройката на гранични стойности да са достатъчно високи, за да се избегне да се генерират много на брой инциденти, където повечето от тези инциденти биха били самокоригиращи се.
Гранични стойности на параметрите на услугата (**SLM thresholds**)	Гранични стойности свързани с управлението на параметрите на услугата са оперативни гранични стойности. Веднъж, ако параметрите на услугата са били застрашени, е наложително Service Desk-а да действа бързо, за да минимизира развалянето на услугата.

За актуалната редакция и съдържание на процедурата проверете в *LODIS*.

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

Страна	Описание
База данни за управление на капацитета (**Capacity Management Database**)	Базата данни за управление на капацитета е свързана към базата данни с управлението на конфигурацията, за да подпомага всички процеси, свързани с управлението на услугата. Наблюдаваните метрики и гранични стойности използвани за оценка на споразумението за параметрите на услугата са записани в CDB, за да са в помощ на SLA прегледа по съвместимост. Данните за себестойността се записват тук, за да се подкрепи създаването на плана за капацитета. Управлението на инциденти и управлението на проблемите използват CDB за преглед метриките на производителността и капацитета, докато се изследват Инцидентите и Проблемите. Управлението на капацитета използва тези същите метрики за моделиране производителността, когато се оценява RFC и докато се планира бъдещи разходи.
Доклади в изключителни случай (**SLM exception reports**)	Заплахите за параметрите на услугите трябва да се наблюдават и докладват.
Доклади за изключителни случаи по отношение за натоварване на ресурсите (**Resource utilization exception reports**)	Натоварването на ресурсите в изключителни случаи трябва да се наблюдават и оценяват. Ценово ефективните действия трябва да се планират, за да се предотврати отново повторение.

8.1.3. Диаграма за последователността при процеса на управление на капацитета за дейностите при поискване



8.1.4. Описание на последователността при процеса на управление на капацитета за дейностите при поискване

Страна	Описание
Управление на бизнес капацитета (**Business Capacity Management**)	Този подпроцес е отговорен за осигуряване, че бъдещите бизнес изисквания за ИТ услугите са взети под внимание, планирани и заложени във времето. Това може да се постигне, чрез съществуващи данни за текущото натоварване на ресурсите и чрез тренда на различните услуги, прогнози или моделиране на бъдещите изисквания. Тези бъдещи изисквания идват от бизнес плана описващ новите услуги, подобрения и растеж в съществуващите услуги , планове за развитие и т.н.
Управление на капацитета на услугата (**Service Capacity Management**)	Фокусът на този подпроцес е управлението на производителността директно по време на работата на ИТ услугата използвана от клиентите. Той е отговорен за осигуряване, че производителността на всички услуги, като детайли в целите в SLAs и SLRs се наблюдават и измерват, а събраните данни се записват, анализират и се правят доклади. Само, ако е необходимо се предприемат действия, за да се осигури че производителността на услугите посрещат бизнес очакванията. Това се извършва от персонала със знания за всички области на технологията използвана в доставянето на услугата от начало до край и често използва съвети от специалисти включени в управлението на капацитета на ресурсите.

Страна	Описание
Управление на капацитета на ресурсите (**Resource Capacity Management**)	Фокусът в този подпроцес е управлението на индивидуалните компоненти на ИТ инфраструктурата. Той е отговорен за осигуряване на всички компоненти в ИТ инфраструктурата, които имат ограничен ресурс, за да се наблюдават и измерват, а събраните данни се записват, анализират и се правят доклади. Само, ако е необходимо, трябва да се предприемат действия за управление на наличните ресурси, за да се установи, че ИТ услугата, която те поддържат, посреща изискванията на бизнеса. За да се погрижат за тази работа, в процеса на управление на капацитета, екипа може да се асистира със специалисти с необходимите знания в точно определена област на технологията.
Повтарящи се дейности (**Iterative activities**)	Повтарящите се дейности бяха описани в предната секция на този документ.
Управление на търсенето (**Demand Management**)	Съгласно ITIL основната цел на Управление на търсенето е да илюстрира търсенето на изчислителни ресурси и на използването на тези ресурсите. Управление на търсенето обхваща всички дейности, които търсят уравновесяване на използването на ресурсите, за да минимизират пикови моменти.
Моделиране (**Modeling**)	Моделирането е всяка дейност, която опитва да предвиди поведението на ресурсите, които ще са резултат на дефинирано на натоварване.
Оразмеряване на приложението (**Application Sizing**)	ITIL казва, че основната цел на оразмеряването на приложението е да направи оценка на необходимите ресурсите, за да поддържа препоръчителните промени за приложението или ново приложение, за да се осигури, че то ще посрещне необходимото ниво на услугата.
Хранилище на данни за управление на капацитета (**Storage of Capacity Management Data**)	Базата данни за управление на капацитета (CDB) е решаваща за успешния процес на управление на капацитета. Управлението на капацитета е отговорен за конфигурацията, администрацията и техническата експлоатация на CDB и на мониторинг инструментите необходими за събиране на метриките на ресурсите и капацитета.

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

Страна	Описание
Създаване на план за управление на капацитета **(Production of the Capacity Plan)**	Плана за капацитета описва дейностите, които Управлението на капацитета препоръчва да предприеме, за да поддържа необходимото ниво на услугата през следващите дванадесет месеца. Този план трябва да включва едно пълно описание на препоръчителните промени и на неговата ценова оценка.
CDB	Базата данни за управление на капацитета е свързана към базата данни за Управление на конфигурацията, за да подкрепят всички процеси на Управлението на услугата. Наблюдаваните метрики и гранични стойности използвани за оценка на параметрите на споразумението за услугата (SLA) се записват в CDB, за да подкрепят прегледа по изпълнение на SLA. Данните за остойностяването се запазват тук, за да подкрепи създаването на Плана за капацитета. Управлението на инцидентите и Управлението на проблемите използва CDB за преглед производителността и метриките на капацитета, докато се изследват инцидентите и проблемите. Управлението на капацитета използва същите метрики за моделиране производителността, когато се оценява RFC и когато се планират бъдещи разходи.

9. Контрол на изпълнението

Оперативният контрол за изпълнението на планиране на капацитета в съответствие с изискванията на настоящата процедура, се осъществява от отговорника за предоставянето на съответната ИТ услуга.

Общият контрол за изпълнението на дейностите от настоящата процедура се изпълняват от ръководителя на съответното направление.

10. Блок схеми

Блок – схемите са изложени в съдържателното описание на процедурата.

11. Термини и съкращения

Система за Управление на качеството и информационната сигурност (СУКИС)	Организационната структура на *ЛИРЕКС.КОМ* в комплекс с регламентирания ред , процесите и ресурсите, необходими за управление на качеството и на информационната сигурност на предлагани продукти и услуги.

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

Сигурност на информацията (информационна сигурност)	Запазване на поверителност, цялостност и наличност на информацията.
Поверителност	Свойството информацията да не се предоставя или разкрива пред неупълномощени лица, служители или процеси.
Цялостност	Свойството за опазване на точността и целостта на активи.
Наличност	Свойството за достъпност и използваемост на информацията при заявка от упълномощено лице.
Политики по информационната сигурност	Цялостните намерения и насоки на дейност на дружествата относно информационната сигурност, официално заявени от висшето ръководство на *Лирекс.ком*. Целите, отговорностите и задълженията за всяко управленско ниво относно официалната политика по качеството на *Лирекс.ком*.
Документ на СУКИС	Документирано описание (процедура, инструкция, ръководство, вътрешно фирмен стандарт) на реда за изпълнение на дейностите/процесите и приложимите форми/бланки/унифицирани документи.
Процедура/инструкция	Регламентиран ред за изпълнение на дейност/ процес/ операция.
Лирекс.ком	Дружествата Лирекс БГ, Лирекс БС, Лирекс Хай Тех, Беолик, Лирекс Скопие, Теза
Упълномощен Представител на Ръководството	Упълномощен от Ръководството на *ЛИРЕКС.КОМ* ръководен служител, отговарящ за контрола по приложимостта и развитието на *СУКИС*.
Ръководител по информационната сигурност	Упълномощен от Ръководството на *ЛИРЕКС.КОМ* служител, отговарящ за цялостната дейност по осигуряване на сигурността на информацията като част от СУКИС.

12. Препратки към документи

ID на документа	*наименование на документа*
LQS Manual	Наръчник по качеството и информационната сигурност
LPP001	Процедура: Подготовка, преглед и сключване на договори
ISO/IEC 27001:2013	Information technology. Security techniques. Information security management systems. Requirements
LPP013	Управление на външни ИТ услуги
LPN002	План за управление на ИТ услуга
LSB-100-RIS	Регистър на вътрешните услуги

За актуалната редакция и съдържание на процедурата проверете в *LODIS*.

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

13. Оценки

На годишния преглед на Ръководството се прави преглед и оценка на необходимостта от промяна на вътрешно-фирмения ИТ капацитет.

14. Документирана информация

ID на формата	*наименование на формата*
LSB702-SCP	План за управление на капацитета

За актуалната редакция и съдържание на процедурата проверете в *LODIS*.

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

1. История на редакциите

версия	описание на промяната	автор	проверил	утвърдил	дата въвеждане
3	Въвеждане на изискванията на ISO/IEC 27001:2005	Пл.Петрова	Вл.Стоев	Д.Илиева	04.02.2009
4	Въвеждане на изискванията на ISO/IEC 20000-1:2005	Б.Йорданов	Вл.Стоев	Д.Илиева	06.04.2010
5	Актуализиране на документите от СУКИС	М.Йончева	Б.Корчев	Д.Илиева	16.08.2013

2. Предназначение

Документът има за предназначение да определи реда за поддържане на мрежови решения с приложението на мрежови технологии в съответствие със задълженията на *Лирекс.ком*, произтичащи от сервизни договори с партньори (напр. *Cisco Systems)*.

Дефинира ескалационния процес при решаване на мрежови проблеми и реда за неговата реализация.

3. Приложимост

Регламентираният в инструкцията ред се прилага при сервизно обслужване на клиенти от *Лирекс.ком* в изпълнение на договорни задължения. Изключения в реда за изпълнение на сервизните дейности и за документиране на сервизните операции се прави само в случаите на специфични изисквания за управление на проекти, регламентирани от процедура *LPP006*.

Взаимодействието на процеса от настоящата инструкция с другите процеси за мрежово сервизно обслужване се осъществява съгласно процедури *LPP301, LPP007, LPP012 and LPP013.*

Инструкцията е задължителна за изпълнение от служителите на *Лирекс.ком*, които осъществяват сервизно поддържане на мрежови решения.

Практическата реализация на сервизни дейности се осъществява съгласно техническата документация за съответните устройства, операционни системи, програми.

4. Отговорности

4.1. Висше ръководство

- осигурява необходимите ресурси за реализация на сервизното обслужване;
- ангажира всички възможни фирмени ресурси за решаване на мрежови проблеми с **приоритет 1**;

4.2. Ръководителят на звено Телекомуникационни услуги

- организира, ръководи и контролира цялостната дейност на компанията за сервизно обслужване на мрежови решения с приложението на информационни технологии;
- участва в решаването на мрежови проблеми, изискващи висока квалификация;
- включва в седмичния отчет за преглед от Ръководството, съгласно процедура LMP003, информация за работата и проблемите в направлението за мрежово сервизно обслужване;

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

- планира дежурствата на DM.

4.3. Изпълняващият длъжността Duty Manager

- пряко организира и съгласува дейността със СЦ – ТКУ;
- координира своевременното и качествено решаване на регистрирани сервизни случаи;
- организира и участва в регламентирания ескалационен процес;
- при необходимост и целесъобразност, лично работи по сервизен case и ескалира неговия приоритет;
- подготвя справка за седмични отчети на дейността за мрежово сервизно обслужване, която предава на ръководителя на ТКУ;
- изготвя регламентираните отчети за измервания и оценки на процеса;
- прави предложения за допълнителни ресурси, необходими за реализация на мрежовото сервизно обслужване;
- прави предложения за превантивни и коригиращи действия относно мрежовото сервизно обслужване;

4.4. Сервизният инженер (СИ)

- регистрира в LCC (cc.lirex.bg) възникналия сервизен проблем;
- работи за решаване на мрежови проблеми във връзка с възложените му сервизни случаи, в съответствие с изискванията от настоящата инструкция;
- качествено и в срок решава възникнали мрежови проблеми;
- записва всички съществени данни и процеси при разрешаване на поет сервизен проблем, като своевременно отразява всяка промяна на състоянието му в LCC системата и 'затваря' неговото досие там при разрешаване на сервизния проблем;
- прави предложения за превантивни и коригиращи действия относно мрежовото сервизно обслужване на базата на практическия опит от решаването на възникнали проблеми;

4.5. Операторът на Call Centre (CCO)

- осъществява обмен на информация с клиентите, в съответствие с изискванията на инструкцията;
- предава получена от клиенти информация на сервизните инженери, администратора на СЦ - ТКУ и ръководни длъжностни лица;

4.6. Администратор на СЦ - ТКУ

- координира дейностите по сервизно поддържане на мрежови решения;
- координира своевременното и качествено решаване на регистрирани сервизни случаи;
- организира и ръководи сервизния склад за мрежово оборудване;
- координира своевременната замяна на дефектирало оборудване съгласно инструкция LPI303;
- прави предложения за допълнителни ресурси, необходими за реализация на мрежово сервизно поддържане;
- прави предложения за превантивни и коригиращи действия относно мрежовото сервизно обслужване.
- регистрира и води на отчет резервни части (устройства, модули, компоненти) за сервизно поддържане;

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

- организира и участва в дейностите за приложението на инструкция LPI303 за замяна на дефектирало оборудване;
- поддържа в актуално състояние регистрите за отчет и контрол на движението на резервни части и заменяно оборудване съгласно инструкция LPI303.

5. Процедура

Процесът за сервизно поддържане на мрежови решения се реализира от следните взаимосвързани подпроцеси:

- приемане на съобщения от клиенти,
- иницииране на СЗ (case сервизни дейности за решаване на проблем),
- решаване на сервизен проблем, обслужване на СЗ;
- замяна на хардуер,
- актуализация на софтуер,
- промяна на конфигурация,
- приключване на СЗ.

Основните връзки между подпроцесите и с други процеси са показани на Фигура 1.

5.1. Общи положения

Сервизно поддържане се изпълнява при:

- съобщения за възникнал проблем в процеса на експлоатацията на поддържано от мрежовите сервизни центрове на *Лирекс.ком* мрежово оборудване, на основание на договорни отношения;
- съобщения за възникнал проблем в процеса на експлоатацията на Интернет мрежата на *Лирекс*.ком.

В процеса на сервизното обслужване се ползват данни от БД на инсталираното оборудване *(InstalledDB*), която се създава от процеса *Информационно осигуряване* на сервизната дейност, съгласно процедура *LPP301*. В процеса на сервизното поддържане данните в БД се актуализират с информация за заменени дефектирали устройства/ модули, инсталирани нови версии на ОС, промяна в конфигурацията за устройства.

6.1.3. За ефективна комуникация на клиентите със СЦ - МТКУ се поддържат 'горещ' телефон и e-mail адрес. Последните са адресирани към т.н. *Call Centre*. Телефонният пост за 'горещ' телефон и e-mail адресът се определят от ръководителя на ТКУ.

Обаждания по 'горещия' телефон се приемат от оператора на Call Centre (CCO). Администраторът на СЦ - ТКУ редовно следи за постъпили електронни съобщения на 'горещия' e-mail адрес. Електронните съобщения са конвенционални съобщения или попълнени специални web форми.

По преценка на ръководителя на ТКУ, в рамките на работното време „горещият" телефон може да се комутира към друг телефонен пост в компанията, на който отговаря винаги компетентен специалист. В извън работно време 'горещият' телефон се комутира към телефона на DM.

CCO изпълнява следните функции:

- приема съобщения от клиенти за възникнали проблеми;
- получава информация от клиенти и я предава на администратора на СЦ – ТКУ, сервизните инженери и ръководни длъжностни лица;

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

По преценка на ръководителя на ТКУ, в рамките на работното време ролята на ССО може да се изпълнява от администратора на СЦ – ТКУ.

6.1.4. Организацията на всички сервизни операции се основава на принципа за работа по възникнал проблем. Всяко съобщение за проблем се регистрира и до приключване на работата по него се разглежда като *сервизен case или СЗ*.

6.1.5. Управлението на фирмените ресурси за решаване на възникнал проблем се основава на оценката за влиянието на функционалността на мрежовото оборудване върху бизнес операциите на клиента. В тази връзка, за възникнал проблем, респ. за СЗ, се определя *приоритет* по следната схема:

Таблица 1. Приоритети на мрежови проблеми

приоритет	*естество на проблема*
Приоритет 1	Цялата поддържана мрежа / система не функционира и това може да повлияе критично на бизнес операциите на клиента, ако проблемът не бъде отстранен. *Лирекс.ком* и клиентът са готови да ангажират денонощно всички свои ресурси до идентифициране на проблема и неговото отстраняване. Работата по СЗ започва в рамките на 1 час от получаване на съобщение за възникнал проблем. Приоритетът е приложим само за договорено сервизно обслужване 7 дни в седмицата х 24 часа в денонощието.
Приоритет 2	Проблемът в поддържаната мрежа / система засяга критични аспекти на бизнес операциите на клиента, системата функционира частично или реално с влошени параметри. *Лирекс.ком* и клиентът са готови да ангажират напълно своите ресурси в границите на нормалното работно време за отстраняване на проблема. Работата по СЗ започва в рамките на 4 часа от получаване на съобщението за възникнал проблем.
Приоритет 3	Съществува проблем в поддържаната мрежа / система. Цялостната функционалност е нарушена, но по-голямата част от бизнес операциите на клиента не са възпрепятствани. *Лирекс.ком* и клиентът са готови да ангажират своите ресурси в границите на нормалното работно време за отстраняване на проблема. Работата по СЗ започва в рамките на 12 часа от получаване на съобщението за възникнал проблем.

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

Приоритет 4	Клиентът изисква информация или консултация относно възможностите на хардуерни / софтуерни ресурси, конфигурация или инсталация. Времето за реакция (начало на работата по СЗ) е в рамките на 24 часа от получаване на съобщението за възникнал проблем.
Приоритет 5	Клиентът изисква обща информация или консултация, която не е с особена важност. Времето за реакция е в рамките на 72 часа от получаване на заявката.

Забележка: Приоритети 2, 3, 4 и 5 са приложими за договорено сервизно обслужване в рамките на стандартно приетото работно време - 5 (дни в седмицата) х 8 (часа в денонощието).

Приоритетът на СЗ се определя и променя по следните правила:

- При първоначално съобщение за възникнал проблем, клиентът задава приоритета по негова преценка, след като му бъде разяснено значението на отделните приоритети.
- Реалният приоритет на СЗ се определя от СИ, изпълняващ сервизната заявка, след анализ на ситуацията при започване на работа по проблема.
- Приоритетът на СЗ може да се промени в процеса на работа при следните условия:
  - намерено е временно решение, с което е възстановена напълно или частично функционалността на устройство / система. Приоритетът може да се намали, с цел обективно иницииране на ескалационен процес;
  - клиентът не приема определения като реален от СИ приоритет. Приоритетът в случая се определя по преценка на DM или на ръководителя на звено ТКУ.
- Всяка промяна на приоритет се съгласува с клиента.

Регистрацията на проблеми – обект на сервизно поддържане и документирането на предприеманите действия се осъществява със записи в LCC (cc.lirex.bg).

Записите в LCC (cc.lirex.bg) се разглеждат като записи по качеството и отговарят на изискванията от процедура *LMP002*.

Структурата на логическите записи в LCC (cc.lirex.bg) се определя от ръководителя на ТКУ и е показана в Приложение 1.

За работа по възникнал проблем се определя *отговорен СИ*, или се сформира екип с отговорник. За проблеми с приоритет 1 или 2 като отговорен СИ се определя DM. За ръководител на екип се определя DM, или ръководителя на звено ТКУ.

Текущото състоянието на работата по СЗ се отразява с промяната на статуса. Възможните състояния за статуса на СЗ са съгласно Приложение 2.

Измерители за оценка на работата по СЗ са времената за реакция и за работа на сервизните специалисти.

Времето за реакция е периодът от момента за постъпване на съобщение от клиент за възникнал проблем и отваряне на сервизна заявка в LCC (cc.lirex.bg) до момента на обратното обаждане от страна на СИ. Времето за реакция се определя от договорните отношения с клиента.

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

Времето за работа по СЗ се измерва с периода от време, през което даден case е в състояние ***ce-pend*** Стойностите на ***WoT*** служат за управление на ескалационния процес, описан в т.6.8.

Системата LCC (cc.lirex.bg) автоматично отчита времената при обслужването на СЗ. Тези времена се използват като отправни в ескалационния процес.

В процеса на работата по СЗ длъжностните лица (отговорен СИ, администратор на СЦ – ТКУ, DM, ръководител на звено ТКУ) информират регулярно клиента относно установеното състояние по проблема, състоянието на работата, предприетите действия и очакваните резултати от тях.

При изпълнение на сервизните дейности се съблюдават следните общосистемни изисквания:

- манипулирането, съхранението и опаковането на технически средства се осъществява съгласно процедури *LPP002, LPP003* и *LPP004*;
- работа с продукти, които не отговарят на изискванията, се осъществява съгласно процедура *LAP004*.

Комуникациите със съответните звена на партньорите (напр. ***Cisco Systems)*** се осъществяват в съответствие с условията на сервизните договори и възприетите процедури.

5.2. Приемане на съобщения

Съобщения от клиенти се получават от ССО, администратора на СЦ – ТКУ, Ръководителят на съответния проект или от отговорния за сервизен case СИ.

6.2.1. При постъпване на първоначално съобщение от клиент за възникнал проблем, ССО предава иннформацията на администратора на СЦ – ТКУ.

Администраторът на СЦ – ТКУ:

- идентифицира клиента в *Installed DB* – сервизен договор, условия за сервиз;
- идентифицира дефектиралото устройство, като ползва данните от клиента и от *Installed DB* – p/n, s/n, зареден софтуер, конфигурация, местонахождение;
- определя отговорен СИ и му предава информацията за възникналия проблем

Сервизният инженер регистрира сервизна заявка в LCC (cc.lirex.bg) след получаване на съобщението за възникналия проблем.

При отваряне на СЗ в LCC (cc.lirex.bg), СИ от 'лист менюта' избира "Клиент" и "Лице за контакти". Системата автоматично попълва полетата:

Комуникация с клиента:	Телефон:	
	e-mail,CC:	
	Адрес:	

Ако информацията за "Клиент", "Лице за контакт", "Комуникация с клиента" не е въведена предварително в LCC системата, СИ е длъжен да я въведе.

СИ отново от 'лист менюта' избира:

- "Тип на case", който може да бъде:
  - Общ въпрос;

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

- Хардуерен дефект (RMA);
- Софтуерен проблем;
- BUG;
- Помощ при конфигурирането.

- "Приоритет":
  - 1 – Критичен (Мрежата не работи)
  - 2 – Висок (Мрежата работи зле)
  - 3 – Нормален (Проблеми с мрежата)
  - 4 – Нисък (Оптимизация на мрежата)
  - 5 - Много нисък (Общи Въпроси)

В полето "Кратко описание на проблема", СИ кратко описва проблема. Това описание служи за заглавие на СЗ.

В полето "Пълно описание на проблема" прилага всички предоставени от клиента данни и материали, както и оригиналното описание на проблема, направено от клиента.

След въвеждане на информацията във всички полета натиска бутона "Submit".

LCC системата автоматично генерира "Case No", дата и час на отваряне на СЗ и името на СИ, който е отворил СЗ.

При постъпване на съобщение от клиент по регистрирана вече СЗ, ССО предава информацията на администратора на СЦ – ТКУ, който реагира в зависимост от същността на съобщението:

За проявен интерес от клиента относно текущото състояние на работата по СЗ, го информира, като за целта ползва LCC (cc.lirex.bg)..

Получена допълнителна информация от клиента предава с електронно съобщение или по телефона на отговорния СИ.

6.2.2.3. За постъпило искане от клиента за промяна на приоритета на проблема уведомява DM и отговорния СИ. Отговорният СИ извършва запис в LCC (cc.lirex.bg), като променя приоритета и статуса на case в състояние ***ce-pend***.

DM установява контакт с отговорния СИ за изясняване на ситуацията, като по преценка може да определи допълнително сервизни специалисти за работа по case, както и да определи нов отговорен СИ. За своето решение DM уведомява клиента.

Промяната на отговорния СИ/ екипа за работа по case се документира в LCC (cc.lirex.bg)..

5.3. Решаване на сервизен case

Процесът се състои в анализ на ситуацията от страна на отговорния СИ (и екипа) за работа по сервизен case, вземане на решение за последващи действия и изпълнението им.

След приемане на задачата за работа по СЗ отговорният СИ, независимо дали до момента е работено или не по проблема,

- уведомява клиента, че е определен за отговорен СИ по case;

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

- анализира наличната информация,
- при необходимост, изисква допълнителна информация или изпълнението на определени операции от клиента,
- определя приоритет на проблема, който съгласува с клиента,
- при необходимост отваря case в специализирана система на партньора (напр. Cisco TAC).

За периода, през който се очаква информация или изпълнението на определени действия от клиента, се установява статус ***cust-pend*** за СЗ.

Възможните последващи действия на сервизните специалисти са *замяна на* дефектирал *хардуер*, *актуализация на софтуер* или *промяна в конфигурацията* за мрежово устройство. За решаване на проблема може да бъде изпълнена само някоя от дейностите или съчетание от тях.

След изпълнение на операции за решаване на мрежови проблем по СЗ, СИ проверява за ефективността на предприетите действия.

В случай на безрезултатни действия за отстраняване на проблема, СИ докладва на DM и изпълнява неговите разпореждания.

При обективна невъзможност за решаване на проблем се търси съдействие от партньора (напр. *Cisco)*, като се прави съответна регистрация / актуализация в неговата специализирана система (*Cisco TAC)* и статусът на съответния case се установява в състояние нерешен (**pending** напр.***Cisco-pend)***.

5.4. Замяна на хардуер

При установен дефектирал хардуер, СИ променя статуса на СЗ в състояние ***RMA-out*** и предприема действия в зависимост от складовите наличности за подмяна на хардуера.

За замяна на дефектирал хардуер, независимо от предприеманите действия за решаване на проблема по case, СИ регистрира *RMA_case* в специализирана система на партньора ***(Cisco TAC)*** в съответствие с инструкция *LPI302.*

СИ уведомява администратора на СЦ – ТКУ за необходимия му хардуер. Администраторът на СЦ – ТКУ проверява складовите наличности в регистъра Depot_NCT, поддържан съгласно инструкция *LPI302.*

При наличие на необходимия хардуер, СИ генерира заявка ***RMA_Lirex*** към администратора на СЦ – ТКУ, който изписва необходимото устройство / модул от склада по реда от инструкция *LPI302.* Предоставянето на клиента на нов хардуер се документира с протокол по образец (форма *L-NET-004-PRMA*).

6.4.2.2. В случай на отсъствие на необходимия хардуер, администраторът на СЦ – ТКУ проверя за наличието на подходящ за решаване на проблема хардуер. Такъв се инсталира за временно ползване до получаване на точно необходимия хардуер от партньора (напр. Cisco). За целта СИ прави заявка ***RMA_Exch***, съгласно инструкция *LPI302.* Хардуерът за временно ползване се предоставя на клиента с протокол по образец (форма L-ADM-008-OPR).

След получаване на необходимия хардуер от партньора (напр. Cisco), същият се изписва от склада и предоставя на клиента, инсталира се по описания в горната точка ред, а предоставеният за временно ползване се приема от клиента, като се проверява техническото му състояние, и се предава в склада. Контролът за операцията се осъществява съгласно инструкция *LPI302.*

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

277

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

При невъзможност за подходяща замяна на дефектирал хардуер се изчаква получаването на необходимото устройство / модул от партньора (напр. Cisco), след което се осъществява замяна по описания ред. За целта СИ генерира заявка ***RMA_Req*** към процеса за управление на резервни части.

Предоставяният на клиента хардуер се инсталира от СИ или му се предава за инсталиране от негови специалисти. Преди предаване, ако е необходимо СИ зарежда софтуер / конфигурация. След инсталиране на хардуера, СИ проверява за функционалната работоспособност на мрежовото оборудване.

Операциите по замяна на хардуер се документират в LCC (cc.lirex.bg), а данните за нов хардуер се отразяват в *Installed DB* в съответствие с процедура *LPP007*.

5.5. Актуализация на софтуер

При необходимост отактуализация на софтуер, СИ осигурява подходящата версия на ОС за хардуердната платформа – от архивните фондове на СЦ – ТКУ или online от интернет страницата на партньора (напр. *www.cisco.com)*.

Софтуерът се инсталира от СИ или от представител на клиента. Ако инсталацията се извършва от представител на клиента, СИ подготвя и инструкция за инсталиране. За периода на инсталиране на софтуер от представител на клиента се установява статус ***cust-pend*** за СЗ.

След инсталиране на софтуер, СИ проверява функционирането на устройството с новоинсталирания софтуер.

Операциите по актуализация на софтуер се документират в LCC (cc.lirex.bg).. Версията на инсталирания софтуер се описва в *Installed DB*.

5.6. Промяна на конфигурацията

Изпълнява се със следната поредност от операции:

- Съвместно с представител на клиента, СИ дефинира описателно желаното поведение на устройство в мрежата. За периода на изпълнението на операцията след описателното дефиниране на желаното поведение се установява статус ***ce-pend*** за СЗ.
- СИ създава резервно копие на съществуващата конфигурация.
- СИ разработва нова конфигурация за устройство, зарежда я в устройството / конфигурационния сървер, и я тества за постигане на желаното поведение (функционалности) на устройството във мрежата.

Зареждането на нова конфигурация се документира в LCC (cc.lirex.bg)., а описанието на същата се включва в *Installed DB*.

5.7. Приключване работата за решаване на мрежов проблем и 'закриване' на case

За предприетите действия и резултатите от тях, при решаването на възникнал мрежов проблем, независимо от приложения подход и средства, СИ уведомява клиента. Ако последният приеме за удовлетворително решаването на проблема, се осъществява 'затваряне' на case – статусът се установява в ***closed***.

За несъгласие на клиента с резултата от решаване на проблема, СИ докладва на DM или на ръководителя на ТКУ и изпълнява неговите разпореждания. Последният може да вземе решение за 'затваряне' на сервизен case или за продължаване на работата с ангажиране на допълнителни ресурси.

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

6Приключването ('затваряне') на case се документира, както следва:

- в LCC (cc.lirex.bg) се отразява приключване на case с основанията за това и се променя статуса в състояние ***closed***;
- изготвя се протокол за мрежово сервизно обслужване по образец (форма *L-NET-003-P*), който се подписва от отговорния СИ и представител на клиента.

За приключени сервизни случаи от клиента се изисква информация за неговата оценка за решаването на проблема. За целта се ползва форма *L-PR-003-NET*, а данните от попълнена форма се обработват съгласно процедура *LAP001*.

5.8. Ескалация на инцидентите

В изпълнение на декларираната политика на компанията за осигуряване изискваното качество на предлаганото сервизно обслужване, при възникване на мрежов инцидент на клиент се ангажират необходимите и достатъчни ресурси за идентифициране на причината и отстраняването й. За целта се прилага механизъм за ескалация на инцидентите, който се състои в следното:

Времето, през което по даден сервизен case работят ефективно специалисти на компанията ('активно състояние ***ce-pend***) се поставя на контрол от момента на регистрацията на сервизен case. За всеки тип приоритет се определят контролни (ескалационни) времена, при настъпването на които се стартира *ескалационен процес*. Последният се състои в уведомяване на определено длъжностно лице, което:

- се запознава с проблема и състоянието на работата по него;
- при необходимост и по преценка, ако това е в неговите правомощия, ангажира допълнителни фирмени ресурси (повече СИ, СИ с по- висока квалификация, ръководни кадри) за работа по case;
- дава указания за предприемане на определени действия;
- уведомява лично клиента за състоянието на работата по case и за предприетите действия.

В зависимост от приоритета на инцидента се прилага следната схема за уведомяване и ангажиране на длъжностни лица:

Таблица 2. Схема за реализация на ескалационен процес

Т от иницииране на case (в h)	*Приоритет 1*	*Приоритет 2*	*Приоритет 3*	*Приоритет 4*	*Приоритет 5*
1	СИ				
4	DM	СИ			
12			СИ		
24	Ръководител ТКУ	DM		СИ	
48	Висше ръководство	Ръководител ТКУ	DM		

72					СИ
96		Висше ръководство	Ръководител ТКУ	DM	

Действията на длъжностните лица при ескалационния процес са описани в Приложение 3.

Забележка: Времето за нотификация е в часове. Нотификацията се извършва през съответните интервали от време считано от момента на отваряне на сервизната заявка.

LCC автоматично изпраща нотификации на СИ по e-mail и SMS според таблицата за ескалация на проблемите или при постъпване на нова информация по сервизната заявка.

Нотификацията на DM, Ръководителя на ТКУ и Висшето ръководство се извършва по e-mail.

Контролните времена за активните в момента сервизни заявки се следят от администратора на СЦ - ТКУ. Когато съществуват неприключени сервизни случаи, последният на всеки астрономически час проверява за наличието на 'активни' cases (статус = ***ce-pend***). За всеки активен case проверява дали не е настъпил момента за контролно време, и ако е настъпил - уведомява съответното длъжностно лице, съгласно горната схема. В случай, че не може да установи контакт с длъжностното лице, администраторът на СЦ - ТКУ уведомява DM и неговия непросредствен ръководител. При ненамерен управител се уведомява някой от директорите на фирмата.

След уведомяване на длъжностно лице, администраторът на СЦ - ТКУ проверява дали за приоритета на case има следващо контролно време.

Стартирането на ескалационен процес се документира в LCC (cc.lirex.bg).

За проверка на съответствието на времената за ескалация на LCC (cc.lirex.bg) с определените в инструкцията се извършват периодични тестове.

За целта DM всеки месец отваря по една служебна сервизна заявка с приоритет 1 и приоритет 2, и регистрира нотификациите, изпращани от автоматизираната информационна система за регистриране и проследяване на обслужването на сервизни проблеми. Резултатите от тези заявки се описват от DM по общия ред за работа с LCC. Когато са налице отклонения от предвидените параметри те също се описват и затова се уведомява ръководителя на сервизния център, който предприема необходимото коригиращо действие. След последващ успешен тест служебната заявка се приключва.

Задължителни тестове се извършват и при промени в конфигурацията на системата (софтуерни и хардуерни), както и при преинсталацията й.

5.9. Управление на проблемите

Процесът на управление на проблемите има за задача да намали броя и въздействието на инцидентите и проблемите върху бизнес процесите като ги решава и отразява в документи, достъпни за ръководството и СЦ-ТКУ. Проблем се идентифицира след голям брой идентични инциденти или единичен инцидент, чиято причина не я е изяснена, но е причинил значителна вреда. Проблем може да бъде ескалиран от СИ, ДМ или СЕО.

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

Управлението на проблемите се **извършва в съответствие с процедура LSP800 и е свързано** с определяне и изпълнение на Анализ **на първопричината** (Root Cause Analyses - RCA). За **входна информация** на RCA се използват:

- записите за инцидентите, **информация за тях и тяхното въздействие;**
- информация за конфигурационната **база данни** (*Installed DB*);
- информация за други процеси.

Изходът на RCA съдържа:

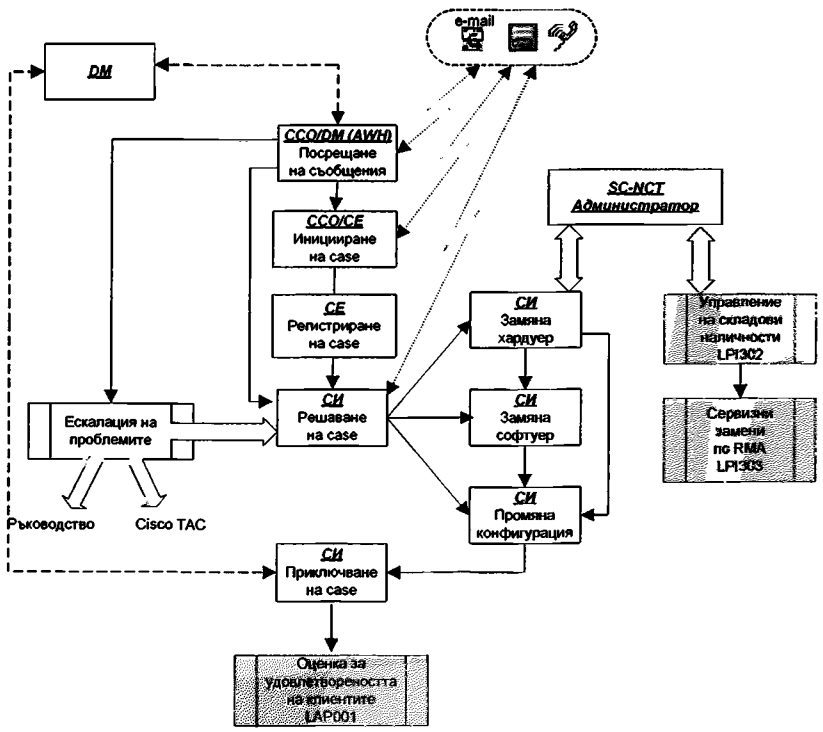
- проучване на проблема и анализ;
- изследване на проблема и решение;
- искания за коригиращи действия (CAR) – ако е необходимо;
- документиране на научени уроци (lessons learned);
- попълване на записите за решените проблеми (ако установения проблем е решен).

За напредъка при решаване на проблемите и за въведените промени се информират ръководството, **СЦ - ТКУ** и клиентите.

6. Оценки

Оценките, свързани с изпълнението на дейностите по настоящия документ, се представят на Годишния преглед от ръководството.

7. Блок схеми



Фигура 1. Схема на процеса за *сервизно поддържане на мрежови решения*

За актуалната редакция и съдържание на процедурата проверете в *LODIS*.

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

8. Термини и съкращения

Ескалация на инцидент	Политика на организацията за своевременно уведомяване на съответни ръководни нива за възникнал инцидент, с цел : • контрол за състоянието на работата по отстраняване на инцидента; • ангажиране на необходимите за решаване на проблема ресурси; • участие на всички ръководни нива за осигуряване на декларираното ниво на качеството на продукти и услуги; • осведомяване на клиента за вземаните мерки за отстраняване на проблем;
Ескалация на проблем	Политика на организацията за своевременно уведомяване на съответни ръководни нива при идентифициране и анализ на причините за поява на еднакви или непознати инциденти и тяхното решаване.
Конфигурация	Набор от команди на операционната система, определящи поведението на устройство в мрежата. Съхранява се в самото устройство или в конфигурационен сървър.
Call Centre	Организационна форма за контакт с СЦ - ТКУ. Реализира се с "горещ" телефон и mail-адрес.
СЦ - ТКУ	Мрежов Сервизен Център. Функционално звено в състава на звено Телекомуникационни услуги. Включва специалисти с необходимата квалификация. Специалистите от СЦ - ТКУ, които работят в офисите на територията на страната, административно са подчинени на ръководителите на офисите.
ТКУ	Телекомуникационни услуги
СИ	Сервизен инженер.
DM	Duty manager - мрежови инженер, контролиращ работата на сервизните инженери по отстраняване на възникнали проблеми.

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

CCO	Оператор на Call Centre.
LCC	Автоматизирана информационна система за регистриране и проследяване на обслужването на сервизни проблеми – *cc.lirex.bg*
Installed DB	База данни с описание на инсталирано и/или поддържано от *Лирекс.ком* мрежово оборудване. За всяко устройство се поддържат данни за: • p/n и s/n; • компоненти (модули) и серийните им номера; • заредена операционна система (версия на ОС); • конфигурация; • данни за клиента; • други данни.
RMA	Return Materials Authorization. Процедура за замяна на (дефектирал) хардуер по предварително договорени сервизни условия с производителя.
СУКИС	Система за управление на качеството и информационната сигурност
Сигурност на информацията (информационна сигурност)	Запазване на поверителност, цялостност и наличност на информацията.
Лирекс.ком	Дружествата Лирекс БГ, Лирекс БС, Лирекс Хай Тех, Беолик, Лирекс Скопие, Теза

9. Препратки към документи

ID на документа	*наименование на документа*
LMP002	Процедура: Управление на документи и записи за реализация на фирмените дейности

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

LMP003	Процедура: Преглед на СУКИС от Ръководството
LPP002	Процедура: Идентификация и проследимост на продукти
LPP003	Процедура: Работа с продукти на клиент
LPP004	Процедура: Манипулиране, съхранение, опаковане и доставка на продукти
LPP006	Процедура: Управление на програми и проекти
LPP007	Процедура: Управление на конфигурацията
LPP012	Процедура: Управление на промените
LPP013	Процедура: Управление на външни ИТ услуги
LPP301	Процедура: Организация и управление на мрежово сервизно обслужване (Support)
LPI302	Инструкция: Управление на резервни части за Support
LAP001	Процедура: Измерване степента на удовлетвореност на клиентите
LAP004	Процедура: Работа с продукти, несъответстващи на определените изисквания
LSP701	Процедура: Управление на пускане в действие
LSP800	Процедура: Управление на инциденти и проблеми

10. Оценки

Оценките, свързани с изпълнението на дейностите по настоящия документ, се представят на Годишния преглед от ръководството.

11. Документирана информация

Сигурността на информацията, свързана с изпълняваните дейности се осигурява от процедурите и инструкциите на въведената Система за управление на качеството и информационната сигурност.

Информацията, свързана с личните данни и търговската дейност на клиентите се събира и използва само във връзка с точното и навременно изпълнение на техните заявки и осигуряване на необходимото качество на обслужването.

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

ЛИРЕКС.КОМ	Инструкция: Сервизно поддържане на мрежови решения (Cisco Support)	Версия 5
	LPI301	16 от 24

план за дежурства на DM (форма *L-NET-001- WSCH*)	*симв.наименование*		**Schedule**
	индексация/регистрация		***Schedule_nnnn*** *nnnn* –календарна година
	е-фонд	*активен*	\LOMIS\Cisco Support\Planning\
		достъп	
		съхранение	календарна година
		архивен	архивен \LOMIS\Cisco Support\
		достъп	
		съхранение	3 години

протокол за мрежово сервизно обслужване (форма *L-NET-003-P*)	*симв.наименование*		**NET-P**
	индексация/регистрация		**PCase-** ***case#*** *case#*– пореден номер на протокол от вида
	е-фонд	*активен*	\LOMIS\Cisco Support\Cases\
		достъп	
		съхранение	до приключване, календарна година
		архивен	архивен \LOMIS\Cisco Support\
		достъп	
		съхранение	Безсрочно
	дос-фонд	*активен*	дело (папка) *Сервизни протоколи*
		достъп	
		съхранение	Безсрочно

протокол за замяна на дефектирало устройство (форма *L-NET-004-PRMA*)	*симв.наименование*		**NET-RMA**
	индексация/регистрация		**CSR*nnn*** ***nnn*** – пореден номер на протокол от вида
	е-фонд	*активен*	\LOMIS\Cisco Support\ Protocols\
		достъп	

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

		съхранение	до приключване, календарна година
		архивен	архивен \LOMIS\Cisco Support\
		достъп	
		съхранение	Безсрочно
	дос-фонд	*активен*	дело (папка) *Сервизни протоколи*
		достъп	
		съхранение	Безсрочно

протокол за предоставяне на хардуер за временно ползване (форма *L-ADM-008-OPR*)	*симв.наименование*	
	индексация/регистрация	***Onnnn*** ***nnnn*** – пореден номер на протокол от вида
	е-фонд *активен*	LOMIS\Protokoli\Protokol vremenno polzvane
	е-фонд *достъп*	
	е-фонд *съхранение*	до закриване на case, календарна година
	е-фонд *архивен*	архивен LOMIS\Protokoli\Protokol vremenno polzvane
	е-фонд *достъп*	
	е-фонд *съхранение*	Безсрочно
	дос-фонд *активен*	дело (папка) *Протоколи за временно ползване*
	дос-фонд *достъп*	
	дос-фонд *съхранение*	Безсрочно

11.1. Форми и бланки

ID на формата	*наименование на формата*
L-NET-001- WSCH	седмичен график за дежурства на DM
L-NET-003-P	протокол за мрежово сервизно обслужване
L-NET-004-PRMA	протокол за замяна на дефектирало устройство
L-ADM-008-OPR	протокол за предоставяне на хардуер (устройство, модул) за временно ползване

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

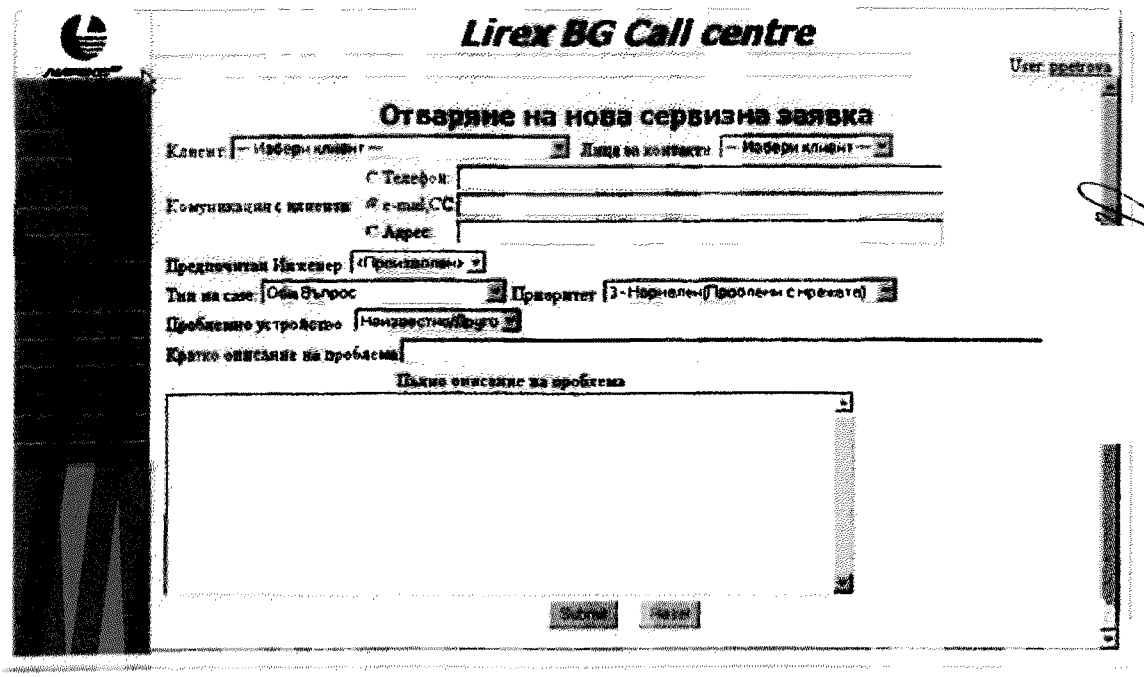
L-PR-003-NET	анкетна карта за проучване степента на удовлетвореност на клиенти на Cisco Support

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

Приложение 1

Сервизна заявка в LCC (cc.lirex.bg)



чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

Приложение 2

Състояния (статус) на сервизна заявка

статус	*Описание*
Новосъздаден/ЛЕ (dispatch)	Поражда се при регистрация на проблем (**"отваряне" на СЗ**).
Чака се реакция от Клиента (cust_pend)	СИ е изискал и очаква информация или резултат от действие от страна на клиента.
Чака се реакция от Инженера (ce_pend)	"Активен" статус за case. Очаква се информация или реакция от назначения по случая СИ.
Чака се реакция от партньора (напр. Cisco-Cisco_pend)	Очаква се информация или реакция от партньора. Статусът е приложим за проблем, който не е от компетенцията на СИ в *Лирекс.БГ* (грешка в операционната система, хардуерен проблем).
Чака се подмяна на устройството от партньора (напр. Cisco - RMA_out)	За решаването на случая се очаква замяна на устройство от партньора, поради хардуерен проблем.
Чака се подмяна на устройството от Лирекс.bg (wap)	Намерено временно решение. Очаква се подмяна на хардуер от Лирекс.бг за окончателно решение.
Затворен (closed)	Проблемът е решен. Приключен case. (**"Затваряне" на СЗ**)

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

Приложение 3

ЕСКАЛАЦИОНЕН ПРОЦЕС

1. Ескалационен процес за приоритет 1

Контролно време (в часове)	*уведомявано длъжностно лице*	*деиствия на длъжностните лиоца*	
		длъжностно лице	*Действия*
1	СИ	СИ	Регистрира case в специализираната система на партньора (напр. Cisco TAC). Докладва на DM и изпълнява неговите нареждания. Информира клиента за ситуацията и предприеманите действия.
		DM	Анализира проблема и ситуацията. Ако е необходимо, определя допълнителни СИ за работа по case. Съвместно с екипа за работа по case, прави анализ и план за действие.
4	DM	DM	Анализира проблема и ситуацията. Взема решение за действие. Докладва на р-л ТКУ и изпълнява неговите нареждания. Сменя СИ, работещ по случая, с друг СИ или определя допълнителни СИ за работа в екипа. Съвместно с екипа за работа по case, прави анализ и план за действие. Информира клиента за ситуацията и предприеманите действия.
24	Р-л ТКУ	Р-л ТКУ	Определя DM за ръководител на екипа / отговорен СИ за работата по case. Информира клиента за ситуацията и предприеманите действия.
		DM	Съвместно с екипа за работа по case, прави анализ и план за действие. Актуализира информацията за case в специализираната система на партньора (Cisco TAC).
48	Висше ръководство	Висше ръководство	Ангажира всички фирмени ресурси за решаване на проблема. Информира клиента за ситуацията и предприеманите действия.
		Р-л ТКУ	Консултира екипа за работа по case.
		DM	Установява контакт с представител на партньора (напр. Cisco TAC Duty Manager). Съвместно с екипа за работа по case, прави анализ и план за действие.

2. Ескалационен процес за приоритет 2

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

Контролно време (в часове)	уведомявано длъжностно лице	действия на длъжностните лица	
		длъжностно лице	Действия
4	СИ	СИ	Регистрира / актуализира case в специализираната система на партньора Cisco TAC). Докладва на DM и изпълнява неговите нареждания. Информира клиента за ситуацията и предприеманите действия.
		DM	Анализира проблема и ситуацията. Ако е необходимо, определя допълнителни СИ за работа по case. Съвместно с екипа за работа по case, прави анализ и план за действие.
24	DM	DM	Анализира проблема и ситуацията. Взема решение за действие. Докладва на р-л ТКУ и изпълнява неговите нареждания. Сменя СИ, работещ по случая, с друг СИ или определя допълнителни СИ за работа в екипа. Съвместно с екипа за работа по case, прави анализ и план за действие. Информира клиента за ситуацията и предприеманите действия.
48	Р-л ТКУ	Р-л ТКУ	Определя DM за ръководител на екипа / отговорен СИ за работата по case. Информира клиента за ситуацията и предприеманите действия.
		DM	Съвместно с екипа за работа по case, прави анализ и план за действие. Актуализира case в системата на партньора (Cisco TAC).
96	Висше ръководство	Висше ръководство	Ангажира всички фирмени ресурси за решаване на проблема. Информира клиента за ситуацията и предприеманите действия.
		Р-л ТКУ	Консултира екипа за работа по case.
		DM	Установява контакт с представител на партньора (Cisco TAC Duty Manager). Съвместно с екипа за работа по case, прави анализ и план за действие.

3. Ескалационен процес за приоритет 3

Контролно време (в часове)	уведомявано длъжностно лице	действия на длъжностните лица	
		длъжностно лице	Действия
12	СИ	СИ	Докладва на DM и изпълнява неговите нареждания. Информира клиента за ситуацията и предприеманите действия.

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

		-DM	Анализира проблема и ситуацията. Ако е необходимо, определя допълнителни СИ за работа по case. Съвместно с екипа за работа по case, прави анализ и план за действие.
48	DM	DM	Анализира проблема и ситуацията. Взема решение за действие. Докладва на р-л ТКУ и изпълнява неговите нареждания. Сменя СИ, работещ по случая, с друг СИ или определя допълнителни СИ за работа в екипа. Съвместно с екипа за работа по case, прави анализ и план за действие. Приключва ("затваря") case, ако прецени. При необходимост, регистрира / актуализира case в системата на партньора (Cisco TAC). Информира клиента за ситуацията и предприеманите действия.
96	Р-л ТКУ	Р-л ТКУ	Анализира проблема и ситуацията. Дава указания за действие. Информира клиента за ситуацията и предприеманите действия.
		DM	Съвместно с екипа за работа по case, прави анализ и план за действие. Приключва ("затваря") case, ако прецени. При необходимост, регистрира / актуализира case в системата на партньора (Cisco TAC).

4. Ескалационен процес за приоритет 4

Контролно време (в часове)	*уведомявано длъжностно лице*	*действия на длъжностните лица*	
		длъжностно лице	*Действия*
24	СИ	СИ	Консултира клиента и/или го информира за предприеманите действия. При необходимост събира необходимата информация за отговор на запитването на клиента. Докладва на DM и изпълнява неговите нареждания.
		DM	Анализира проблема / запитването. Ако е необходимо, определя друг СИ за работа по case.
96	DM	DM	Анализира поставения въпрос / проблем. Взема решение за действие. Докладва на р-л ТКУ и изпълнява неговите нареждания. Сменя СИ, работещ по случая, с друг СИ или определя допълнителни СИ за работа в екипа. Съвместно с екипа за работа по case, прави анализ и план за действие.

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

			Приключва (“затваря”) case, ако прецени. При необходимост, регистрира / актуализира case в системата на партньора (Cisco TAC). Информира клиента за ситуацията и предприеманите действия.

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

ЛИРЕКС.КОМ	ПЛАН ЗА УПРАВЛЕНИЕ НА ВЪНШНА ИТ УСЛУГА (точно наименование на външната ИТ услуга по договор)	Версия .....
	LPN002	1 от 9

1 История на редакциите

версия	описание на промяната	автор	проверил	утвърдил	дата въвеждане
1	Начална редакция				

2 Ограничения

Информацията, съдържаща се в този План, е собственост на Доставчика на ИТ услуга. Никаква част от документа не може да бъде репродуцирана, копирана, предавана или използвана без негово писменото разрешение. Нова редакция на документа се изготвя след съгласувани със страните промени в условията на доставка на услугата.

3 Поверителна информация

Този План може да съдържа информация, свързана с лични данни, търговска тайна, авторски права и др. Информацията не трябва да бъде предоставяна на лица извън пряко отговорните по изпълнение на доставката на тази ИТ услуга. За неоторизирано разпространяване на такава информация служителите носят персонална отговорност.

4 Описание на ИТ услугата

4.1 Наименование на доставяната ИТ услуга

(точното наименования на ИТ услугата по договор/споразумение)

4.2 Описание на доставяната ИТ услуга

(разширено описание и обхват на доставяната ИТ услуга)

4.3 Основание за доставяне на ИТ услугата

(посочва се основанието за доставка на посочената ИТ услуга – договор, споразумение, поръчка, др.)

4.4 Дружество/функционално звено, доставящо ИТ услугата

... ...

4.5 Ръководител на функционално звено, доставящо ИТ услугата

Име:	
Длъжност:	
Тел.:	
Мобилен номер:	
E-mail:	

4.6 Отговорник за ИТ услугата

Име:	

Длъжност:	
Отдел:	
Тел.:	
Мобилен номер:	
E-mail:	

5 Комуникация

5.1 Контакти за връзка с КЛИЕНТА:

Клиент	
Описание	*Данни*
Име:	
Длъжност:	
Отдел:	
Тел.:	
Мобилен номер:	
E-mail:	

Име:	
Длъжност:	
Отдел:	
Тел.:	
Мобилен номер:	
E-mail:	

(ЗАБЕЛЕЖКА: При повече клиенти на един вид услуга с еднакви параметри, адресите могат да бъдат в Приложение към един План за управление на услугата.)

5.2 Контакти за връзка с ОСНОВНИТЕ ПОДДОСТАВЧИЦИ:

ДОСТАВЧИК НА:	Фирми
Поддоставчик:	
Договор/ Споразумение:	
Контактно лице:	
Длъжност:	
Отдел:	
Тел.:	
Мобилен номер:	
E-mail:	

Договор/ Споразумение:	
Поддоставчик:	
Контактно лице:	
Длъжност:	
Отдел:	
Тел.:	
Мобилен номер:	
E-mail:	

5.3 Контакти за връзка с РЕЗЕРВНИТЕ ПОДДОСТАВЧИЦИ:

Към услугите на резервните поддоставчици се прибягва, когато основният поддоставчик не е в състояния да изпълнява задълженията си за период, по-голям от установения в договора/споразумението с него. Комуникацията с основните и резервните поддоставчици, както и условията и начина на преминаване от един поддоставчик към друг е уреден в договора/споразумението с тях.

(Ако това е приложимо към конкретната услуга, да се опише накратко)

ЛИРЕКС.КОМ	ПЛАН ЗА УПРАВЛЕНИЕ НА ВЪНШНА ИТ УСЛУГА (точно наименование на външната ИТ услуга по договор)	Версия .....
	LPN002	4 от 9

ДОСТАВЯНЕ НА:	Данни
Договор/ Споразумение:	
Поддоставчик:	
Контактно лице:	
Длъжност:	
Отдел:	
Тел.:	
Мобилен номер:	
E-mail:	

Договор/ Споразумение:	
Поддоставчик:	
Контактно лице:	
Длъжност:	
Отдел:	
Тел.:	
Мобилен номер:	
E-mail:	

6 Изисквания за ресурси

6.1 Човешки ресурси

Служител	Роля

6.2 Хардуер

Спецификация	Място

6.3 Софтуер

Спецификация	Място

6.4 Документация

Спецификация	Място

6.5 Финансови ресурси:

За изпълнението на договора за доставка на услугата са идентифицирани следните средства:

Предназначение	Средства

6.6 Ресурси, собственост на клиента (*АКО ИМА ТАКИВА):*

Спецификация	Място

7 Процедури и инструкции за изпълнение на доставяната услуга

7.1 Процедури и инструкции от СУКИС:

(ПРИМЕР: Изпълнението на външната услуга „Предоставяне на Интернет достъп" се извършва в съответствие с:

1.1.1. *LPP501 „Управление на Интернет-услуги и продукти";*
1.1.2. *LPI502 „Оперативно управление на мрежовите ресурси";*
1.1.3. *LPI504 „Ескалация на инцидентите при поддържане на Интернет – мрежата".*

7.2 Други ръководства и инструкции:

(Тези документи не са част от СУКИС – те са собственост на клиента или са специфични за дадения клиент процедури и инструкции – **АКО ИМА ТАКИВА**!)

8 Изисквания за нивото на доставяната услуга

8.1 Съгласуван с клиента документ със SLA:

(договор, приложение към договор, самостоятелен документ)

8.2 Контролирани показатели на SLA:

Показател	Стойност

9 Оценка на риска

(1 вариант: Оценката на риска се прави по методиката в процедура LSP200 „Управление на риска"

2 вариант: Качествена оценка на риска по показателите, посочени по-долу. По време на изпълнението на услугата, в процеса на управление на риска, да се вземат предвид и да се изследват внимателно заплахите, които биха повлияли върху успешната реализация, както и да се търси решение в посока намаляване на риска от конкретните заплахи съвместно от ключовите заинтересовани страни – доставчик и клиент).

Такива заплахи биха могли да бъдат обобщени като:

1. Технически -
2. Организационни, административни и регулаторни (законови);
3. Свързани с бизнес условията;
4. Свързани с потребителите.

Рисковете, свързани с тези заплахи, се оценяват експертно като приемливи и с по-високо от приемливото ниво. За рисковете с нива над приемливите се предприемат мерки за намаляване на риска, които се отразяват в Плана за управление на съответната услуга.)

Или по следните показатели:

1. Организационни

Потенциална липса на ясно и конкретно дефинирани задължения за някоя от страните по договора/споразумението за доставка на ИТ услугата.

Потенциална липса на компетентни или неподходящи ресурси.

Некоректно организиране на дейностите във времето.

2. Човешки грешки

Недостатъчно познаване на правила и процедури от страна на работещите.

Неспазване на мерките за сигурност.

3. Отказоустойчивост

Форс-мажорни обстоятелства – наводнения, пожари, земетресения, причиняващи отказ и срив на системите, поради външни, независещи от страните обстоятелства.

4. Инциденти в сигурността

Неправилно управление на инцидентите в сигурността.

5. Хардуерни

Несъвместимост между параметрите на специфицираното оборудване, доставяно по Договора, и параметрите на наличното при Клиента оборудване, към което ще се интегрира новата ИТ услуга.

6. Софтуерни

Забавяне на разработката на приложния софтуер за предоставяната ИТ услуга.

Несъвместимост на използваните операционни системи при клиента и приложния софтуер за ИТ услугата.

Скрити грешки в новата версия на софтуера за управление на ИТ услугата.

ВАЖНО: Няма задължителна методика, но е задължително да се покаже, че е оценен риска при доставяне на определената услуга и той е доведен до приемлив!

10 Управление на капацитета на услугата

(Планът за управление на капацитета за конкретната услуга да се включи тук или в приложение, като тогава трябва има надпис „Приложение към Плана за управление на ....., ред.1) и да има в началото Таблица „История на редакциите").

Управлението на капацитета зависи от конкретната ИТ услуга, като един примерен План за управление на капацитета в най-общия случай съдържа:

- Планиран капацитет за изпълнение на договореното Ниво на услугата, както и измерената натовареност на използвания капацитет;
- Параметрите на договореното Ниво на услугата, както и методите за мониторинг на нейното изпълнение;
- Анализ на въздействието върху ИТ капацитета за осигуряване на услугата при евентуални промени / допълнения / анулиране на ИТ услугата от клиента. Предполагаема тенденция при изпълнението на доставяната услуга (очаквано увеличение / намаление на параметрите) и праговите стойности, при които трябва да се предприемат мерки за разширяване / намаляване на необходимия капацитета за изпълнение на такава услуга.
- Инциденти, довели до неизпълнение на договореното Ниво на услугата, вид на инцидента, причини за появата, мерки за отстраняване на проблема (ако е идентифициран проблем – управление по процедурата LSP800 „Управление на инциденти и проблеми".
- Мерки за предотвратяване на бъдещи подобни инциденти;
- Планирана промяна на капацитета поради въвеждане на нови технологии, свързани с конкретната услуга или наложителни промени поради външни фактори (например законодателни промени – за контрол на услугата и т.н.)

ВАЖНО: Няма задължителна форма на този план, но е задължително да се покаже, че капацитета за доставяне на определената услуга е оценен и е осигурен!)

11 Управление на непрекъснатостта и наличността на услугата

11.1. План за управление на непрекъснатостта и наличността на конкретната услуга

(Планът за управление на непрекъснатостта и наличността на конкретната услуга да се включи тук или в приложение, като тогава трябва има надпис „Приложение към Плана за управление на ....., ред.1) и да има в началото Таблица „История ма редакциите".

Изискванията за непрекъснатост и наличност на конкретната услуга се определят на основата на Споразумението за ниво на услугата и оценката на риска. Да се включат правата за достъп, времето за реакция, допустимо време на прекъсване. Да се покаже как се осигурява непрекъснатото наличие на всички компоненти на услугата – персонал, хардуер, поддръжка,

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

осигуряване на друг поддоставчик при прекъсване на доставката от основния поддоставчик, достъпът до списъка с лицата за контакти и базата с данните за управление на конфигурацията да са достъпни, когато нормалният достъп до офиса е затруднен.

Плановете да се преглеждат поне веднъж годишно (доказателство - нова редакция всяка година), за да се осигури спазване на изискванията при всички обстоятелства – от нормална работа до значителни прекъсвания на услугата. Плановете за непрекъснатост и наличност трябва да се изпитват отново при всяка значителна промяна на бизнес средата.

Достъпността на услугата трябва да бъде измервана и записвана. Непланирана недостъпност на услугата трябва да бъде разследвана и да се предприемат подходящи коригиращи действия).

12 Управление на инциденти и проблеми

Информация за инцидент се получава от (посочва се приложимото за съответната услуга):

- системата за наблюдение на доставяната услуга;
- от клиентите по установените канали за комуникация, посочени в договора, приложенията към него или Споразумението за ниво на услугата;
- по начина, посочен в процедурата LSP420 „Service Desk".

(Да може да се демонстрира начина на записване, задаване на приоритет, класифициране, обновяване, придвижване по йерархията, окончателно решение и официално приключване на всички инциденти.)

Клиентът се информира от отговорника на съответната услуга или от отговорника на съответното звено за напредъка на докладвания от него инцидент, както и се предупреждава предварително, ако нивото на услугата не може да бъде постигнато за определен период от време.

13 Управление на рекламации

Рекламации от клиенти (писмено или устно изразено недоволство от предлаганата услуга) се получава от клиентите по установените канали за комуникация, посочени в договора, приложенията към него или Споразумението за ниво на услугата, както и по начина, посочен в процедурата LAP001 „Измерване степента на удовлетвореност на клиентите".

Приелият рекламацията служител уведомява отговорника на съответното звено с цел вземане на отношение и предприемане на превантивни или коригиращи действия.

За получените рекламации, на първото мениджърско събиране, ръководителите на съответните дейности/процеси докладват за всеки конкретен случай, както и за резултатите от анализа и предприетите мерки по този повод.

Когато клиентът не е доволен от уреждането на неговата рекламация или има спор по изпълнението на договора за доставка на ИТ услугата, както и за всички въпроси, неуредени в този договор, се прилага българското гражданско и търговско право, като страните уреждат отношенията си чрез споразумение. При непостигане на съгласие спорът се отнася за решаване пред компетентния съд.

14 Отчитане и оценяване на ИТ услугата

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

Отчети за доставяните ИТ услуги се предоставят на клиентите от техните ръководители на съответните функционални звена съгласно условията на съответния договор.

Резултатите за предоставяните ИТ услуги от съответните функционални звена се докладват от техните ръководители на Прегледите от ръководството на СУКИС в съответствие с изискванията на процедура LMP003.

15 Промяна в условията на доставяната услуга

Промяна в условията на доставяне на ИТ услуга се инициира по предложение на клиента, от функционалното звено-доставчик на услугата или по решение от Прегледа на ръководството. Процесът на промяна се извършва в съответствие с процедура LPP012 „Управление на промените".

След съгласуване и приемане от клиента (и от поддоставчика – ако е необходимо) на промените, по разпореждане на ръководителя на функционалното звено- доставчик на услугата, се изготвя и утвърждава нова редакция на настоящия План за нейното управление и променената ИТ услуга се въвежда в конкретната работна среда.

Старата редакция на Плана се съхранява (в електронен вид или на хартия) в съответния архив на ИТ услугата.

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

ЛИРЕКС.КОМ	Процедура: Управление на здравословните и безопасни условия на труд	Версия 5
	LRP004	1 от 26

1. История на редакциите

версия	описание на промяната	автор	проверил	утвърдил	дата въвеждане
3	Отразяване на забележки от външен одит по OHSAS 18001:2007	Б.Йорданов	К.Иванов	Д.Илиева	15.11.2012
4	Въвеждане на строителни дейности в обхвата по BS OHSAS 18001:2007	Б.Йорданов	К.Иванов	Д.Илиева	25.07.2014
5	Актуализиране на СУКИС	М. Йончева	К. Иванов	Д. Илиева	01.06.2019

2. Предназначение

Процедурата има за цел да определи елементите на Системата за управление на здравословните и безопасни условия на труд (СУЗБУТ), техните взаимодействия и начините им на управление и контрол в рамките на СУКИС в дружествата Лирекс.ком. СУЗБУТ се въвежда, управлява и контролира в съответствие с изискванията на стандарта ISO 45001 и действащото законодателство в тази област.

3. Приложимост

Процедурата се прилага по отношение на здравословните и безопасни условия на труд за всички процеси и дейности, изпълнявани от служителите на Лирекс.ком, вкл. временно наетите; подизпълнителите или посетителите на работните места в дружествата или на техни външни обекти.

4. Отговорности

4.1. Висше ръководство:

- Осигуряват здравословните и безопасни условия на труд на служителите;
- Определят политиката по осигуряване на здравословните и безопасни условия на труд, включваща организацията на работа, елементите на работната среда и трудовия процес, както и социалните взаимоотношения;
- Организират оценката на професионалния риск за здравето и безопасността с помощта на външни организации (СТМ и др.), която обхваща работните процеси и оборудване, помещенията, работните места, организацията на труда, използването на материалите и други странични фактори;
- Утвърждават подходящите мерки за управление на риска в съответствие с направената оценка с цел осигуряване защитата на работещите и на другите лица;
- Осигуряват ефективен контрол за извършване на работата без риск за здравето и по безопасен начин;
- Отчитат специфичните опасности за служителите, които се нуждаят от специална закрила, включително и тези с ограничена работоспособност и осигурява съответните улеснения за тях.

- Предприемат необходимите мерки за координация на действията за осигуряване на здравето и безопасността при работа, когато на една работна площадка се извършват работи или дейности от и служители и на други работодатели.

4.2. Упълномощен представител на Ръководството (УПР) по Системата за управление на здравословните и безопасни условия на труд (СУЗБУТ):

- Организира разработването на политиките, процедурите и инструкциите от Системата за управление на здравословните и безопасни условия на труд (СУЗБУТ) в рамките на СУКИС;
- Разглежда и анализира предложенията за актуализация, изменение и допълнение на документите на СУЗБУТ;
- Осъществява постоянна оперативна координация, контрол и провежда дейности за осигуряване функционирането, поддържането и развитието на СУЗБУТ;
- Контролира обучението на персонала на дружествата по въпроси, свързани със СУЗБУТ;
- Организира провеждането на вътрешни одити на СУЗБУТ;
- Контролира и анализира прилагането, поддържането и подобрението на процесите от СУЗБУТ в рамките на СУКИС;
- Представлява пред и се занимава с комуникацията и връзките с външните за организацията заинтересовани страни като държавни и контролни органи; сертифициращи, браншови или други неправителствени организации; клиенти, доставчици, партньори и техните представители по въпросите на СУЗБУТ;
- Организира провеждането на Прегледите от ръководството на СУЗБУТ, на които се отчита състоянието й, изпълнението на целите и предлага мерки за нейното развитие и усъвършенстване;

4.3. Орган по безопасност и здраве при работа (ОБЗР) - служител по безопасност и здраве в дружествата Лирекс.ком:

- Организира и координира дейността по СУЗБУТ в конкретното дружество;
- Консултира работещите в съответното дружество по прилагането на изискванията на СУЗБУТ и подпомага управителите и другите длъжностни лица по прилагане на изискванията за осигуряване на безопасни и здравословни условия на труд при организиране и осъществяване на трудовата дейност;
- Провежда инструктажи на служителите по ЗБУТ;
- Контролира служителите по спазването на изискванията на въведената СУЗБУТ и на нормите и изискванията на законодателството по ЗБУТ;
- Предлага на Ръководството и прилага мерки за въздействие при нарушаване на изискванията и нормите по ЗБУТ.

4.4. Отговорник на Системата за управление на здравословните и безопасни условия на труд (Технически организатор на административно-стопански дейности (АСД)):

- Участва при изработването на документите по ЗБУТ за дружествата, за които отговаря;

- Организира снабдяването на служителите с лични предпазни средства и провежда обучение за тяхното използване и правилно съхранение;
- Организира обучението на работниците, за придобиване на квалификационна степен по електробезопасност и за работа на височина;
- Оказва съдействие на органите по трудова медицина при изпълнение на задълженията им;
- Участва при изработването и актуализиране на плановете за действие при стихийни бедствия и пожари и на плановете за евакуация при тях;
- Организира проверката на изправността на подвижните средства за гасене на пожари;
- Води регистър на актовете за трудови злополуки;
- Извършва текущи ремонти на оборудването в офисите.

4.5. Комитет / група по условия на труд (КУТ / ГУТ):

- Обсъжда цялостната дейност по опазване на здравето и осигуряване на безопасността на служителите в съответното дружество;
- Обсъжда на резултатите от оценката на професионалния риск и анализите на здравното състояние на служителите, докладите на службата по трудова медицина и други въпроси по осигуряване и опазване здравето и безопасността на работещите в Лирекс.ком;
- Обсъжда планираните промени в организацията на труда и работните места и предлага решения за опазване на здравето и осигуряване на безопасността на служителите;
- Извършва проверки по спазване на изискванията за здравословни и безопасни условия на труд в съответното дружество;
- Следи състоянието на трудовия травматизъм и професионалната заболеваемост на служителите от дружеството;
- Участва в разработването на програми за информиране и обучение на служителите по проблемите на здравословните и безопасни условия на труд.

4.6. Ръководител на функционално звено:

- Съдейства на органите по безопасност и здраве и СТМ при изпълнение на задълженията им по осигуряване на здравословни и безопасни условия на труд;
- Контролира спазването на изискванията за техника на безопасност от служителите във функционалното звено;
- Участва в Прегледите от Ръководството на СУКИС по дейностите по здраве и безопасност и развитието на Системата за здравословни и безопасни условия на труд.

4.7. Ръководител на офис:

- Организира и координира дейността по СУЗБУТ в конкретния офис;
- Оказва съдействие на органите по безопасност и здраве и СТМ при изпълнение на задълженията им;

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

- Участва при изработването и актуализиране на плановете за действие при стихийни бедствия и пожари и на плановете за евакуация при тях;
- Създава необходимата организация за правилното съхраняване и опазване на подвижните средства за гасене на пожар;
- Води регистър на актовете за трудови злополуки;
- Ръководителите на офиси извън София провеждат начален и периодичен инструктаж по ЗБУТ и организират извършването на ежедневен инструктаж на своите служители, когато това се налага.

4.8. Ръководител на проект:

- Определя специфичните мерки за здраве и безопасност при изпълнение на нов проект в зависимост от опасността на изпълняваните дейности от работещите в съответствие с инструкцията LRI004;
- Когато изпълняваните дейности изискват, той:
  - определя един или повече Отговорни инструктори, които да провеждат ежедневен инструктаж по ЗБУТ и пожарна безопасност, когато това се налага на работещите по проекта на външен обект;
  - подготвя заповед със задълженията и отговорностите на Отговорния инструктор;
  - предоставя на Отговорния инструктор Книгата за ежедневен инструктаж, в която предварително е записал обекта за работа и името на проекта;
  - след приключване на проекта, използва Книгата за ежедневен инструктаж и за други обекти, а след нейното изписване я предава на Техническия организатор на АСД за съхранение;
- Предприема необходимите мерки за координация на действията за осигуряване на здравословни и безопасни условия на труд, когато на един обект или работна площадка се извършват работи или дейности от служители и на други работодатели;
- Прилага по своя преценка допълнителни специфични мерки за осигуряване на ЗБУТ при изпълнение на дейности на външен обект.

4.9. Отговорен инструктор по ЗБУТ:

- След преминаване на допълнително обучение по здравословни и безопасни условия на труд му се издава удостоверение за завършен курс по ЗБУТ и му се делегират права за провеждане на ежедневен инструктаж;
- Провежда ежедневен инструктаж по безопасност, хигиена на труда и пожарна безопасност на работещите на същия ден на обект с зависимост от опасността на изпълняваните дейности в съответствие с инструкцията LRI004 „Осигуряване на здравословни и безопасни условия на труд а работните места";
- Води и съхранява Книгата за ежедневен инструктаж до приключване на проекта, след което я предава на Ръководителя на проекта.

4.10. Служба по трудова медицина (СТМ) – външна организация

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

- Консултира и подпомага управителите, комитетите и групите по условия на труд в планирането, организирането и изпълнението на задълженията му по осигуряване на здравословни и безопасни условия на труд и за укрепване здравето и работоспособността на работещите във връзка с извършваната от тях работа;
- Участва в идентифициране на опасностите на работните места и оценката на професионалните рискове в на работните места;
- Разработва и предлага мерки за отстраняване и намаляване на риска за здравето и безопасността при работа;
- Участва в разработването и включването на програми за здравословни и безопасни условия на труд в цялостната политика на управление на фирмата;
- Наблюдава здравословното състояние на работниците и анализирането му във връзка с извършваната работа;
- Участва в анализа на трудовите злополуки и професионалните болести;
- Обучава служителите и длъжностни лица по правилата за опазване на здравето при работа и оказване на първа помощ.

4.11. Всички служители на дружествата Лирекс.ком, вкл. временно наетите и клиентите на територията на дружествата:

- Спазват процедурите, инструкциите и указанията за безопасност и здраве при работа;
- Длъжни са да се грижат за здравето и безопасността си, както и за здравето и безопасността и на другите лица, пряко засегнати от неговата дейност, в съответствие с квалификацията си и дадените им инструкции;
- Спазват Правилника за вътрешния трудов ред;
- Притежават необходимите документи за правоспособност за извършване на дейностите, за които са наети;
- Използват правилно оборудването и инструментите;
- Информират незабавно съответните длъжностни лица за всяка възникнало обстоятелство, което може да представлява непосредствена опасност за здравето им и за всички неизправности в средствата за колективна защита.
- Съдействат на съответните длъжностни лица при изпълнението на мерките за осигуряване на здравословни и безопасни условия на труд.

5. Политика по здравословни и безопасни условия на труд

Настоящата политика по отношение на здравословните и безопасни условия на труд е част от общата политика на интегрираната Система за управление на качеството и информационната сигурност (СУКИС) в дружествата Лирекс.ком. Тази политика е насочена конкретно към непрекъснато подобряване на работната среда в изпълнение на действащите изисквания на българското законодателство и има за цел осигуряване на здравословни и безопасни условия на труд при всички дейности и процеси в дружествата; защита на интересите на работещите в тях и на клиентите, съблюдаване очакванията на обществото и изискванията на държавните институции в това отношение.

Политиката на Ръководството по отношение на здравословните и безопасни условия на труд в дружествата Лирекс.ком включва:

- Непрекъснато подобряване на работната среда в изпълнение на действащите изисквания на българското законодателство с цел постигане на високо качество на извършваните дейности; защита на здравето и работоспособността както на своите служители, така и на всички посетители, намиращи се на територията на дружествата и на очакванията на обществото.
- Ефективно управление на рисковете за здравето и сигурността, намаляване до минимум рисковете за персонала и другите заинтересовани страни, свързани с дейността на дружествата;
- Непрекъснато наблюдение и измерване на процесите и дейностите, имащи значимо въздействие върху работната среда;
- Постоянно идентифициране на опасностите и оценяване на риска за здравето и безопасността при работа, определяне на мерки и осигуряване на ресурси за неговото овладяване;
- Стриктно спазване на приложимите законови и други изисквания, свързани с идентифицираните опасности и оценените рискове за здравословните и безопасни условия на труд;
- Периодично преглеждане на изпълнението на общите и конкретни цели по ЗБУТ и актуализирането им при необходимост;
- Осигуряване на достатъчно информация, инструктажи и обучение на служителите и засилване на персоналната отговорност към спазването на безопасните и здравословни условия на труд;
- Активно сътрудничество с упълномощените организации за контрол на здравословните и безопасни условия на труд и всички заинтересовани страни при решаване на проблемите, свързани с осигуряването на ЗБУТ;
- Разследване и регистриране на всеки инцидент, злополука и/или професионално заболяване, с цел анализ и предприемане на мерки за превенция срещу повторната им поява.

Политиката по отношение на здравословните и безопасни условия на труд в дружествата Лирекс.ком се намира на Интернет сайта и на вътрешния портал. Тя се разглежда и обсъжда на периодичните Прегледи от ръководството на СУЗБУТ и се актуализира при необходимост.

6. Въвеждане на СУЗБУТ

6.1. Общи изисквания

Системата за управление на здравословните и безопасни условия на труд (СУЗБУТ) в Лирекс.ком се основава на резултатите от оценяването на риска. Това включва оценяване на условията на труд и опасностите на работните места по дружества, оценката на риска от тях и определяне на съответните мерки за неговото премахване или намаляване в съответствие с изискванията на нормативните актове и другите изисквания (вътрешно-фирмени документи като правилници, ръководства, инструкции и др.).

Тези дейности се включват в **Програмите за оценяване на риска** (*Progr_Ocen_Risk.doc*), съставени за всички офиси на дружествата и утвърдени от Управителя. Тези Програми се намират на Вътрешния портал на дружествата Лирекс.ком.

Оценяването на риска е извършва по решение на Управителя под методическото ръководство на Службата по трудова медицина. В оценяването активно участват лицата, ангажирани в трудовия процес - ръководители, служители и техните представители в комитетите и групите по условия на труд, органите за безопасност и здраве в различните дружества.

6.2. Оценяване на професионалните рискове в дружествата Лирекс.ком

Оценяването се прави в съответствие със Закона за здравословни и безопасни условия на труд и Наредба №5 на МТСП и МЗ за реда, начина и периодичността на извършване на оценка на риска. Практически оценяването се реализира в два основни етапа:

- Идентифициране на опасностите (трудовите дейности или ситуациите, които е възможно да имат увреждащо действие) на работните места. Този етап включва събиране на информация от всички видове източници от и извън дружествата.
- Оценка на професионалния риск, която показва необходимо ли е прилагане на мерки за отстраняване или намаляване на установения риск.

6.2.1. Идентифициране на опасностите на работните места

От СТМ и съответно членовете на КУТ/ГУТ във всяко дружество е направен анализ на трудовите дейности, който включва определяне на работните места в тях и идентифициране на потенциалните опасности. Идентифицирането на опасностите включва:

- Анализ на често повтарящите се, както и на възможните извънредни дейности, които се изпълняват на работните места;
- Преглед на дейността на всички, които присъстват на работните места (служители, подизпълнители, клиенти или посетители;
- Поведението на хората, техните способности и други човешки фактори;
- Преглед на опасностите извън конкретното работно място, но които могат да повлияят неблагоприятно на ЗБУТ на служителите на това работно място;
- Опасностите от дейности, изпълнявани от други служители в близост до конкретно работно място;
- Инфраструктурата, съоръженията и материалите на работното място;
- Промени или предложени промени в дружествата, в СУЗБУТ или в изпълняваните дейности;
- Приложимите изисквания на нормативните актове по отношение на оценяването на риска от опасностите и предприемането на необходимите мерки;
- Състоянието на работните места и работните площадки, процесите, инсталациите, машините и съоръженията, процедури и инструкциите за работа и за нейната организация, включително тяхното приспособяване към човешките възможности.

Прилагат се следните подходи за идентифициране на опасностите:

- Наблюдение на трудовия процес - насочено е към конкретните действия и начините, по които те се извършват. Отчита се възможността за промяна в начина на работата от самия работещ и последствията от това по отношение на възникване на нови, непредвидени опасности. Наблюдението се осъществява от служители на СТМ и ОБЗР със сътрудничество от страна на работещите, като работната обстановка се обсъжда с тях.

- Използване на анкетни карти - въпросите в тях са насочени към технологичното оборудване, работата, работния процес и работната среда и имат за цел да установят потенциалните опасности за всяка дейност на работното място, а също така и произхода на опасността, готовността на работещите сами да въздействат на тази опасност и към предприетите мерки за колективна и индивидуална защита и тяхната ефективност. Използват се: Карта за оценка на условията на труд (Karta_Ocenka_uslovia_trud.doc) и Анкетна карта за работните места в офисите на дружествата (Anketna_Karta_rab_mesta.doc).
- Измерване параметрите на работната среда - за определяне на съответните опасности се използват данни от актуалните измервания на параметрите на работната среда: стойностите на елементите за микроклимат, шума, вибрациите и осветлението. За целите на оценката на риска измерванията се извършват от акредитирана лаборатория. Резултатите от измерванията дават обективната информация за рисковите фактори на работното място

При използването на посочените подходи от СТМ и с участието на ОБЗР, КУТ/ГУТ и служители от всички офиси на дружествата Лирекс.ком се идентифицират потенциално опасните фактори на работната среда. Те се отразяват в разработените за всяко работно място Карти за идентифициране на опасностите и оценка на риска за безопасност и здраве на работещите (*Karti_Ocenki_RM & Risk*).

6.2.2. Оценка на професионалните рискове

Оценката на риска е качествено или количествено градиране на риска по определена методика относно допустимостта на риска. Оценката на риска от потенциално опасните фактори на работната среда в офисите на дружествата Лирекс.ком се извършва по Методиката за оценка на професионалния риск (***Metodika-Ocenka_Risk.doc***), предложена от СТМ. Тя се намира на Вътрешния портал.

За всяка идентифицирана опасност се определят елементите на риска, които тя създава по посочената методика, а именно:

- Вероятността за нанасяне на конкретната вреда се определя от:
  - честотата, продължителността и спецификата на въздействие;
  - възможността да настъпи опасното събитие;
  - техническите средства за избягване или ограничаване на вредата;
  - човешките възможности за избягване или ограничаване на вредата – квалификация, опит, практически знания и умения, осмисляне на рисковете, взаимодействие между хората, психологични, социални и ергономични аспекти и др., които могат да окажат въздействие върху риска;
  - стойността на измерените стойности на факторите на работната среда от оторизирани лаборатории.
- Експозиция - отчита времето на въздействие на идентифицираната опасност върху работещите и спецификата на излагане на тази опасност;
- Последици от вредата (тежест) - оценява се в съответствие с:
  - вида на обектите, подлежащи на защита – хора, имущество, работна и околна среда;

- тежестта на възможните наранявания или увреждания на здравето – незначителни, сериозни, опасни, фатални;
- обхвата на вредата.

След оценката на риска от всяка опасност на работните места по Методиката се установява допустимостта на определения риск и необходимостта от прилагане на мерки за неговото предотвратяване или намаляване и ограничаване. Основните критерии за установяване допустимостта на риска са:

- съответствие с разпоредбите на нормативните актове за осигуряване на здравословни и безопасни условия на труд;
- приложението на принципите за превантивна дейност, посочени в Закона за здравословни и безопасни условия на труд;
- отчитането на информацията от източниците на информация, които нямат силата на нормативен акт, но прилагането им осигурява ЗБУТ.

Картите с идентифицираните опасности и оценка на риска за безопасност и здраве на работещите на всички работни места в офисите на дружествата Лирекс.ком и обобщената оценка на професионалния риск по дружества (*Ocenka_Risk.doc*) се намират на Вътрешния портал.

6.2.3. Управление на риска

Управлението на риска е процес на предотвратяване, отстраняване или ограничаване на риска за здравето и безопасността, включващ предприемането на организационни, контролни, комуникационни, технически и технологични мерки в дейностите на дружествата Лирекс.ком.

Определянето на конкретните мерки (дейности) е в зависимост от оценката на риска за съответната опасност или работно място. Мерките за управление на риска се планират и прилагат, като се цели последователно:

- премахване на опасността или риска;
- заместване на опасни дейности с по-малко опасни;
- прилагане на технически контрол или други организационни мерки;
- предупредителни и/или административни мерки;
- използване на средства за колективна защита;
- използване на средства за индивидуална защита.

Мерките за управление на риска се включват в Програмите за предотвратяване на професионалния риска в дружествата Лирекс.ком. Тези Програми се отнасят за периода, за който е актуална оценката на професионалния риск. Програмите се изготвят от СТМ съвместно с КУТ/ ГУТ на съответното дружество и се одобряват от Управителя.

При нова оценка на риска Програмите за предотвратяване на професионалния риска се актуализират в съответствие с новите стойности.

6.2.4. Преразглеждане на оценката на риска

Оценката на риска се преразглежда, когато:

- настъпят промени, които могат да окажат влияние върху риска като въвеждане на нови производствени процеси, оборудване, продукти и материали, промяна на организацията на труда, нови сгради и помещения, реконструкция на съществуващи и др.;

- след настъпили промени в приложимата нормативна уредба;
- оценката е направена на основата на данни и информация, станали невалидни или неподходящи;
- има условия оценката да бъде подобрена;
- прилаганите защитни и профилактични мерки са неефективни или неадекватни;
- резултатите от разследвания на злополуки, аварии, професионални заболявания и инциденти без злополуки налагат преразглеждане.

Преразглеждане на оценката на риска се извършва:

- по преценка на Висшето ръководство;
- по предписание на контролните органи.

Периодичността на оценяване на риска се определя от Висшето ръководство, в зависимост от установения риск и в съответствие с изискванията на нормативните актове.

При планиране на промени, свързани с организационна структура, нови изисквания на приложимата нормативна база, модифициране или въвеждане на нови работни процеси, дейности, материали или оборудване в дружествата Лирекс.ком, преди тяхната реализация, по решение на Висшето ръководство, се извършва повторно идентифициране на опасностите на работното място и оценка на риска. Това оценяване се консултира с работещите, КУТ/ ГУТ, ОБЗР и СТМ.

След приемането на решението за промяна, УПР и ОЗБУТ информират, обучават и консултират всички заинтересовани страни, имащи отношение към конкретното изменение.

6.3. Изисквания на нормативните актове и други изисквания по ЗБУТ

Оценяването на риска по същество е оценяване на съответствието на условията на труд с приложимото законодателство и с другите изисквания (стандарти, правилници и ръководства по безопасност при работа и др. п.) на производители, браншови организации и други заинтересовани страни.

С цел изпълнение на изискванията на законодателството по здраве и безопасност за дейностите, продуктите и услугите на дружествата Лирекс.ком е създаден Регистър на нормативни актове по ЗБУТ (RegisterLegOHSAS). Той се намира на Вътрешния портал на дружествата Лирекс.ком. Регистърът се поддържа актуален от УПР по СУЗБУТ или определен от него служител. Достъпът до актуалното съдържание на нормативните актове се осигурява от намиращите се в Интернет бази данни с такава информация.

В съответствие с приложимите за дейностите, продуктите и услугите на дружествата нормативни актове са изготвени и утвърдени вътрешно-фирмените документи, които включват изисквания по ЗБУТ (Правилник за вътрешния трудов ред, Инструкции за безопасност при различни дейности и др.). Всички те се намират на Вътрешния портал със свободен достъп от всички служители на Лирекс.ком.

6.4. Цели и програми по ЗБУТ

6.4.1. Цели по ЗБУТ

Целите се определят в съответствие с утвърдените основни цели на СУКИС, на политиката по ЗБУТ, включително и ангажимента за непрекъснато подобряване, направената оценка на риска, правните и други изисквания, работните процеси в дружествата, причините за трудовия травматизъм и професионалната заболеваемост, въведените корпоративни изисквания по ЗБУТ,

финансовите и бизнес възможности, както и с препоръките от външни контролни или консултиращи органи.

Целите по здравословни и безопасни условия на труд в рамките на СУЗБУТ се приемат, обсъждат и отчитат на Прегледите от Ръководството на интегрираната СУКИС в дружествата Лирекс.ком. Те се отразяват в документа Програма по ЗБУТ на дружествата Лирекс.ком (OHSAS_Progr-YYYY).

6.4.2. Програма по ЗБУТ

За постигане на целите по ЗБУТ, ежегодно се изготвя Програма по ЗБУТ на дружествата Лирекс.ком. В нея се отразяват дейностите за постигане на поставените цели, както и конкретните мерки за осигуряване на ЗБУТ от Програмите за предотвратяване на професионалния риск (Progr_Predot_Risk.doc) за всички офиси на дружествата.

Програмата се утвърждава от Висшето ръководство и се намира на Вътрешния портал на Лирекс.ком. В нея са посочени отговорните лица, сроковете и ресурсите за изпълнение на поставените цели.

Изпълнението на целите в Програмата по ЗБУТ се разглежда и обсъжда на заседания на КУТ/ ГУТ в дружествата и на периодичните прегледи от Ръководството на СУЗБУТ в рамките на интегрираната СУКИС.

Когато е необходимо, Програмата се актуализира в съответствие с промените в дейностите, продуктите, услугите или условията на работа в офисите на дружествата Лирекс.ком. Новата Програма за ЗБУТ се утвърждава от Висшето ръководство.

7. Организация на дейностите по ЗБУТ

7.1. Общи изисквания

Целта е дейностите по управление на ЗБУТ в рамките на СУКИС да осигуряват:

- въвеждане на изискванията за ЗБУТ според съответните нормативни актове и другите приложими изисквания (вътрешно-фирмени документи като правилници, инструкции, ръководства за работа и др.) и осигуряване на необходимите ресурси за това;
- организиране и изпълнение на работните и спомагателните процеси в дружествата Лирекс.ком в съответствие с въведените изисквания за ЗБУТ;
- ефективно и ефикасно постигане на поставените цели по ЗБУТ;
- подобряване на резултатите, характеризиращи ЗБУТ.

7.2. Ресурси

- Ръководството отговаря за осигуряването на необходимите ресурси за въвеждане и поддържане на ЗБУТ в дружествата Лирекс.ком в рамките на СУКИС, включително оборудването, служителите и тяхното обучение;
- Ръководството определя Упълномощен представител на Ръководството (УПР) по Системата за управление на здравословни и безопасни условия на труд (СУЗБУТ), който осигурява тази система да бъде разработена, внедрена и поддържана в съответствие с изискванията на стандарта ISO 45001 в рамките на интегрираната СУКИС. УПР докладва на Прегледите от Ръководството за изпълнение на СУЗБУТ в интегрираната СУКИС;

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

- Висшето ръководство определя служителите, които имат конкретни права и отговорности по ЗБУТ – Органи по безопасност и здраве при работа (ОБЗР) и Отговорници по пожарна и аварийна безопасност (ПАБ) по дружества и издава съответните заповеди за това.
- Висшето ръководство упражнява контрол върху дейностите по ЗБУТ и ПАБ и делегира права в това отношение на ръководителите на всички нива в дружествата Лирекс.ком.

7.3. Компетентност, обучение и осъзнаване

Ръководството осъзнава важността на квалификацията и компетентността на персонала в дружествата Лирекс.ком по отношение на ЗБУТ. Като предпоставка за безопасно изпълнение на служебните задължения, наемането на служители с необходимата професионална подготовка и квалификация се извършва в съответствие с процедурата LRP002 „Набиране и подбор на персонал".

Компетентността, обучението и осъзнаването на служителите по отношение на здравето и безопасността при работа се осигурява от:

- Редовно провежданите инструктажи по ЗБУТ;
- Специализирано обучение на служителите, които извършват дейности, за които се изисква определена правоспособност (напр. квалификационна група по електробезопасност, работа на височина, шофьори и др.);
- Периодично обучение на ОБЗР и на служителите, които участват в КУТ/ ГУТ.

7.3.1. Инструктажи по ЗБУТ

Всички служители на дружествата Лирекс.ком, вкл. временно наетите и клиентите на територията на дружествата се информират за опасностите на работното място и се инструктират по безопасност и здраве при работа. Инструктажите се провеждат в съответствие с Наредбата за условията и реда за провеждането на периодично обучение и инструктаж на работниците и служителите по правилата за осигуряване на здравословни и безопасни условия на труд:

- при постъпване на работа на служители на Лирекс.ком и на клиенти при обучение на работни места в дружествата;
- при преместване на друга работа или промяна на работата на служители;
- при въвеждане на ново или при промяна на работно оборудване и технология;
- периодично за поддържане и допълване на знанията на работещите в дружествата по безопасност и здраве при работа;

Инструктажите по безопасност и здраве при работа се подразделят на:

- Начален - целта е новопостъпилите служители да се запознаят с основните правила и изисквания по ЗБУТ и ПАБ в дружеството, както и с изискванията към тяхното поведение с оглед опазване на здравето и живота им;
- На работното място (вкл. и на клиенти за обучение) – целта е практическо запознаване на служителя с конкретните изисквания за безопасната работа и се провежда на работното място, преди да му бъде възложена самостоятелна работа. Когато е възможно, началния инструктаж и инструктажа на работното място се извършват едновременно;

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

- Периодичен - целта е да се поддържат и допълват знанията на служителите по ЗБУТ и ПАБ;
- Ежедневен - целта е служителите, които извършват дейности с по-висок риск, да се инструктират всеки ден с цел опазване на здравето и живота им;
- Извънреден – целта е да не се допуска повтарянето на злополуки или аварии по вина на работещите. Инструктажите се провеждат от ОБЗР в съответното дружество по ред, условия и продължителност, определени със заповеди на Управителите на дружествата *(Zap.insruktaji.pdf, Zap.vid.instruktaji.pdf)*.

В зависимост от изпълняваните работи, инструктажите се провеждат по програмите за съответния инструктаж, одобрени от Управителя. Те са поставени на Вътрешния портал.

Проведените инструктажи се документират в Книги за инструктажите, които се съхраняват от ОБЗР на дружествата. Органът по безопасност и здраве, провел началния инструктаж на лицата, които постъпват на работа, издава служебна бележка, която се съхранява в личното досие на работещия. Бележката се подписва от извършващия инструктажа и от инструктирания служител.

При изпълняване на дейности на обект на клиент, в зависимост от характера на работа, по преценка на Ръководителя на проекта и след издаване на заповед, специално обучен Отговорен инструктор провежда ежедневен инструктаж по безопасност и здраве на работещите в съответствие с LRI004 „Осигуряване на здравословни и безопасни условия на труд на работните места".

На всички водачи на служебни автомобили в дружеството се провежда ежедневен инструктаж от упълномощено лице. Такъв вид инструктаж се провежда и на служителите, на които временно е предоставено правото да управляват служебен автомобил.

Извънреден инструктаж се провежда по нареждане на Висшето ръководство след всяка трудова злополука, пожар, промишлена авария, природно бедствие или при констатирани груби нарушения на ЗБУТ; при промяна на технологии, машини, организацията на работа или по предписание на контролен орган. Той се регистрира в Дневника за трудови злополуки и професионални заболявания, който се съхранява от ОБЗР.

Инструктажи на клиентите, които присъстват за обучение на работни места в офисите на дружествата се документират на бланка "InstructionOHSAS-Extern.doc".

7.4. Специализирано и периодично обучение по ЗБУТ

Служителите, които извършват настройка и ремонт на компютърна техника и монтаж на системи за сигурност, се допускат до самостоятелна работа само след успешно положен изпит за придобиване на трета квалификационна група за електробезопасност от лицензирана организация. ОБЗР на дружеството води отчет на работниците които трябва да притежават такива документи за правоспособност. Същото се отнася и за работниците които извършват работа на височина.

Всички служители, които управляват служебните МПС на дружествата Лирекс.ком, трябва да притежават необходимите свидетелства за управление, предвидени в **Закона за движението по пътищата**, с което се удостоверява правоспособността им за управление на МПС от съответната категория. Свидетелствата се подновяват от водачите на определените за това периоди.

Служителите, които са избрани в КУТ/ ГУТ и ОБЗР в дружествата Лирекс.ком периодично се обучават от служители на СТМ.

7.4.1. Оценяване на ефективността на обучението по ЗБУТ

Ефективността от провежданите инструктажи и обучения по ЗБУТ се оценява при периодичните проверки по работните места от ОБЗР, по констатираните нарушения на процедурите и инструкциите от СУЗБУТ при вътрешните и външните одити, по трудовия травматизъм и заболеваемост. Тези показатели се контролират при мониторинга по ЗБУТ и се отчитат на периодичните Прегледи по СУКИС.

7.5. Обмен на информация, участие и консултиране по отношение на ЗБУТ

Служителите се информират за своите ангажименти по ЗБУТ при провежданите инструктажи по ЗБУТ, от преките си ръководители или от мениджърите на съответните дружества.

Вътрешният обмен на информация между различните нива и функционални звена в дружествата Лирекс.ком се извършва чрез:

- Вътрешния портал на дружествата, където се намират документите по ЗБУТ, включително процедури, инструкции, оценка на риска за работните места, доклади от вътрешни и външни одити на СУЗБУТ и др. Тази информация се преглежда и актуализира при необходимост от УПР или определен от него служител;
- Използване на корпоративната електронна поща;
- Обсъждане на дейностите по ЗБУТ на съвещания и оперативки по дружествата, както и на редовните прегледи от Ръководството на интегрираната СУКИС. Записи от тези обсъждания се водят съгласно процедурата LMP003 „Преглед на СУКИС от Ръководството".
- Клиентите и другите посетители на дружествата Лирекс.ком, които участват в обучения или други дейности на работни места в дружествата, се информират и инструктират в зависимост от целта на посещението им.

7.5.1. Служителите се включват чрез:

- Участие в избора на техни представители в КУТ/ГУТ на съответното дружество;
- Работа в КУТ/ГУТ като представители на работещите от съответното дружество;
- Информиране за опасностите на техните работните места на оценителите на риска и съдействие при определяне на мерките за отстраняване или намаляване на риска от тях;
- Съдействие като очевидци при разследване на евентуални инциденти.

При работа с подизпълнители, отговорниците за съответната дейност или проект от страна на Лирекс.ком, се консултират с тях при всички промени, които може да повлияят върху ЗБУТ при съвместната им работа.

Получаване или даване на консултация или информация в подходяща форма за ЗБУТ в дружествата Лирекс.ком на външни заинтересувани страни (държавни и контролни органи; сертифициращи, браншови или други неправителствени организации; клиенти, доставчици и др.) се прави от УПР или от други, определени от Висшето ръководство служители.

Когато офисите на дружествата Лирекс.ком се намират в жилищни или бизнес сгради; или в близост до места с постоянно присъствие на хора, ръководителите на офисите или упълномощени от тях служители установяват контакти с отговорни лица в тях за обмен на информация и предупреждение при възникване на потенциална опасност, включително и при извънредни ситуации, с цел опазване на безопасността и здравето на служителите и другите лица.

7.6. Изпълнение на дейностите по ЗБУТ

За изпълнение на процесите и операциите в дружествата Лирекс.ком без опасност или с минимален риск за здравето и безопасността на служителите, в процедурите и инструкциите за съответния процес или в самостоятелни инструкции за безопасна работа, хигиена на труда и пожарна безопасност са въведени изискванията по ЗБУТ. Те осигуряват безопасността и здравето както на работещите, така и на клиентите, посетителите и другите заинтересовани страни. Тези инструкции са изброени в Регистър на инструкциите за безопасност и здраве при работа. Инструктажите се извършват от определените за това лица и се документират в Книгите за инструктаж.

При въвеждане на нови или промени в съществуващите процеси и организация на работа, в зависимост от новата оценка на риска за тях, се създават нови или се актуализират изискванията за здраве и безопасност в съществуващите процедури или инструкции.

За осигуряване на здравословни и безопасни условия на труд в дружествата Лирекс.ком се осигуряват, контролират и поддържат следните инсталации и оборудване:

- електрозахранване;
- отопление и климатизация;
- алармена / пожароизвестителна система;
- пожарогасители в помещенията на офисите;
- лични предпазни средства – осигуряват се по списък на служителите, които извършват дейности, за които са необходими ЛПС;
- ръчни електрически инструменти, преносими лампи и трансформатори – използват се от служителите при конкретни дейности в офисите и на обекти на клиентите;
- подвижно товаро-разтоварно оборудване за складове – подвижна платформа за повдигане и спускане на товари в бл. 306, палетни колички, двуколесни и четириколесни товарни колички;
- моторни превозни средства (МПС) – леки и лекотоварни автомобили за превоз на хора и стоки до офисите, клиентите и обектите, на които работят служителите на дружествата. Актуален списък на МПС се поддържа от Ръководител „Логистика".
- съоръжения с повишена опасност (СПО) - по смисъла на Закона за техническите изисквания към продуктите (ЗТИП), Лирекс.ком експлоатира едно такова съоръжение – асансьор в бл. 306.

В съответствие с Наредбата за безопасната експлоатация и техническия надзор на асансьори като ползвател дружество Лирекс БГ има писмен договор за поддържането и ремонтирането на асансьора с вписана в регистъра по чл. 36, ал. 1 ЗТИП организация.

В дружествата Лирекс.ком не се закупуват и не се използват опасни химични продукти и материали, които да изискват специфични условия за безопасно съхранение и контрол на достъпа до тях. Излязлото от употреба електрическо и електронно оборудване, включително това, което съдържа опасни вещества (луминисцентни лампи и др.п.) и представлява потенциална опасност за здравето на работещите, се управлява в съответствие с процедурата LRP003 „Управление на околната среда".

Дейностите в дружествата Лирекс.ком, свързани с идентифицираните опасности и при които е необходимо да се прилагат определени мерки за управление на рисковете за здравето и безопасността при работа, са обобщени в инструкцията LRI004 „Осигуряване на здравословни и безопасни условия на труд на работните места". В зависимост от изпълняваните дейности на работните места се изпълняват съответните дейности и инструктажи по ЗБУТ, посочени в таблицата от инструкцията.

Безопасността и здравето на служителите по отношение на закупуваните стоки, технически средства и услуги се осигурява съгласно процедурата LPP101 „Закупуване на стоки и услуги". Изпълнението на изискванията по безопасност и здраве от доставчиците на стоки и услуги (вкл. подизпълнителите) се оценява ежегодно.

Изискванията по безопасност и здраве по отношение на външните лица и другите посетители в офисите на Лирекс.ком се изпълняват, като те постоянно се придружават от служители на дружествата, а при участие в обучения или други дейности в офисите на дружествата, те се инструктират и инструктажите се документират на бланка "InstructionOHSAS-Extern.doc".

7.7. Готовност за реагиране при извънредни ситуации

Резултатите от идентификацията на опасностите, оценката и контрола на риска на работните места и създадената организация по спазване на противопожарната безопасност и наличното противопожарно оборудване в офисите на дружествата Лирекс.ком показват малка вероятност за възникване на извънредни ситуации в офисите на дружествата Лирекс.ком, които могат да повлияят на здравословните и безопасни условия на труд и/или да причинят злополуки или заболявания на работещите.

Поради невъзможността да се изключи вероятността за извънредни ситуации или поради външни причини (земетресение, пожар, буря и др.), които могат да застрашат безопасността и здравето на работещите, са изготвени и утвърдени Планове за действие при пожар или авария (Plan-Av-deistv) на личния състав за всеки офис на дружествата и Планове за евакуация при пожар (Plan-evak), отнасящи се за служителите и за намиращите се в офисите външни лица. Плановете се намират на Вътрешния портал и всички служители са запознати с тях и са обучени как да реагират в случай на необходимост в съответствие с одобрените планове. Всяка година се прави тренировка за изпълнение на дейностите по Плановете. Резултатите от проведената тренировка и оценката на ефективността й се отразяват в протокол, който се съхранява в противопожарното досие на обекта.

Тези планове се преразглеждат след възникване на извънредни ситуации и анализа от Ръководството за нея, както и след проверки от оторизираните органи, ако е необходимо.

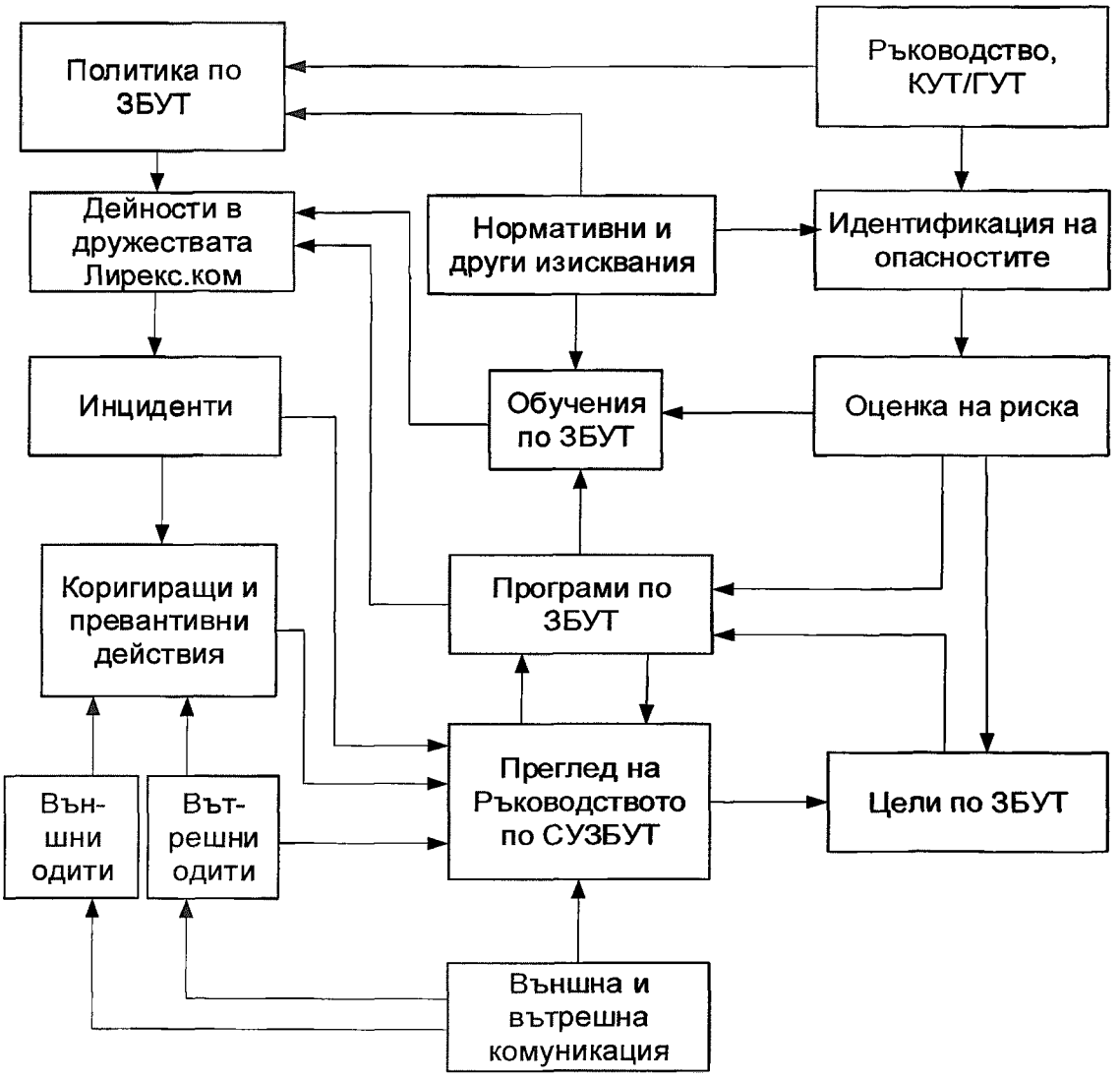
При поява на потенциална опасност, включително и при извънредни ситуации извън офисите на Лирекс.ком, Техническият организатор на АСД и ОБЗР следят и изпълняват указанията на държавните и местни компетентни органи, предавани чрез медиите и други средства за оповестяване с цел опазване на безопасността и здравето на служителите и другите лица.

Когато извънредната ситуация е съпроводена с инциденти и проблеми в информационната и комуникационна инфраструктура, се изпълняват и изискванията на инструкция LSI801 „Действие при инциденти в информационната сигурност".

Когато вследствие на извънредната ситуация е сериозно нарушена или прекъсната дейността в даден офис или дружество, се изпълняват и дейностите по инструкцията LSI901 „Действия при бедствия или аварии". За осигуряване на дейностите по Плановете за действие на личния състав при пожар или авария за всеки офис на дружествата се поддържа в изправност

оборудване за извънредни ситуации - алармени системи, резервно осветление и захранване; пожарогасителни средства; средства за оказване на първа помощ, комуникационни съоръжения и др.

8. Блок схеми



9. Термини и съкращения

Система за управление на качеството и	Организационната структура на ЛИРЕКС.КОМ в комплекс с регламентирания ред, процесите и ресурсите, необходими за

информационната сигурност (СУКИС)	управление на предлаганите продукти и услуги в съответствие с ISO 9001, ISO/IEC 27001, ISO/IEC 20000-1, ISO 14001 и ISO 45001.
Лирекс.ком	Дружествата Лирекс БГ, Лирекс БС, Лирекс Хай Тех, Лирекс Скопие, Беолик и Теза.
Здравословни и безопасни условия на труд	Условия и фактори, които влияят или могат да повлияят върху здравето и безопасността на персонала (включително временно наетия персонал и персонала на контрагентите), посетителите и всички други хора на дадено работно място.
Система за управление на здравословни и безопасни условия на труд (СУЗБУТ)	Част от СУКИС, която съдържа и изпълнява своя политика по здравословни и безопасни условия на труд и управлява рисковете за здравето и безопасността при работа.
Политика по здравословни и безопасни условия на труд	Общи намерения и насоки по отношение на изпълнение на дейностите, свързани със здравословните и безопасни условия на труд, заявени от висшето ръководство на Лирекс.ком.
Заинтересована страна	Лице или организация, която може да повлияе, да бъде повлияна от, или тя самата да се възприема като засегната от решение или дейност.
Работник	Лице, което изпълнява работа или дейности, свързани с работата, под управление на организацията.
Висше ръководство	Лице или група лица, които ръководят и контролират дадена организация на най – високо ниво.
Риск	Комбинация от вероятността за възникване на опасно събитие или за излагане на опасности и сериозността на нараняването или

	заболяването, които могат да бъдат причинени от това опасно събитие или от излагането на опасности.
Оценяване на риска	Процес на оценяване на риска, произтичащ от опасности, съобразявайки се с адекватността на съществуващите предпазни мерки и вземане на решение дали рискът е приемлив или не.
Риск за здравето и безопасността при работа	Комбинация от възможността за поява на свързано с работа опасно събитие или излагане на действието му и сериозността на нараняването и заболяването, които могат да бъдат причинени от събитието или излагането.
Работно място	Място под управление на организацията, където дадено лице трябва да се намира или да отиде, за да работи.
Строителни дейности	Дейности, свързани с проектиране и/или строително-монтажни работи при изграждане, ремонт и реконструкция на административни, обществени, промишлени и инфраструктурни обекти.
Възложител/ Клиент/Потребител	Юридическо или физическо лице, с което е сключен договор или друго споразумение за изпълнение на строителни дейности самостоятелно или като част от проект.
Изпълнител	Външна организация, предоставяща услуги на организацията, в съответствие с договорени спецификации, срокове и условия.
Подизпълнител	Юридическо или физическо лице, с което има действащ договор или друго споразумение за изпълнение на определена част от строителните дейности.
Опасност	Източник, ситуация или действие, които може да доведат до нараняване на хора или до заболяване, или комбинация от тях.

Идентифициране на опасност	Процес за определяне на съществуването на опасност и за определяне на нейните характеристики.
Заболяване	Разпознаваемо лошо физическо или умствено състояние, произтичащо от и/или влошавашо се при работа и/или при ситуации, свързани с работата.
Инцидент	Свързано с работата събитие, при което има нараняване или заболяване (независимо от тежестта) или смърт, или което може да доведе до такива последици. Инцидент, който е довел до нараняване, заболяване или смърт, е злополука. Инцидент, при който няма нараняване, заболяване или смърт, се нарича „почти инцидент".
Служба по трудова медицина (СТМ)	Звена с превантивни функции, което консултира и подпомага работодателя, комитетите и групите по условия на труд в планирането и организирането на дейностите по осигуряване и поддържане на ЗБУТ.
Орган по безопасност и здраве	Служител на Лирекс.ком, на когото е възложено изпълнението на дейностите по организация, координация и контрол на дейностите по осигуряване на ЗБУТ.
Комитет / Група по условията на труд	Колективни органи в дружествата Лирекс.ком, които обсъждат цялостната работа, оценката на риска и предлагат мерки по ЗБУТ.

10. Препратки към документи

ID на документа	*наименование на документа*
LRI004	Инструкция: Осигуряване на здравословни и безопасни условия на труд на работните места
LQS Manual	Наръчник на СУКИС
LMP003	Преглед на СУКИС от Ръководството
LMP002	Управление на документи и записи за реализация на фирмените дейности
LSI901	Действия при бедствия и аварии

За актуалната редакция и съдържание на процедурата проверете в *LODIS*.

LSI801	Действия при инциденти в информационната сигурност
LAP003	Коригиращи действия. Непрекъснато подобрение
LPP101	Закупуване на стоки и услуги

11. Оценки

11.1. Изпълнение

Наблюдението и измерването са постоянна дейност, при която се проверява степента на осъществяване на политиката по ЗБУТ, на целите по ЗБУТ и изпълнението на възложените функции, задачи и задължения от служителите в това отношение.

Контролът върху дейностите по СУЗБУТ се осъществява на основата на въведената в дружествата Лирекс.ком интегрирана СУКИС, зависи от изпълняваната дейност и е с периодика и насоченост, свързани с проявата и степента на съществуващите професионални рискове. Активното наблюдение (мониторинг) включва следните елементи на СУЗБУТ:

- Ежедневен контрол от ръководителите на дружествата, на отделните офиси и от ръководителите на проекти за безопасното изпълнение на работните операции от служителите на Лирекс.ком;
- Ежемесечно инспектиране от Техническия организатор на АСД и на ОБЗР по дружествата на системите за работа, работните помещения, работното оборудване, поведението на работниците и т.н.;
- Измерване на параметрите на работната среда (микроклимат, осветеност, ниво на шума) – извършва се от оторизирани лаборатории на интервали, определени от оценката на риска или при сигнали от работещите;
- Наблюдение на здравето на работещите чрез предварителните и периодичните медицински прегледи, провеждани от компетентни медицински органи или СТМ, с цел откриване в ранен стадий и проследяване на признаци и симптоми на увреждания, основно от трудовата дейност, за да се определи и приложи ефективна защита;
- Ежегоден анализ на дейността и състоянието на безопасните и здравословни условия на труд по дружества, който се изготвя от СТМ и се обсъжда в КУТ/ГУТ и на Прегледите от Ръководството на СУЗБУТ;
- Ежемесечна проверка на състоянието и срока на годност на пожарогасителите в помещенията на офисите от Техническия организатор на АСД и отговорниците по офисите;
- Техническото обслужване и презареждане на преносимите пожарогасители се извършва от лицензирана организация ежегодно или при необходимост;
- Периодично измерване на параметрите на електроинсталациите в офисите: импеданс на контура „фаза / защитен проводник" и "фаза / нулев проводник (PEN)" – извършва се от Службата по трудова медицина. Периодичността на измерванията се определя от Наредбата за техническа експлоатация на енергообзавеждането;

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

- Наблюдение на осветителните инсталации в офисите – извършва се от Техническия организатор на АСД и отговорниците по офисите, като при необходимост осветителните тела се подменят;
- Наблюдение на инсталациите за отопление и климатизация в офисите – извършва се от Техническия организатор на АСД и отговорниците по офисите, а при необходимост се поддържат или ремонтират от специализирани организации;
- Проверка на пожароизвестителни системи в офисите – извършва се от отговорника за пожарната безопасност на офиса или от оторизирана организация;
- Обслужването и специфичните ремонти на моторните превозни средства (МПС) се извършват във фирмените сервизи на съответната марка автомобил, а преминават задължителния годишен технически преглед (ГТП) в оторизиран сервиз. Два пъти годишно се прави проверка на състоянието на гумите, като всеки автомобил е оборудван с комплект зимни и комплект летни гуми. Смяната се извършва по списък всяка пролет и есен в специализиран сервиз. Контролът на дейността се осъществява от Мениджър Логистика;
- Ежемесечен контрол на безопасността на ръчните електрически инструменти, преносимите лампи и трансформатори - извършва се от определени в заповед на Управителя специалисти от отделните офиси. Резултатите от проверките се отразяват в специален Дневник.
- Подвижно товаро-разтоварно оборудване за складове – не се е необходимо специализирано обслужване, състоянието им се наблюдава от работещите с тях, а се контролира от Ръководител „Логистика";
- Проверка на състоянието на личните предпазни средства – извършва се от Техническия организатор на АСД, като негодните се заменят с нови;
- Провеждане на вътрешни одити на дейностите по ЗБУТ в рамките на СУКИС;
- Провеждане на външни одити от сертифициращите организации или проверки от компетентните държавни органи (инспекция по труда, органите по ПБ и др.п.);
- Периодични заседания на КУТ/ГУТ за обсъждане на дейностите по ЗБУТ по дружества;
- Периодичните прегледи от Ръководството на СУЗБУТ в рамките на интегрираната СУКИС – за обсъждане и преглед на изпълнението на целите и програмите за ЗБУТ и предотвратяване на професионалния риск; анализ и оценка на изпълнението на коригиращите / превантивни мерки и тяхната ефективност; оценка на ефективността на СУЗБУТ по степента на установените рискове и поддържането им в допустимите граници, установените нарушения на ЗБУТ от служителите, регистрираните инциденти и / или аварии, резултатите от проведените одити и забележките от тях, анализа за условията на труд и заболеваемостта на работещите от СТМ.

Мониторинг за изпълнението на дейностите по осигуряване на ЗБУТ, включително контрола на техническите, на пожароизвестителните и пожарогасителните средства, на работните помещения и работното оборудване в офисите на Лирекс.ком се извършва ежемесечно от Отговорника по СУЗБР в дружествата Лирекс.ком и се отразява на бланка Checklist OHSAS-YYYY-MM.doc.

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

Когато при наблюдението или измерването на дейностите по ЗБУТ се установи пропуск или отклонение от задължителните изисквания, въведени в процедурите, инструкциите или другите изисквания, за това се информират преките ръководители, ОБЗР, отговорниците на офиси или управителите на дружествата. Ако пропуските или отклоненията не могат да се отстранят незабавно, те се отразяват на бланка L-QS-012-OUNP „Протокол за несъответствие, установено при одит" и се предават на УПР за организиране на тяхното отстраняване.

Когато се използват технически средства за измерване, собственост на дружествата Лирекс.ком, тези средства се поддържат, контролират и калибрират в съответствие с процедурата LPP005 „Управление на средства за измерване и контрол".

11.2. Оценяване на съответствието

Оценяване на съответствието на дейностите по СУЗБУТ с приложимите изисквания на нормативните актове и с другите изисквания, които са въведени в дружествата Лирекс.ком (правилник за вътрешния трудов ред, инструкциите от СУКИС, свързани със ЗБУТ) се извършва под ръководството на УПР при въвеждане на нови технологии, продукти, услуги или при промени в приложимото законодателство.

Резултатите от оценяването на съответствието се отразяват на бланка „OHSAS Assessment" и се представят за обсъждане на Прегледа от Ръководството на СУЗБУТ.

11.3. Разследване на инциденти, несъответствия, коригиращи и превантивни действия

11.3.1. Разследване на инциденти

Инцидент е свързано с работата събитие, при което има нараняване, заболяване или смърт, или което може да доведе до такива последици. Инцидент, който е довел до нараняване, заболяване или смърт, е злополука; а инцидент, при който няма нараняване, заболяване или смърт, се нарича „почти инцидент". Всяка извънредна ситуация е частен случай на инцидент.

При настъпване на инцидент незабавно се предприемат мерки за оказване на първа долекарска медицинска помощ на засегнатите от инцидента и транспортиране на пострадалия до болнично заведение или повикване на бърза помощ. В същото време трябва да бъде обезопасено мястото на злополуката с ограничаване на достъпа от други лица.

След това се изпълняват изискванията на Наредбата за установяване, разследване, регистриране и отчитане на трудовите злополуки. В съответствие с нея за всяка трудова злополука пострадалият, непосредственият му ръководител или свидетелите на злополуката незабавно уведомяват Управителя или упълномощеното от него длъжностно лице.

След уведомлението за трудова злополука, Управителят или упълномощеното от него длъжностно лице са длъжни да организират разследване на обстоятелствата на злополуката. За резултатите от разследването се съставя Протокол, като към него се прилагат писмени показания на свидетелите на злополуката. Протоколът се завежда в Регистъра на актовете за трудови злополуки.

При настъпване на малък инцидент (напр. леко нараняване или др.п., при който не се налага издаване на болничен лист), след оказване, ако е необходимо, на първа долекарска медицинска помощ, този инцидент се регистрира в Регистъра на инциденти, които не са свързани с издаване на болничен лист. Предпазването от такива инциденти е включено в тематиката на началните и периодичните инструктажи по ЗБУТ.

След всяка трудова злополука/инцидент от ОБЗР с помощта СТМ се прави анализ, в който се определят пропуските и недостатъците в ЗБУТ и другите фактори, които могат да причинят това, идентифицира се необходимостта от коригиращи действия, както и възможните превантивни действия с цел да се осигури непрекъснатото подобряване на СУЗБУТ. Служителите се информират за резултатите от анализа.

11.3.2. Несъответствие, коригиращо и превантивно действие

Всички инциденти и „почти инциденти"; констатираните несъответствия или забележки при вътрешните и външните одити на СУЗБУТ; предписания и препоръки от проверки на контролните органи; оплаквания от клиенти или други заинтересовани страни; получените неприемливи стойности при нова оценка на риска; нова информация за опасности на работните места; забелязани пропуски при периодичните проверки на работните места от ОБЗР, както и новите изисквания в приложимото законодателство по ЗБУТ и др.п. се управляват по процедурата LAP003 „Коригиращи действия. Непрекъснато подобрение". Съгласно нея констатираните несъответствия се регистрират на бланките Заявка за коригиращо действие (L-QS-002-CAR) или Протокол за несъответствие, установено при одит (L-QS-012-OUNP).

Констатираните несъответствия се управляват и тяхната ефективност се оценява съгласно процедурата LAP003 „Коригиращи и превантивни действия".

УПР контролира изпълнението на регистрираните коригиращи действия и докладва за състоянието им на Прегледите от Ръководството на СУКИС. Когато се установи, че предприетите действия са неадекватни по отношение на опасностите или може да станат такива, те се преразглеждат и управляват по указания ред. Ако вследствие на тях се въвеждат нови системи, технологии или операции, оценката на риска на работните места от тях се актуализира.

11.4. Вътрешен одит

Вътрешните одити на Системата за управление на здравословните и безопасни условия на труд в рамките на СУКИС се провеждат, за да се установи доколко внедрената в дружествата Лирекс.ком система съответства на планираните дейности за управление на ЗБУТ, включително на изискванията на стандарта ISO 45001, как се поддържа и дали е ефикасна при постигане на политиката и целите.

Периодичните вътрешни одити се извършват в съответствие с процедура LAP002 „Организация на вътрешния контрол (одити)" и Годишния план за вътрешни одити (Audits plans.xls). При установени несъответствия се попълва бланка създават искания за коригиращи действия в съответствие с процедура LAP003 „Коригиращи и превантивни действия".

11.5. Преглед от Ръководството

Висшето ръководство извършва преглед на Системата за управление на здравословните и безопасни условия на труд в дружествата Лирекс.ком през планирани интервали, за да осигури нейната непрекъсната актуалност, адекватност и ефикасност. Прегледите включват оценяване на възможностите за подобряване и необходимостта от промени в СУЗБУТ, включително определената политика и цели.

Периодичните прегледи от Ръководството на СУЗБУТ се извършват в рамките на прегледите от Ръководството на СУКИС в съответствие с процедура LMP003 „Преглед на СУКИС от Ръководството" и Годишния план за прегледите (MngReview Plan).

УПР представя информация на прегледите от Ръководството на СУЗБУТ за:

- действията, последвали от предишни прегледи от ръководството;

- резултатите от вътрешните одити и от оценяване на съответствието с приложимите изисквания на нормативните актове и с другите изисквания, които дружествата са приели да спазват
- резултати от участието на служителите, както консултациите и информацията, съобщена от външни заинтересувани страни, включително жалби;
- изпълнението на дейностите, свързани със ЗБУТ и тяхната ефективност;
- степента на изпълнение на целите по здраве и безопасност при работа;
- състоянието на разследването на инциденти, на коригиращите и превантивните действия;
- промени в обстоятелствата, включително изменения в изискванията на нормативните актове и други изисквания, свързани със здравето и безопасността при работа;
- препоръки за подобряване.

На прегледите от Ръководството на СУЗБУТ се обсъждат и вземат решения и действия, с ангажимент за непрекъснато подобряване и свързани с възможни промени по:

- изпълнение на дейностите, свързани със здравето и безопасността при работа;
- политиката и целите по здраве и безопасност при работа;
- ресурсите;
- другите елементи на СУЗБУТ.

Приетите решения на Прегледа от Ръководството на СУЗБУТ са достъпни за обмен на информация и консултация на Вътрешния портал.

12. Документирана информация

- Всички документи и записи, свързани с въведената СУЗБУТ в рамките на интегрираната СУКИС в дружествата Лирекс.ком, отговарят на изискванията на стандарта ISO 45001 и на приложимото законодателство.
- Документите и записите по СУЗБУТ се оформят в съответствие с изискванията на инструкцията LMI001 „Съдържание и оформление на документи от СУКИС“ или според изискванията на приложимото законодателство.
- Когато съгласно изискванията на приложимото законодателство, актуалните документи (инструкции по ЗБР, методики, планове и др.) и записите (карти за оценка на риска, заповеди, протоколи и др.) трябва да са на хартиен носител и има специфични изисквания към тяхното оформление, те се поставят сканирани на Вътрешния портал.
- Актуалните и валидни версии на документите и записите от СУЗБУТ на Вътрешния портал са достъпни в режим „само за четене“ за всички служители на дружествата Лирекс.ком. Актуализацията на документите в електронен вид се прави от УПР или от Администратора на Вътрешния портал. Файловете на заменените документи и записи се поставят в папка „Архив“, до която достъп имат само УПР и Администратора на Вътрешния портал.
- Документите и записите по СУЗБУТ, които според приложимото законодателство са на хартиен носител, се съхраняват от ОБЗР и Техническия организатор на АСД.

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

- Сигурността на информацията, свързана с изпълняваните дейности по ЗБУТ в дружествата Лирекс.ком, се осигурява от процедурите и инструкциите на въведената Система за управление на качеството и информационната сигурност (СУКИС).
- Информацията, свързана с личните данни и здравословното състояние на работещите в дружествата Лирекс.ком се събира и използва само във връзка с пълното и точно изпълнение на дейностите по ЗБУТ от медицинските специалисти от СТМ и се съхранява, разпространява и предоставя на трети лица при строго спазване на изискванията на приложимото законодателство.
- Унищожаване на излезли от употреба носители на информация, свързана с дейностите по ЗБУТ, се извършва в съответствие с процедурата LSP472 „Унищожаване на информация".

12.1. Форми и бланки

ID на формата	*наименование на формата*
Karta_Ocenka_uslovia_trud.doc	Карта за оценка на условията на труд
Anketna_Karta_rab_mesta.doc	Анкетна карта за работните места
Karti_Ocenki_RM & Risk).	Карти за идентифициране на опасностите и оценка на риска за безопасност и здраве на работещите
InstructionOHSAS-extern.doc	Инструктаж на клиенти на работните места
OHSAS Assessment-YYYYMMDD	Оценяване на съответствието на СУЗБУТ с приложимите изисквания
L-QS-002-CAR	Заявка за коригиращо действие
L-QS-012-OUNP	Протокол L-QS-002-CAR за несъответствие, установено при одит

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

1. История на редакциите

версия	описание на промяната	автор	проверил	утвърдил	дата въвеждане
3	Отразяване на забележки от външен одит по OHSAS 18001:2007	Б.Йорданов	К.Иванов	Д.Илиева	15.11.2012
4	Въвеждане на строителни дейности в обхвата по BS OHSAS 18001:2007	Б.Йорданов	К.Иванов	Д.Илиева	25.07.2014
5	Актуализиране на СУКИС	М. Йончева	К. Иванов	Д. Илиева	01.06.2019

2. Предназначение

Процедурата има за цел да определи елементите на Системата за управление на здравословните и безопасни условия на труд (СУЗБУТ), техните взаимодействия и начините им на управление и контрол в рамките на СУКИС в дружествата Лирекс.ком. СУЗБУТ се въвежда, управлява и контролира в съответствие с изискванията на стандарта ISO 45001 и действащото законодателство в тази област.

3. Приложимост

Процедурата се прилага по отношение на здравословните и безопасни условия на труд за всички процеси и дейности, изпълнявани от служителите на Лирекс.ком, вкл. временно наетите; подизпълнителите или посетителите на работните места в дружествата или на техни външни обекти.

4. Отговорности

4.1. Висше ръководство:

- Осигуряват здравословните и безопасни условия на труд на служителите;
- Определят политиката по осигуряване на здравословните и безопасни условия на труд, включваща организацията на работа, елементите на работната среда и трудовия процес, както и социалните взаимоотношения;
- Организират оценката на професионалния риск за здравето и безопасността с помощта на външни организации (СТМ и др.), която обхваща работните процеси и оборудване, помещенията, работните места, организацията на труда, използването на материалите и други странични фактори;
- Утвърждават подходящите мерки за управление на риска в съответствие с направената оценка с цел осигуряване защитата на работещите и на другите лица;
- Осигуряват ефективен контрол за извършване на работата без риск за здравето и по безопасен начин;
- Отчитат специфичните опасности за служителите, които се нуждаят от специална закрила, включително и тези с ограничена работоспособност и осигурява съответните улеснения за тях.

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

- Предприемат необходимите мерки за координация на действията за осигуряване на здравето и безопасността при работа, когато на една работна площадка се извършват работи или дейности от и служители и на други работодатели.

4.2. Упълномощен представител на Ръководството (УПР) по Системата за управление на здравословните и безопасни условия на труд (СУЗБУТ):

- Организира разработването на политиките, процедурите и инструкциите от Системата за управление на здравословните и безопасни условия на труд (СУЗБУТ) в рамките на СУКИС;
- Разглежда и анализира предложенията за актуализация, изменение и допълнение на документите на СУЗБУТ;
- Осъществява постоянна оперативна координация, контрол и провежда дейности за осигуряване функционирането, поддържането и развитието на СУЗБУТ;
- Контролира обучението на персонала на дружествата по въпроси, свързани със СУЗБУТ;
- Организира провеждането на вътрешни одити на СУЗБУТ;
- Контролира и анализира прилагането, поддържането и подобрението на процесите от СУЗБУТ в рамките на СУКИС;
- Представлява пред и се занимава с комуникацията и връзките с външните за организацията заинтересовани страни като държавни и контролни органи; сертифициращи, браншови или други неправителствени организации; клиенти, доставчици, партньори и техните представители по въпросите на СУЗБУТ;
- Организира провеждането на Прегледите от ръководството на СУЗБУТ, на които се отчита състоянието й, изпълнението на целите и предлага мерки за нейното развитие и усъвършенстване;

4.3. Орган по безопасност и здраве при работа (ОБЗР) - служител по безопасност и здраве в дружествата Лирекс.ком:

- Организира и координира дейността по СУЗБУТ в конкретното дружество;
- Консултира работещите в съответното дружество по прилагането на изискванията на СУЗБУТ и подпомага управителите и другите длъжностни лица по прилагане на изискванията за осигуряване на безопасни и здравословни условия на труд при организиране и осъществяване на трудовата дейност;
- Провежда инструктажи на служителите по ЗБУТ;
- Контролира служителите по спазването на изискванията на въведената СУЗБУТ и на нормите и изискванията на законодателството по ЗБУТ;
- Предлага на Ръководството и прилага мерки за въздействие при нарушаване на изискванията и нормите по ЗБУТ.

4.4. Отговорник на Системата за управление на здравословните и безопасни условия на труд (Технически организатор на административно-стопански дейности (АСД)):

- Участва при изработването на документите по ЗБУТ за дружествата, за които отговаря;

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

- Организира снабдяването на служителите с лични предпазни средства и провежда обучение за тяхното използване и правилно съхранение;
- Организира обучението на работниците, за придобиване на квалификационна степен по електробезопасност и за работа на височина;
- Оказва съдействие на органите по трудова медицина при изпълнение на задълженията им;
- Участва при изработването и актуализиране на плановете за действие при стихийни бедствия и пожари и на плановете за евакуация при тях;
- Организира проверката на изправността на подвижните средства за гасене на пожари;
- Води регистър на актовете за трудови злополуки;
- Извършва текущи ремонти на оборудването в офисите.

4.5. Комитет / група по условия на труд (КУТ / ГУТ):

- Обсъжда цялостната дейност по опазване на здравето и осигуряване на безопасността на служителите в съответното дружество;
- Обсъжда на резултатите от оценката на професионалния риск и анализите на здравното състояние на служителите, докладите на службата по трудова медицина и други въпроси по осигуряване и опазване здравето и безопасността на работещите в Лирекс.ком;
- Обсъжда планираните промени в организацията на труда и работните места и предлага решения за опазване на здравето и осигуряване на безопасността на служителите;
- Извършва проверки по спазване на изискванията за здравословни и безопасни условия на труд в съответното дружество;
- Следи състоянието на трудовия травматизъм и професионалната заболеваемост на служителите от дружеството;
- Участва в разработването на програми за информиране и обучение на служителите по проблемите на здравословните и безопасни условия на труд.

4.6. Ръководител на функционално звено:

- Съдейства на органите по безопасност и здраве и СТМ при изпълнение на задълженията им по осигуряване на здравословни и безопасни условия на труд;
- Контролира спазването на изискванията за техника на безопасност от служителите във функционалното звено;
- Участва в Прегледите от Ръководството на СУКИС по дейностите по здраве и безопасност и развитието на Системата за здравословни и безопасни условия на труд.

4.7. Ръководител на офис:

- Организира и координира дейността по СУЗБУТ в конкретния офис;
- Оказва съдействие на органите по безопасност и здраве и СТМ при изпълнение на задълженията им;

- Участва при изработването и актуализиране на плановете за действие при стихийни бедствия и пожари и на плановете за евакуация при тях;
- Създава необходимата организация за правилното съхраняване и опазване на подвижните средства за гасене на пожар;
- Води регистър на актовете за трудови злополуки;
- Ръководителите на офиси извън София провеждат начален и периодичен инструктаж по ЗБУТ и организират извършването на ежедневен инструктаж на своите служители, когато това се налага.

4.8. Ръководител на проект:

- Определя специфичните мерки за здраве и безопасност при изпълнение на нов проект в зависимост от опасността на изпълняваните дейности от работещите в съответствие с инструкцията LRI004;
- Когато изпълняваните дейности изискват, той:
  - определя един или повече Отговорни инструктори, които да провеждат ежедневен инструктаж по ЗБУТ и пожарна безопасност, когато това се налага на работещите по проекта на външен обект;
  - подготвя заповед със задълженията и отговорностите на Отговорния инструктор;
  - предоставя на Отговорния инструктор Книгата за ежедневен инструктаж, в която предварително е записал обекта за работа и името на проекта;
  - след приключване на проекта, използва Книгата за ежедневен инструктаж и за други обекти, а след нейното изписване я предава на Техническия организатор на АСД за съхранение;
- Предприема необходимите мерки за координация на действията за осигуряване на здравословни и безопасни условия на труд, когато на един обект или работна площадка се извършват работи или дейности от служители и на други работодатели;
- Прилага по своя преценка допълнителни специфични мерки за осигуряване на ЗБУТ при изпълнение на дейности на външен обект.

4.9. Отговорен инструктор по ЗБУТ:

- След преминаване на допълнително обучение по здравословни и безопасни условия на труд му се издава удостоверение за завършен курс по ЗБУТ и му се делегират права за провеждане на ежедневен инструктаж;
- Провежда ежедневен инструктаж по безопасност, хигиена на труда и пожарна безопасност на работещите на същия ден на обект с зависимост от опасността на изпълняваните дейности в съответствие с инструкцията LRI004 „Осигуряване на здравословни и безопасни условия на труд а работните места";
- Води и съхранява Книгата за ежедневен инструктаж до приключване на проекта, след което я предава на Ръководителя на проекта.

4.10. Служба по трудова медицина (СТМ) – външна организация

- Консултира и подпомага управителите, комитетите и групите по условия на труд в планирането, организирането и изпълнението на задълженията му по осигуряване на здравословни и безопасни условия на труд и за укрепване здравето и работоспособността на работещите във връзка с извършваната от тях работа;
- Участва в идентифициране на опасностите на работните места и оценката на професионалните рискове в на работните места;
- Разработва и предлага мерки за отстраняване и намаляване на риска за здравето и безопасността при работа;
- Участва в разработването и включването на програми за здравословни и безопасни условия на труд в цялостната политика на управление на фирмата;
- Наблюдава здравословното състояние на работниците и анализирането му във връзка с извършваната работа;
- Участва в анализа на трудовите злополуки и професионалните болести;
- Обучава служителите и длъжностни лица по правилата за опазване на здравето при работа и оказване на първа помощ.

4.11. Всички служители на дружествата Лирекс.ком, вкл. временно наетите и клиентите на територията на дружествата:

- Спазват процедурите, инструкциите и указанията за безопасност и здраве при работа;
- Длъжни са да се грижат за здравето и безопасността си, както и за здравето и безопасността и на другите лица, пряко засегнати от неговата дейност, в съответствие с квалификацията си и дадените им инструкции;
- Спазват Правилника за вътрешния трудов ред;
- Притежават необходимите документи за правоспособност за извършване на дейностите, за които са наети;
- Използват правилно оборудването и инструментите;
- Информират незабавно съответните длъжностни лица за всяка възникнало обстоятелство, което може да представлява непосредствена опасност за здравето им и за всички неизправности в средствата за колективна защита.
- Съдействат на съответните длъжностни лица при изпълнението на мерките за осигуряване на здравословни и безопасни условия на труд.

5. Политика по здравословни и безопасни условия на труд

Настоящата политика по отношение на здравословните и безопасни условия на труд е част от общата политика на интегрираната Система за управление на качеството и информационната сигурност (СУКИС) в дружествата Лирекс.ком. Тази политика е насочена конкретно към непрекъснато подобряване на работната среда в изпълнение на действащите изисквания на българското законодателство и има за цел осигуряване на здравословни и безопасни условия на труд при всички дейности и процеси в дружествата; защита на интересите на работещите в тях и на клиентите, съблюдаване очакванията на обществото и изискванията на държавните институции в това отношение.

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

Политиката на Ръководството по отношение на здравословните и безопасни условия на труд в дружествата Лирекс.ком включва:

- Непрекъснато подобряване на работната среда в изпълнение на действащите изисквания на българското законодателство с цел постигане на високо качество на извършваните дейности; защита на здравето и работоспособността както на своите служители, така и на всички посетители, намиращи се на територията на дружествата и на очакванията на обществото.
- Ефективно управление на рисковете за здравето и сигурността, намаляване до минимум рисковете за персонала и другите заинтересовани страни, свързани с дейността на дружествата;
- Непрекъснато наблюдение и измерване на процесите и дейностите, имащи значимо въздействие върху работната среда;
- Постоянно идентифициране на опасностите и оценяване на риска за здравето и безопасността при работа, определяне на мерки и осигуряване на ресурси за неговото овладяване;
- Стриктно спазване на приложимите законови и други изисквания, свързани с идентифицираните опасности и оценените рискове за здравословните и безопасни условия на труд;
- Периодично преглеждане на изпълнението на общите и конкретни цели по ЗБУТ и актуализирането им при необходимост;
- Осигуряване на достатъчно информация, инструктажи и обучение на служителите и засилване на персоналната отговорност към спазването на безопасните и здравословни условия на труд;
- Активно сътрудничество с упълномощените организации за контрол на здравословните и безопасни условия на труд и всички заинтересовани страни при решаване на проблемите, свързани с осигуряването на ЗБУТ;
- Разследване и регистриране на всеки инцидент, злополука и/или професионално заболяване, с цел анализ и предприемане на мерки за превенция срещу повторната им поява.

Политиката по отношение на здравословните и безопасни условия на труд в дружествата Лирекс.ком се намира на Интернет сайта и на вътрешния портал. Тя се разглежда и обсъжда на периодичните Прегледи от ръководството на СУЗБУТ и се актуализира при необходимост.

6. Въвеждане на СУЗБУТ

6.1. Общи изисквания

Системата за управление на здравословните и безопасни условия на труд (СУЗБУТ) в Лирекс.ком се основава на резултатите от оценяването на риска. Това включва оценяване на условията на труд и опасностите на работните места по дружества, оценката на риска от тях и определяне на съответните мерки за неговото премахване или намаляване в съответствие с изискванията на нормативните актове и другите изисквания (вътрешно-фирмени документи като правилници, ръководства, инструкции и др.).

Тези дейности се включват в **Програмите за оценяване на риска** (*Progr_Ocen_Risk.doc*), съставени за всички офиси на дружествата и утвърдени от Управителя. Тези Програми се намират на Вътрешния портал на дружествата Лирекс.ком.

За актуалната редакция и съдържание на процедурата проверете в *LODIS*.
чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

Оценяването на риска е извършва по решение на Управителя под методическото ръководство на Службата по трудова медицина. В оценяването активно участват лицата, ангажирани в трудовия процес - ръководители, служители и техните представители в комитетите и групите по условия на труд, органите за безопасност и здраве в различните дружества.

6.2. Оценяване на професионалните рискове в дружествата Лирекс.ком

Оценяването се прави в съответствие със Закона за здравословни и безопасни условия на труд и Наредба №5 на МТСП и МЗ за реда, начина и периодичността на извършване на оценка на риска. Практически оценяването се реализира в два основни етапа:

- Идентифициране на опасностите (трудовите дейности или ситуациите, които е възможно да имат увреждащо действие) на работните места. Този етап включва събиране на информация от всички видове източници от и извън дружествата.
- Оценка на професионалния риск, която показва необходимо ли е прилагане на мерки за отстраняване или намаляване на установения риск.

6.2.1. Идентифициране на опасностите на работните места

От СТМ и съответно членовете на КУТ/ГУТ във всяко дружество е направен анализ на трудовите дейности, който включва определяне на работните места в тях и идентифициране на потенциалните опасности. Идентифицирането на опасностите включва:

- Анализ на често повтарящите се, както и на възможните извънредни дейности, които се изпълняват на работните места;
- Преглед на дейността на всички, които присъстват на работните места (служители, подизпълнители, клиенти или посетители;
- Поведението на хората, техните способности и други човешки фактори;
- Преглед на опасностите извън конкретното работно място, но които могат да повлияят неблагоприятно на ЗБУТ на служителите на това работно място;
- Опасностите от дейности, изпълнявани от други служители в близост до конкретно работно място;
- Инфраструктурата, съоръженията и материалите на работното място;
- Промени или предложени промени в дружествата, в СУЗБУТ или в изпълняваните дейности;
- Приложимите изисквания на нормативните актове по отношение на оценяването на риска от опасностите и предприемането на необходимите мерки;
- Състоянието на работните места и работните площадки, процесите, инсталациите, машините и съоръженията, процедури и инструкциите за работа и за нейната организация, включително тяхното приспособяване към човешките възможности.

Прилагат се следните подходи за идентифициране на опасностите:

- Наблюдение на трудовия процес - насочено е към конкретните действия и начините, по които те се извършват. Отчита се възможността за промяна в начина на работата от самия работещ и последствията от това по отношение на възникване на нови, непредвидени опасности. Наблюдението се осъществява от служители на СТМ и ОБЗР със сътрудничество от страна на работещите, като работната обстановка се обсъжда с тях.

- Използване на анкетни карти - въпросите в тях са насочени към технологичното оборудване, работата, работния процес и работната среда и имат за цел да установят потенциалните опасности за всяка дейност на работното място, а също така и произхода на опасността, готовността на работещите сами да въздействат на тази опасност и към предприетите мерки за колективна и индивидуална защита и тяхната ефективност. Използват се: Карта за оценка на условията на труд (Karta_Ocenka_uslovia_trud.doc) и Анкетна карта за работните места в офисите на дружествата (Anketna_Karta_rab_mesta.doc).
- Измерване параметрите на работната среда - за определяне на съответните опасности се използват данни от актуалните измервания на параметрите на работната среда: стойностите на елементите за микроклимат, шума, вибрациите и осветлението. За целите на оценката на риска измерванията се извършват от акредитирана лаборатория. Резултатите от измерванията дават обективната информация за рисковите фактори на работното място

При използването на посочените подходи от СТМ и с участието на ОБЗР, КУТ/ГУТ и служители от всички офиси на дружествата Лирекс.ком се идентифицират потенциално опасните фактори на работната среда. Те се отразяват в разработените за всяко работно място Карти за идентифициране на опасностите и оценка на риска за безопасност и здраве на работещите (*Karti_Ocenki_RM & Risk*).

6.2.2. Оценка на професионалните рискове

Оценката на риска е качествено или количествено градиране на риска по определена методика относно допустимостта на риска. Оценката на риска от потенциално опасните фактори на работната среда в офисите на дружествата Лирекс.ком се извършва по Методиката за оценка на професионалния риск (***Metodika-Ocenka_Risk.doc***), предложена от СТМ. Тя се намира на Вътрешния портал.

За всяка идентифицирана опасност се определят елементите на риска, които тя създава по посочената методика, а именно:

- Вероятността за нанасяне на конкретната вреда се определя от:
  - честотата, продължителността и спецификата на въздействие;
  - възможността да настъпи опасното събитие;
  - техническите средства за избягване или ограничаване на вредата;
  - човешките възможности за избягване или ограничаване на вредата – квалификация, опит, практически знания и умения, осмисляне на рисковете, взаимодействие между хората, психологични, социални и ергономични аспекти и др., които могат да окажат въздействие върху риска;
  - стойността на измерените стойности на факторите на работната среда от оторизирани лаборатории.
- Експозиция - отчита времето на въздействие на идентифицираната опасност върху работещите и спецификата на излагане на тази опасност;
- Последици от вредата (тежест) - оценява се в съответствие с:
  - вида на обектите, подлежащи на защита – хора, имущество, работна и околна среда;

- тежестта на възможните наранявания или увреждания на здравето – незначителни, сериозни, опасни, фатални;
- обхвата на вредата.

След оценката на риска от всяка опасност на работните места по Методиката се установява допустимостта на определения риск и необходимостта от прилагане на мерки за неговото предотвратяване или намаляване и ограничаване. Основните критерии за установяване допустимостта на риска са:

- съответствие с разпоредбите на нормативните актове за осигуряване на здравословни и безопасни условия на труд;
- приложението на принципите за превантивна дейност, посочени в Закона за здравословни и безопасни условия на труд;
- отчитането на информацията от източниците на информация, които нямат силата на нормативен акт, но прилагането им осигурява ЗБУТ.

Картите с идентифицираните опасности и оценка на риска за безопасност и здраве на работещите на всички работни места в офисите на дружествата Лирекс.ком и обобщената оценка на професионалния риск по дружества (*Ocenka_Risk.doc*) се намират на Вътрешния портал.

6.2.3. Управление на риска

Управлението на риска е процес на предотвратяване, отстраняване или ограничаване на риска за здравето и безопасността, включващ предприемането на организационни, контролни, комуникационни, технически и технологични мерки в дейностите на дружествата Лирекс.ком.

Определянето на конкретните мерки (дейности) е в зависимост от оценката на риска за съответната опасност или работно място. Мерките за управление на риска се планират и прилагат, като се цели последователно:

- премахване на опасността или риска;
- заместване на опасни дейности с по-малко опасни;
- прилагане на технически контрол или други организационни мерки;
- предупредителни и/или административни мерки;
- използване на средства за колективна защита;
- използване на средства за индивидуална защита.

Мерките за управление на риска се включват в Програмите за предотвратяване на професионалния риска в дружествата Лирекс.ком. Тези Програми се отнасят за периода, за който е актуална оценката на професионалния риск. Програмите се изготвят от СТМ съвместно с КУТ/ ГУТ на съответното дружество и се одобряват от Управителя.

При нова оценка на риска Програмите за предотвратяване на професионалния риска се актуализират в съответствие с новите стойности.

6.2.4. Преразглеждане на оценката на риска

Оценката на риска се преразглежда, когато:

- настъпят промени, които могат да окажат влияние върху риска като въвеждане на нови производствени процеси, оборудване, продукти и материали, промяна на организацията на труда, нови сгради и помещения, реконструкция на съществуващи и др.;

- след настъпили промени в приложимата нормативна уредба;
- оценката е направена на основата на данни и информация, станали невалидни или неподходящи;
- има условия оценката да бъде подобрена;
- прилаганите защитни и профилактични мерки са неефективни или неадекватни;
- резултатите от разследвания на злополуки, аварии, професионални заболявания и инциденти без злополуки налагат преразглеждане.

Преразглеждане на оценката на риска се извършва:

- по преценка на Висшето ръководство;
- по предписание на контролните органи.

Периодичността на оценяване на риска се определя от Висшето ръководство, в зависимост от установения риск и в съответствие с изискванията на нормативните актове.

При планиране на промени, свързани с организационна структура, нови изисквания на приложимата нормативна база, модифициране или въвеждане на нови работни процеси, дейности, материали или оборудване в дружествата Лирекс.ком, преди тяхната реализация, по решение на Висшето ръководство, се извършва повторно идентифициране на опасностите на работното място и оценка на риска. Това оценяване се консултира с работещите, КУТ/ ГУТ, ОБЗР и СТМ.

След приемането на решението за промяна, УПР и ОЗБУТ информират, обучават и консултират всички заинтересовани страни, имащи отношение към конкретното изменение.

6.3. Изисквания на нормативните актове и други изисквания по ЗБУТ

Оценяването на риска по същество е оценяване на съответствието на условията на труд с приложимото законодателство и с другите изисквания (стандарти, правилници и ръководства по безопасност при работа и др. п.) на производители, браншови организации и други заинтересовани страни.

С цел изпълнение на изискванията на законодателството по здраве и безопасност за дейностите, продуктите и услугите на дружествата Лирекс.ком е създаден Регистър на нормативни актове по ЗБУТ (RegisterLegOHSAS). Той се намира на Вътрешния портал на дружествата Лирекс.ком. Регистърът се поддържа актуален от УПР по СУЗБУТ или определен от него служител. Достъпът до актуалното съдържание на нормативните актове се осигурява от намиращите се в Интернет бази данни с такава информация.

В съответствие с приложимите за дейностите, продуктите и услугите на дружествата нормативни актове са изготвени и утвърдени вътрешно-фирмените документи, които включват изисквания по ЗБУТ (Правилник за вътрешния трудов ред, Инструкции за безопасност при различни дейности и др.). Всички те се намират на Вътрешния портал със свободен достъп от всички служители на Лирекс.ком.

6.4. Цели и програми по ЗБУТ

6.4.1. Цели по ЗБУТ

Целите се определят в съответствие с утвърдените основни цели на СУКИС, на политиката по ЗБУТ, включително и ангажимента за непрекъснато подобряване, направената оценка на риска, правните и други изисквания, работните процеси в дружествата, причините за трудовия травматизъм и професионалната заболеваемост, въведените корпоративни изисквания по ЗБУТ,

финансовите и бизнес възможности, както и с препоръките от външни контролни или консултиращи органи.

Целите по здравословни и безопасни условия на труд в рамките на СУЗБУТ се приемат, обсъждат и отчитат на Прегледите от Ръководството на интегрираната СУКИС в дружествата Лирекс.ком. Те се отразяват в документа Програма по ЗБУТ на дружествата Лирекс.ком (OHSAS_Progr-YYYY).

6.4.2. Програма по ЗБУТ

За постигане на целите по ЗБУТ, ежегодно се изготвя Програма по ЗБУТ на дружествата Лирекс.ком. В нея се отразяват дейностите за постигане на поставените цели, както и конкретните мерки за осигуряване на ЗБУТ от Програмите за предотвратяване на професионалния риск (Progr_Predot_Risk.doc) за всички офиси на дружествата.

Програмата се утвърждава от Висшето ръководство и се намира на Вътрешния портал на Лирекс.ком. В нея са посочени отговорните лица, сроковете и ресурсите за изпълнение на поставените цели.

Изпълнението на целите в Програмата по ЗБУТ се разглежда и обсъжда на заседания на КУТ/ ГУТ в дружествата и на периодичните прегледи от Ръководството на СУЗБУТ в рамките на интегрираната СУКИС.

Когато е необходимо, Програмата се актуализира в съответствие с промените в дейностите, продуктите, услугите или условията на работа в офисите на дружествата Лирекс.ком. Новата Програма за ЗБУТ се утвърждава от Висшето ръководство.

7. Организация на дейностите по ЗБУТ

7.1. Общи изисквания

Целта е дейностите по управление на ЗБУТ в рамките на СУКИС да осигуряват:

- въвеждане на изискванията за ЗБУТ според съответните нормативни актове и другите приложими изисквания (вътрешно-фирмени документи като правилници, инструкции, ръководства за работа и др.) и осигуряване на необходимите ресурси за това;
- организиране и изпълнение на работните и спомагателните процеси в дружествата Лирекс.ком в съответствие с въведените изисквания за ЗБУТ;
- ефективно и ефикасно постигане на поставените цели по ЗБУТ;
- подобряване на резултатите, характеризиращи ЗБУТ.

7.2. Ресурси

- Ръководството отговаря за осигуряването на необходимите ресурси за въвеждане и поддържане на ЗБУТ в дружествата Лирекс.ком в рамките на СУКИС, включително оборудването, служителите и тяхното обучение;
- Ръководството определя Упълномощен представител на Ръководството (УПР) по Системата за управление на здравословни и безопасни условия на труд (СУЗБУТ), който осигурява тази система да бъде разработена, внедрена и поддържана в съответствие с изискванията на стандарта ISO 45001 в рамките на интегрираната СУКИС. УПР докладва на Прегледите от Ръководството за изпълнение на СУЗБУТ в интегрираната СУКИС;

- Висшето ръководство определя служителите, които имат конкретни права и отговорности по ЗБУТ – Органи по безопасност и здраве при работа (ОБЗР) и Отговорници по пожарна и аварийна безопасност (ПАБ) по дружества и издава съответните заповеди за това.
- Висшето ръководство упражнява контрол върху дейностите по ЗБУТ и ПАБ и делегира права в това отношение на ръководителите на всички нива в дружествата Лирекс.ком.

7.3. Компетентност, обучение и осъзнаване

Ръководството осъзнава важността на квалификацията и компетентността на персонала в дружествата Лирекс.ком по отношение на ЗБУТ. Като предпоставка за безопасно изпълнение на служебните задължения, наемането на служители с необходимата професионална подготовка и квалификация се извършва в съответствие с процедурата LRP002 „Набиране и подбор на персонал".

Компетентността, обучението и осъзнаването на служителите по отношение на здравето и безопасността при работа се осигурява от:

- Редовно провежданите инструктажи по ЗБУТ;
- Специализирано обучение на служителите, които извършват дейности, за които се изисква определена правоспособност (напр. квалификационна група по електробезопасност, работа на височина, шофьори и др.);
- Периодично обучение на ОБЗР и на служителите, които участват в КУТ/ ГУТ.

7.3.1. Инструктажи по ЗБУТ

Всички служители на дружествата Лирекс.ком, вкл. временно наетите и клиентите на територията на дружествата се информират за опасностите на работното място и се инструктират по безопасност и здраве при работа. Инструктажите се провеждат в съответствие с Наредбата за условията и реда за провеждането на периодично обучение и инструктаж на работниците и служителите по правилата за осигуряване на здравословни и безопасни условия на труд:

- при постъпване на работа на служители на Лирекс.ком и на клиенти при обучение на работни места в дружествата;
- при преместване на друга работа или промяна на работата на служители;
- при въвеждане на ново или при промяна на работно оборудване и технология;
- периодично за поддържане и допълване на знанията на работещите в дружествата по безопасност и здраве при работа;

Инструктажите по безопасност и здраве при работа се подразделят на:

- Начален - целта е новопостъпилите служители да се запознаят с основните правила и изисквания по ЗБУТ и ПАБ в дружеството, както и с изискванията към тяхното поведение с оглед опазване на здравето и живота им;
- На работното място (вкл. и на клиенти за обучение) – целта е практическо запознаване на служителя с конкретните изисквания за безопасната работа и се провежда на работното място, преди да му бъде възложена самостоятелна работа. Когато е възможно, началния инструктаж и инструктажа на работното място се извършват едновременно;

- Периодичен - целта е да се поддържат и допълват знанията на служителите по ЗБУТ и ПАБ;
- Ежедневен - целта е служителите, които извършват дейности с по-висок риск, да се инструктират всеки ден с цел опазване на здравето и живота им;
- Извънреден – целта е да не се допуска повтарянето на злополуки или аварии по вина на работещите. Инструктажите се провеждат от ОБЗР в съответното дружество по ред, условия и продължителност, определени със заповеди на Управителите на дружествата *(Zap.insruktaji.pdf, Zap.vid.instruktaji.pdf)*.

В зависимост от изпълняваните работи, инструктажите се провеждат по програмите за съответния инструктаж, одобрени от Управителя. Те са поставени на Вътрешния портал.

Проведените инструктажи се документират в Книги за инструктажите, които се съхраняват от ОБЗР на дружествата. Органът по безопасност и здраве, провел началния инструктаж на лицата, които постъпват на работа, издава служебна бележка, която се съхранява в личното досие на работещия. Бележката се подписва от извършващия инструктажа и от инструктирания служител.

При изпълняване на дейности на обект на клиент, в зависимост от характера на работа, по преценка на Ръководителя на проекта и след издаване на заповед, специално обучен Отговорен инструктор провежда ежедневен инструктаж по безопасност и здраве на работещите в съответствие с LRI004 „Осигуряване на здравословни и безопасни условия на труд на работните места".

На всички водачи на служебни автомобили в дружеството се провежда ежедневен инструктаж от упълномощено лице. Такъв вид инструктаж се провежда и на служителите, на които временно е предоставено правото да управляват служебен автомобил.

Извънреден инструктаж се провежда по нареждане на Висшето ръководство след всяка трудова злополука, пожар, промишлена авария, природно бедствие или при констатирани груби нарушения на ЗБУТ; при промяна на технологии, машини, организацията на работа или по предписание на контролен орган. Той се регистрира в Дневника за трудови злополуки и професионални заболявания, който се съхранява от ОБЗР.

Инструктажи на клиентите, които присъстват за обучение на работни места в офисите на дружествата се документират на бланка "InstructionOHSAS-Extern.doc".

7.4. Специализирано и периодично обучение по ЗБУТ

Служителите, които извършват настройка и ремонт на компютърна техника и монтаж на системи за сигурност, се допускат до самостоятелна работа само след успешно положен изпит за придобиване на трета квалификационна група за електробезопасност от лицензирана организация. ОБЗР на дружеството води отчет на работниците които трябва да притежават такива документи за правоспособност. Същото се отнася и за работниците които извършват работа на височина.

Всички служители, които управляват служебните МПС на дружествата Лирекс.ком, трябва да притежават необходимите свидетелства за управление, предвидени в **Закона за движението по пътищата**, с което се удостоверява правоспособността им за управление на МПС от съответната категория. Свидетелствата се подновяват от водачите на определените за това периоди.

Служителите, които са избрани в КУТ/ ГУТ и ОБЗР в дружествата Лирекс.ком периодично се обучават от служители на СТМ.

7.4.1. Оценяване на ефективността на обучението по ЗБУТ

Ефективността от провежданите инструктажи и обучения по ЗБУТ се оценява при периодичните проверки по работните места от ОБЗР, по констатираните нарушения на процедурите и инструкциите от СУЗБУТ при вътрешните и външните одити, по трудовия травматизъм и заболеваемост. Тези показатели се контролират при мониторинга по ЗБУТ и се отчитат на периодичните Прегледи по СУКИС.

7.5. Обмен на информация, участие и консултиране по отношение на ЗБУТ

Служителите се информират за своите ангажименти по ЗБУТ при провежданите инструктажи по ЗБУТ, от преките си ръководители или от мениджърите на съответните дружества.

Вътрешният обмен на информация между различните нива и функционални звена в дружествата Лирекс.ком се извършва чрез:

- Вътрешния портал на дружествата, където се намират документите по ЗБУТ, включително процедури, инструкции, оценка на риска за работните места, доклади от вътрешни и външни одити на СУЗБУТ и др. Тази информация се преглежда и актуализира при необходимост от УПР или определен от него служител;
- Използване на корпоративната електронна поща;
- Обсъждане на дейностите по ЗБУТ на съвещания и оперативки по дружествата, както и на редовните прегледи от Ръководството на интегрираната СУКИС. Записи от тези обсъждания се водят съгласно процедурата LMP003 „Преглед на СУКИС от Ръководството".
- Клиентите и другите посетители на дружествата Лирекс.ком, които участват в обучения или други дейности на работни места в дружествата, се информират и инструктират в зависимост от целта на посещението им.

7.5.1. Служителите се включват чрез:

- Участие в избора на техни представители в КУТ/ГУТ на съответното дружество;
- Работа в КУТ/ГУТ като представители на работещите от съответното дружество;
- Информиране за опасностите на техните работните места на оценителите на риска и съдействие при определяне на мерките за отстраняване или намаляване на риска от тях;
- Съдействие като очевидци при разследване на евентуални инциденти.

При работа с подизпълнители, отговорниците за съответната дейност или проект от страна на Лирекс.ком, се консултират с тях при всички промени, които може да повлияят върху ЗБУТ при съвместната им работа.

Получаване или даване на консултация или информация в подходяща форма за ЗБУТ в дружествата Лирекс.ком на външни заинтересувани страни (държавни и контролни органи; сертифициращи, браншови или други неправителствени организации; клиенти, доставчици и др.) се прави от УПР или от други, определени от Висшето ръководство служители.

Когато офисите на дружествата Лирекс.ком се намират в жилищни или бизнес сгради; или в близост до места с постоянно присъствие на хора, ръководителите на офисите или упълномощени от тях служители установяват контакти с отговорни лица в тях за обмен на информация и предупреждение при възникване на потенциална опасност, включително и при извънредни ситуации, с цел опазване на безопасността и здравето на служителите и другите лица.

7.6. Изпълнение на дейностите по ЗБУТ

За изпълнение на процесите и операциите в дружествата Лирекс.ком без опасност или с минимален риск за здравето и безопасността на служителите, в процедурите и инструкциите за съответния процес или в самостоятелни инструкции за безопасна работа, хигиена на труда и пожарна безопасност са въведени изискванията по ЗБУТ. Те осигуряват безопасността и здравето както на работещите, така и на клиентите, посетителите и другите заинтересовани страни. Тези инструкции са изброени в Регистър на инструкциите за безопасност и здраве при работа. Инструктажите се извършват от определените за това лица и се документират в Книгите за инструктаж.

При въвеждане на нови или промени в съществуващите процеси и организация на работа, в зависимост от новата оценка на риска за тях, се създават нови или се актуализират изискванията за здраве и безопасност в съществуващите процедури или инструкции.

За осигуряване на здравословни и безопасни условия на труд в дружествата Лирекс.ком се осигуряват, контролират и поддържат следните инсталации и оборудване:

- електрозахранване;
- отопление и климатизация;
- алармена / пожароизвестителна система;
- пожарогасители в помещенията на офисите;
- лични предпазни средства – осигуряват се по списък на служителите, които извършват дейности, за които са необходими ЛПС;
- ръчни електрически инструменти, преносими лампи и трансформатори – използват се от служителите при конкретни дейности в офисите и на обекти на клиентите;
- подвижно товаро-разтоварно оборудване за складове – подвижна платформа за повдигане и спускане на товари в бл. 306, палетни колички, двуколесни и четириколесни товарни колички;
- моторни превозни средства (МПС) – леки и лекотоварни автомобили за превоз на хора и стоки до офисите, клиентите и обектите, на които работят служителите на дружествата. Актуален списък на МПС се поддържа от Ръководител „Логистика".
- съоръжения с повишена опасност (СПО) - по смисъла на Закона за техническите изисквания към продуктите (ЗТИП), Лирекс.ком експлоатира едно такова съоръжение – асансьор в бл. 306.

В съответствие с Наредбата за безопасната експлоатация и техническия надзор на асансьори като ползвател дружество Лирекс БГ има писмен договор за поддържането и ремонтирането на асансьора с вписана в регистъра по чл. 36, ал. 1 ЗТИП организация.

В дружествата Лирекс.ком не се закупуват и не се използват опасни химични продукти и материали, които да изискват специфични условия за безопасно съхранение и контрол на достъпа до тях. Излязлото от употреба електрическо и електронно оборудване, включително това, което съдържа опасни вещества (луминисцентни лампи и др.п.) и представлява потенциална опасност за здравето на работещите, се управлява в съответствие с процедурата LRP003 „Управление на околната среда".

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

Дейностите в дружествата Лирекс.ком, свързани с идентифицираните опасности и при които е необходимо да се прилагат определени мерки за управление на рисковете за здравето и безопасността при работа, са обобщени в инструкцията LRI004 „Осигуряване на здравословни и безопасни условия на труд на работните места". В зависимост от изпълняваните дейности на работните места се изпълняват съответните дейности и инструктажи по ЗБУТ, посочени в таблицата от инструкцията.

Безопасността и здравето на служителите по отношение на закупуваните стоки, технически средства и услуги се осигурява съгласно процедурата LPP101 „Закупуване на стоки и услуги". Изпълнението на изискванията по безопасност и здраве от доставчиците на стоки и услуги (вкл. подизпълнителите) се оценява ежегодно.

Изискванията по безопасност и здраве по отношение на външните лица и другите посетители в офисите на Лирекс.ком се изпълняват, като те постоянно се придружават от служители на дружествата, а при участие в обучения или други дейности в офисите на дружествата, те се инструктират и инструктажите се документират на бланка "InstructionOHSAS-Extern.doc".

7.7. Готовност за реагиране при извънредни ситуации

Резултатите от идентификацията на опасностите, оценката и контрола на риска на работните места и създадената организация по спазване на противопожарната безопасност и наличното противопожарно оборудване в офисите на дружествата Лирекс.ком показват малка вероятност за възникване на извънредни ситуации в офисите на дружествата Лирекс.ком, които могат да повлияят на здравословните и безопасни условия на труд и/или да причинят злополуки или заболявания на работещите.

Поради невъзможността да се изключи вероятността за извънредни ситуации или поради външни причини (земетресение, пожар, буря и др.), които могат да застрашат безопасността и здравето на работещите, са изготвени и утвърдени Планове за действие при пожар или авария (Plan-Av-deistv) на личния състав за всеки офис на дружествата и Планове за евакуация при пожар (Plan-evak), отнасящи се за служителите и за намиращите се в офисите външни лица. Плановете се намират на Вътрешния портал и всички служители са запознати с тях и са обучени как да реагират в случай на необходимост в съответствие с одобрените планове. Всяка година се прави тренировка за изпълнение на дейностите по Плановете. Резултатите от проведената тренировка и оценката на ефективността ѝ се отразяват в протокол, който се съхранява в противопожарното досие на обекта.

Тези планове се преразглеждат след възникване на извънредни ситуации и анализа от Ръководството за нея, както и след проверки от оторизираните органи, ако е необходимо.

При поява на потенциална опасност, включително и при извънредни ситуации извън офисите на Лирекс.ком, Техническият организатор на АСД и ОБЗР следят и изпълняват указанията на държавните и местни компетентни органи, предавани чрез медиите и други средства за оповестяване с цел опазване на безопасността и здравето на служителите и другите лица.

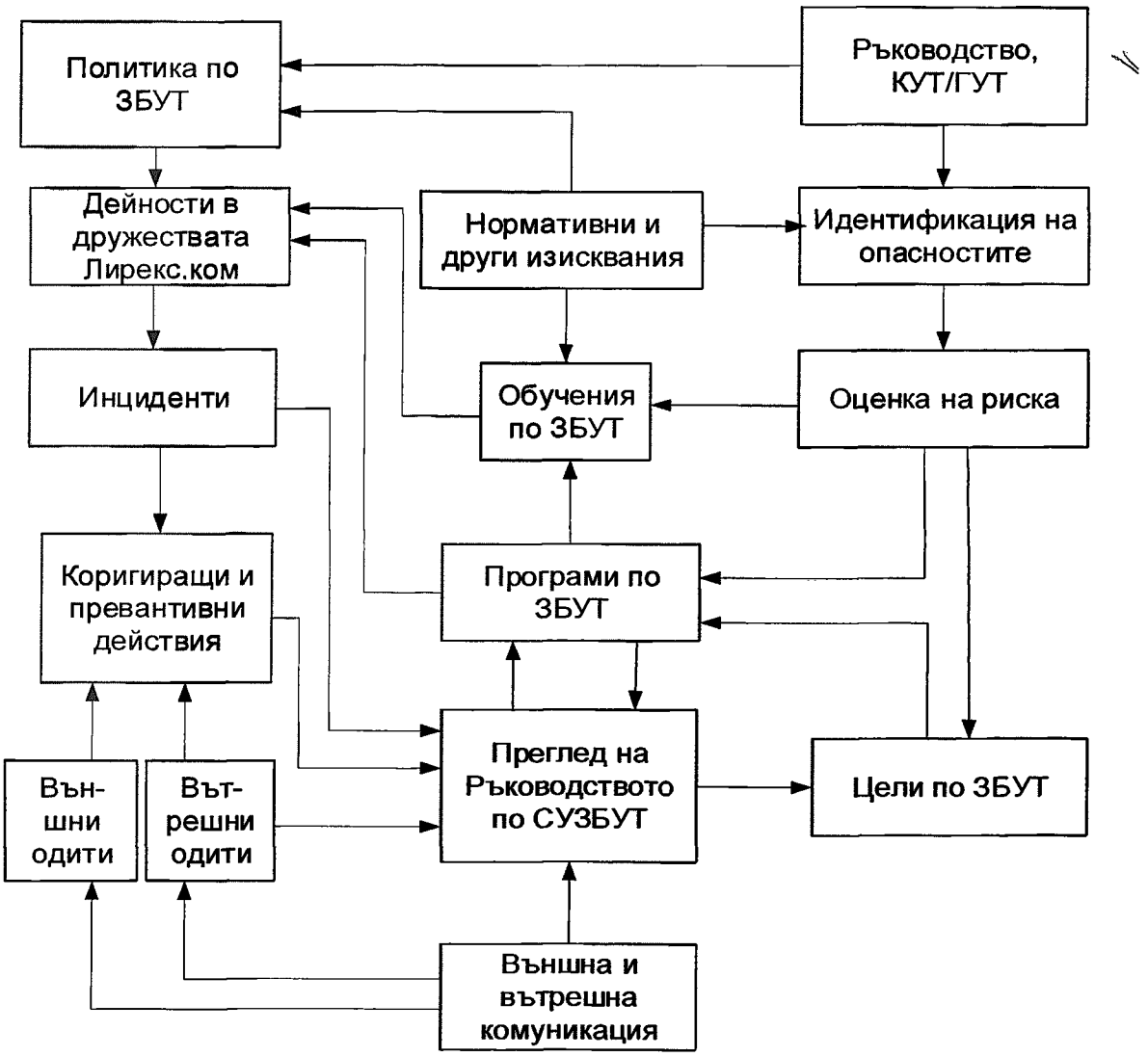
Когато извънредната ситуация е съпроводена с инциденти и проблеми в информационната и комуникационна инфраструктура, се изпълняват и изискванията на инструкция LSI801 „Действие при инциденти в информационната сигурност".

Когато вследствие на извънредната ситуация е сериозно нарушена или прекъсната дейността в даден офис или дружество, се изпълняват и дейностите по инструкцията LSI901 „Действия при бедствия или аварии". За осигуряване на дейностите по Плановете за действие на личния състав при пожар или авария за всеки офис на дружествата се поддържа в изправност

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

оборудване за извънредни ситуации - алармени системи, резервно осветление и захранване; пожарогасителни средства; средства за оказване на първа помощ, комуникационни съоръжения и др.

8. Блок схеми



9. Термини и съкращения

Система за управление на качеството и	Организационната структура на ЛИРЕКС.КОМ в комплекс с регламентирания ред, процесите и ресурсите, необходими за

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

информационната сигурност (СУКИС)	управление на предлаганите продукти и услуги в съответствие с ISO 9001, ISO/IEC 27001, ISO/IEC 20000-1, ISO 14001 и ISO 45001.
Лирекс.ком	Дружествата Лирекс БГ, Лирекс БС, Лирекс Хай Тех, Лирекс Скопие, Беолик и Теза.
Здравословни и безопасни условия на труд	Условия и фактори, които влияят или могат да повлияят върху здравето и безопасността на персонала (включително временно наетия персонал и персонала на контрагентите), посетителите и всички други хора на дадено работно място.
Система за управление на здравословни и безопасни условия на труд (СУЗБУТ)	Част от СУКИС, която съдържа и изпълнява своя политика по здравословни и безопасни условия на труд и управлява рисковете за здравето и безопасността при работа.
Политика по здравословни и безопасни условия на труд	Общи намерения и насоки по отношение на изпълнение на дейностите, свързани със здравословните и безопасни условия на труд, заявени от висшето ръководство на Лирекс.ком.
Заинтересована страна	Лице или организация, която може да повлияе, да бъде повлияна от, или тя самата да се възприема като засегната от решение или дейност.
Работник	Лице, което изпълнява работа или дейности, свързани с работата, под управление на организацията.
Висше ръководство	Лице или група лица, които ръководят и контролират дадена организация на най – високо ниво.
Риск	Комбинация от вероятността за възникване на опасно събитие или за излагане на опасности и сериозността на нараняването или

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

	заболяването, които могат да бъдат причинени от това опасно събитие или от излагането на опасности.
Оценяване на риска	Процес на оценяване на риска, произтичащ от опасности, съобразявайки се с адекватността на съществуващите предпазни мерки и вземане на решение дали рискът е приемлив или не.
Риск за здравето и безопасността при работа	Комбинация от възможността за поява на свързано с работа опасно събитие или излагане на действието му и сериозността на нараняването и заболяването, които могат да бъдат причинени от събитието или излагането.
Работно място	Място под управление на организацията, където дадено лице трябва да се намира или да отиде, за да работи.
Строителни дейности	Дейности, свързани с проектиране и/или строително-монтажни работи при изграждане, ремонт и реконструкция на административни, обществени, промишлени и инфраструктурни обекти.
Възложител/ Клиент/Потребител	Юридическо или физическо лице, с което е сключен договор или друго споразумение за изпълнение на строителни дейности самостоятелно или като част от проект.
Изпълнител	Външна организация, предоставяща услуги на организацията, в съответствие с договорени спецификации, срокове и условия.
Подизпълнител	Юридическо или физическо лице, с което има действащ договор или друго споразумение за изпълнение на определена част от строителните дейности.
Опасност	Източник, ситуация или действие, които може да доведат до нараняване на хора или до заболяване, или комбинация от тях.

Идентифициране на опасност	Процес за определяне на съществуването на опасност и за определяне на нейните характеристики.
Заболяване	Разпознаваемо лошо физическо или умствено състояние, произтичащо от и/или влошаващо се при работа и/или при ситуации, свързани с работата.
Инцидент	Свързано с работата събитие, при което има нараняване или заболяване (независимо от тежестта) или смърт, или което може да доведе до такива последици. Инцидент, който е довел до нараняване, заболяване или смърт, е злополука. Инцидент, при който няма нараняване, заболяване или смърт, се нарича „почти инцидент".
Служба по трудова медицина (СТМ)	Звена с превантивни функции, което консултира и подпомага работодателя, комитетите и групите по условия на труд в планирането и организирането на дейностите по осигуряване и поддържане на ЗБУТ.
Орган по безопасност и здраве	Служител на Лирекс.ком, на когото е възложено изпълнението на дейностите по организация, координация и контрол на дейностите по осигуряване на ЗБУТ.
Комитет / Група по условията на труд	Колективни органи в дружествата Лирекс.ком, които обсъждат цялостната работа, оценката на риска и предлагат мерки по ЗБУТ.

10. Препратки към документи

ID на документа	*наименование на документа*
LRI004	Инструкция: Осигуряване на здравословни и безопасни условия на труд на работните места
LQS Manual	Наръчник на СУКИС
LMP003	Преглед на СУКИС от Ръководството
LMP002	Управление на документи и записи за реализация на фирмените дейности
LSI901	Действия при бедствия и аварии

За актуалната редакция и съдържание на процедурата проверете в *LODIS*.

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

LSI801	Действия при инциденти в информационната сигурност
LAP003	Коригиращи действия. Непрекъснато подобрение
LPP101	Закупуване на стоки и услуги

11. Оценки

11.1. Изпълнение

Наблюдението и измерването са постоянна дейност, при която се проверява степента на осъществяване на политиката по ЗБУТ, на целите по ЗБУТ и изпълнението на възложените функции, задачи и задължения от служителите в това отношение.

Контролът върху дейностите по СУЗБУТ се осъществява на основата на въведената в дружествата Лирекс.ком интегрирана СУКИС, зависи от изпълняваната дейност и е с периодика и насоченост, свързани с проявата и степента на съществуващите професионални рискове. Активното наблюдение (мониторинг) включва следните елементи на СУЗБУТ:

- Ежедневен контрол от ръководителите на дружествата, на отделните офиси и от ръководителите на проекти за безопасното изпълнение на работните операции от служителите на Лирекс.ком;
- Ежемесечно инспектиране от Техническия организатор на АСД и на ОБЗР по дружествата на системите за работа, работните помещения, работното оборудване, поведението на работниците и т.н.;
- Измерване на параметрите на работната среда (микроклимат, осветеност, ниво на шума) – извършва се от оторизирани лаборатории на интервали, определени от оценката на риска или при сигнали от работещите;
- Наблюдение на здравето на работещите чрез предварителните и периодичните медицински прегледи, провеждани от компетентни медицински органи или СТМ, с цел откриване в ранен стадий и проследяване на признаци и симптоми на увреждания, основно от трудовата дейност, за да се определи и приложи ефективна защита;
- Ежегоден анализ на дейността и състоянието на безопасните и здравословни условия на труд по дружества, който се изготвя от СТМ и се обсъжда в КУТ/ГУТ и на Прегледите от Ръководството на СУЗБУТ;
- Ежемесечна проверка на състоянието и срока на годност на пожарогасителите в помещенията на офисите от Техническия организатор на АСД и отговорниците по офисите;
- Техническото обслужване и презареждане на преносимите пожарогасители се извършва от лицензирана организация ежегодно или при необходимост;
- Периодично измерване на параметрите на електроинсталациите в офисите: импеданс на контура „фаза / защитен проводник" и "фаза / нулев проводник (PEN)" – извършва се от Службата по трудова медицина. Периодичността на измерванията се определя от Наредбата за техническа експлоатация на енергообзавеждането;

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

- Наблюдение на осветителните инсталации в офисите – извършва се от Техническия организатор на АСД и отговорниците по офисите, като при необходимост осветителните тела се подменят;
- Наблюдение на инсталациите за отопление и климатизация в офисите – извършва се от Техническия организатор на АСД и отговорниците по офисите, а при необходимост се поддържат или ремонтират от специализирани организации;
- Проверка на пожароизвестителни системи в офисите – извършва се от отговорника за пожарната безопасност на офиса или от оторизирана организация;
- Обслужването и специфичните ремонти на моторните превозни средства (МПС) се извършват във фирмените сервизи на съответната марка автомобил, а преминават задължителния годишен технически преглед (ГТП) в оторизиран сервиз. Два пъти годишно се прави проверка на състоянието на гумите, като всеки автомобил е оборудван с комплект зимни и комплект летни гуми. Смяната се извършва по списък всяка пролет и есен в специализиран сервиз. Контролът на дейността се осъществява от Мениджър Логистика;
- Ежемесечен контрол на безопасността на ръчните електрически инструменти, преносимите лампи и трансформатори - извършва се от определени в заповед на Управителя специалисти от отделните офиси. Резултатите от проверките се отразяват в специален Дневник.
- Подвижно товаро-разтоварно оборудване за складове – не се е необходимо специализирано обслужване, състоянието им се наблюдава от работещите с тях, а се контролира от Ръководител „Логистика";
- Проверка на състоянието на личните предпазни средства – извършва се от Техническия организатор на АСД, като негодните се заменят с нови;
- Провеждане на вътрешни одити на дейностите по ЗБУТ в рамките на СУКИС;
- Провеждане на външни одити от сертифициращите организации или проверки от компетентните държавни органи (инспекция по труда, органите по ПБ и др.п.);
- Периодични заседания на КУТ/ГУТ за обсъждане на дейностите по ЗБУТ по дружества;
- Периодичните прегледи от Ръководството на СУЗБУТ в рамките на интегрираната СУКИС – за обсъждане и преглед на изпълнението на целите и програмите за ЗБУТ и предотвратяване на професионалния риск; анализ и оценка на изпълнението на коригиращите / превантивни мерки и тяхната ефективност; оценка на ефективността на СУЗБУТ по степента на установените рискове и поддържането им в допустимите граници, установените нарушения на ЗБУТ от служителите, регистрираните инциденти и / или аварии, резултатите от проведените одити и забележките от тях, анализа за условията на труд и заболеваемостта на работещите от СТМ.

Мониторинг за изпълнението на дейностите по осигуряване на ЗБУТ, включително контрола на техническите, на пожароизвестителните и пожарогасителните средства, на работните помещения и работното оборудване в офисите на Лирекс.ком се извършва ежемесечно от Отговорника по СУЗБР в дружествата Лирекс.ком и се отразява на бланка Checklist OHSAS-YYYY-MM.doc.

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

Когато при наблюдението или измерването на дейностите по ЗБУТ се установи пропуск или отклонение от задължителните изисквания, въведени в процедурите, инструкциите или другите изисквания, за това се информират преките ръководители, ОБЗР, отговорниците на офиси или управителите на дружествата. Ако пропуските или отклоненията не могат да се отстранят незабавно, те се отразяват на бланка L-QS-012-OUNP „Протокол за несъответствие, установено при одит" и се предават на УПР за организиране на тяхното отстраняване.

Когато се използват технически средства за измерване, собственост на дружествата Лирекс.ком, тези средства се поддържат, контролират и калибрират в съответствие с процедурата LPP005 „Управление на средства за измерване и контрол".

11.2. Оценяване на съответствието

Оценяване на съответствието на дейностите по СУЗБУТ с приложимите изисквания на нормативните актове и с другите изисквания, които са въведени в дружествата Лирекс.ком (правилник за вътрешния трудов ред, инструкциите от СУКИС, свързани със ЗБУТ) се извършва под ръководството на УПР при въвеждане на нови технологии, продукти, услуги или при промени в приложимото законодателство.

Резултатите от оценяването на съответствието се отразяват на бланка „OHSAS Assessment" и се представят за обсъждане на Прегледа от Ръководството на СУЗБУТ.

11.3. Разследване на инциденти, несъответствия, коригиращи и превантивни действия

11.3.1. Разследване на инциденти

Инцидент е свързано с работата събитие, при което има нараняване, заболяване или смърт, или което може да доведе до такива последици. Инцидент, който е довел до нараняване, заболяване или смърт, е злополука; а инцидент, при който няма нараняване, заболяване или смърт, се нарича „почти инцидент". Всяка извънредна ситуация е частен случай на инцидент.

При настъпване на инцидент незабавно се предприемат мерки за оказване на първа долекарска медицинска помощ на засегнатите от инцидента и транспортиране на пострадалия до болнично заведение или повикване на бърза помощ. В същото време трябва да бъде обезопасено мястото на злополуката с ограничаване на достъпа от други лица.

След това се изпълняват изискванията на Наредбата за установяване, разследване, регистриране и отчитане на трудовите злополуки. В съответствие с нея за всяка трудова злополука пострадалият, непосредственият му ръководител или свидетелите на злополуката незабавно уведомяват Управителя или упълномощеното от него длъжностно лице.

След уведомлението за трудова злополука, Управителят или упълномощеното от него длъжностно лице са длъжни да организират разследване на обстоятелствата на злополуката. За резултатите от разследването се съставя Протокол, като към него се прилагат писмени показания на свидетелите на злополуката. Протоколът се завежда в Регистъра на актовете за трудови злополуки.

При настъпване на малък инцидент (напр. леко нараняване или др.п., при който не се налага издаване на болничен лист), след оказване, ако е необходимо, на първа долекарска медицинска помощ, този инцидент се регистрира в Регистъра на инциденти, които не са свързани с издаване на болничен лист. Предпазването от такива инциденти е включено в тематиката на началните и периодичните инструктажи по ЗБУТ.

За актуалната редакция и съдържание на процедурата проверете в *LODIS*.

След всяка трудова злополука/инцидент от ОБЗР с помощта СТМ се прави анализ, в който се определят пропуските и недостатъците в ЗБУТ и другите фактори, които могат да причинят това, идентифицира се необходимостта от коригиращи действия, както и възможните превантивни действия с цел да се осигури непрекъснатото подобряване на СУЗБУТ. Служителите се информират за резултатите от анализа.

11.3.2. Несъответствие, коригиращо и превантивно действие

Всички инциденти и „почти инциденти"; констатираните несъответствия или забележки при вътрешните и външните одити на СУЗБУТ; предписания и препоръки от проверки на контролните органи; оплаквания от клиенти или други заинтересовани страни; получените неприемливи стойности при нова оценка на риска; нова информация за опасности на работните места; забелязани пропуски при периодичните проверки на работните места от ОБЗР, както и новите изисквания в приложимото законодателство по ЗБУТ и др.п. се управляват по процедурата LAP003 „Коригиращи действия. Непрекъснато подобрение". Съгласно нея констатираните несъответствия се регистрират на бланките Заявка за коригиращо действие (L-QS-002-CAR) или Протокол за несъответствие, установено при одит (L-QS-012-OUNP).

Констатираните несъответствия се управляват и тяхната ефективност се оценява съгласно процедурата LAP003 „Коригиращи и превантивни действия".

УПР контролира изпълнението на регистрираните коригиращи действия и докладва за състоянието им на Прегледите от Ръководството на СУКИС. Когато се установи, че предприетите действия са неадекватни по отношение на опасностите или може да станат такива, те се преразглеждат и управляват по указания ред. Ако вследствие на тях се въвеждат нови системи, технологии или операции, оценката на риска на работните места от тях се актуализира.

11.4. Вътрешен одит

Вътрешните одити на Системата за управление на здравословните и безопасни условия на труд в рамките на СУКИС се провеждат, за да се установи доколко внедрената в дружествата Лирекс.ком система съответства на планираните дейности за управление на ЗБУТ, включително на изискванията на стандарта ISO 45001, как се поддържа и дали е ефикасна при постигане на политиката и целите.

Периодичните вътрешни одити се извършват в съответствие с процедура LAP002 „Организация на вътрешния контрол (одити)" и Годишния план за вътрешни одити (Audits plans.xls). При установени несъответствия се попълва бланка създават искания за коригиращи действия в съответствие с процедура LAP003 „Коригиращи и превантивни действия".

11.5. Преглед от Ръководството

Висшето ръководство извършва преглед на Системата за управление на здравословните и безопасни условия на труд в дружествата Лирекс.ком през планирани интервали, за да осигури нейната непрекъсната актуалност, адекватност и ефикасност. Прегледите включват оценяване на възможностите за подобряване и необходимостта от промени в СУЗБУТ, включително определената политика и цели.

Периодичните прегледи от Ръководството на СУЗБУТ се извършват в рамките на прегледите от Ръководството на СУКИС в съответствие с процедура LMP003 „Преглед на СУКИС от Ръководството" и Годишния план за прегледите (MngReview Plan).

УПР представя информация на прегледите от Ръководството на СУЗБУТ за:

- действията, последвали от предишни прегледи от ръководството;

- резултатите от вътрешните одити и от оценяване на съответствието с приложимите изисквания на нормативните актове и с другите изисквания, които дружествата са приели да спазват
- резултати от участието на служителите, както консултациите и информацията, съобщена от външни заинтересувани страни, включително жалби;
- изпълнението на дейностите, свързани със ЗБУТ и тяхната ефективност;
- степента на изпълнение на целите по здраве и безопасност при работа;
- състоянието на разследването на инциденти, на коригиращите и превантивните действия;
- промени в обстоятелствата, включително изменения в изискванията на нормативните актове и други изисквания, свързани със здравето и безопасността при работа;
- препоръки за подобряване.

На прегледите от Ръководството на СУЗБУТ се обсъждат и вземат решения и действия, с ангажимент за непрекъснато подобряване и свързани с възможни промени по:

- изпълнение на дейностите, свързани със здравето и безопасността при работа;
- политиката и целите по здраве и безопасност при работа;
- ресурсите;
- другите елементи на СУЗБУТ.

Приетите решения на Прегледа от Ръководството на СУЗБУТ са достъпни за обмен на информация и консултация на Вътрешния портал.

12. Документирана информация

- Всички документи и записи, свързани с въведената СУЗБУТ в рамките на интегрираната СУКИС в дружествата Лирекс.ком, отговарят на изискванията на стандарта ISO 45001 и на приложимото законодателство.
- Документите и записите по СУЗБУТ се оформят в съответствие с изискванията на инструкцията LMI001 „Съдържание и оформление на документи от СУКИС“ или според изискванията на приложимото законодателство.
- Когато съгласно изискванията на приложимото законодателство, актуалните документи (инструкции по ЗБР, методики, планове и др.) и записите (карти за оценка на риска, заповеди, протоколи и др.) трябва да са на хартиен носител и има специфични изисквания към тяхното оформление, те се поставят сканирани на Вътрешния портал.
- Актуалните и валидни версии на документите и записите от СУЗБУТ на Вътрешния портал са достъпни в режим „само за четене“ за всички служители на дружествата Лирекс.ком. Актуализацията на документите в електронен вид се прави от УПР или от Администратора на Вътрешния портал. Файловете на заменените документи и записи се поставят в папка „Архив“, до която достъп имат само УПР и Администратора на Вътрешния портал.
- Документите и записите по СУЗБУТ, които според приложимото законодателство са на хартиен носител, се съхраняват от ОБЗР и Техническия организатор на АСД.

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

- Сигурността на информацията, свързана с изпълняваните дейности по ЗБУТ в дружествата Лирекс.ком, се осигурява от процедурите и инструкциите на въведената Система за управление на качеството и информационната сигурност (СУКИС).
- Информацията, свързана с личните данни и здравословното състояние на работещите в дружествата Лирекс.ком се събира и използва само във връзка с пълното и точно изпълнение на дейностите по ЗБУТ от медицинските специалисти от СТМ и се съхранява, разпространява и предоставя на трети лица при строго спазване на изискванията на приложимото законодателство.
- Унищожаване на излезли от употреба носители на информация, свързана с дейностите по ЗБУТ, се извършва в съответствие с процедурата LSP472 „Унищожаване на информация".

12.1. Форми и бланки

ID на формата	*наименование на формата*
Karta_Ocenka_uslovia_trud.doc	Карта за оценка на условията на труд
Anketna_Karta_rab_mesta.doc	Анкетна карта за работните места
Karti_Ocenki_RM & Risk).	Карти за идентифициране на опасностите и оценка на риска за безопасност и здраве на работещите
InstructionOHSAS-extern.doc	Инструктаж на клиенти на работните места
OHSAS Assessment-YYYYMMDD	Оценяване на съответствието на СУЗБУТ с приложимите изисквания
L-QS-002-CAR	Заявка за коригиращо действие
L-QS-012-OUNP	Протокол L-QS-002-CAR за несъответствие, установено при одит

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

1. История на редакциите

версия	описание на промяната	автор	проверил	утвърдил	дата въвеждане
2	Въвеждане на строителни дейности в обхвата по BS OHSAS 18001:2007	К. Иванов	Б.Йорданов	Д. Илиева	16.09.2014
3	Въвеждане на допълнителни мерки за осигуряване на здравословни и безопасни условия на труд на работните места	К. Иванов	Б.Йорданов	Д. Илиева	10.01.2017
4	Актуализиране на документите от СУКИС	К. Иванов	М.Йончева	Д. Илиева	17.07.2019

2. Предназначение

Документът се използва за определяне на съдържанието на инструктажите и мерките по осигуряване на здравословните и безопасни условия на труд на служителите, които работят на определено работно място в офисите или на обект на клиент на дружествата Лирекс.ком.

3. Приложимост

Документът се прилага за всички работни места в офисите или за обекти на дружествата Лирекс.ком от отговорните служители за провеждане на инструктажите по ЗБУТ и за въвеждане на необходимите мерки за защита за конкретното работно място или дейност.

4. Отговорности

Виж т.4 от процедура LRP004 „Управление на здравословните и безопасни условия на труд".

5. Осигуряване на ЗБУТ на работните места и на обекти на клиент

5.1. Общи изисквания

На всички служители се осигуряват здравословни и безопасни условия на труд съобразно спецификата на провежданата дейност, оценката на риска, другите изисквания на нормативните актове и въведената СУЗБУТ.

При изпълнение на дейности на обект на клиент, по преценка на Ръководителя на проекта в зависимост от характера на работата и след издаване на заповед, специално обучен Отговорен инструктор провежда ежедневни инструктажи по безопасност и здраве на работещите. Той води и съхранява Книгата за ежедневен инструктаж до приключване на проекта, след което я предава на Ръководителя на проекта.

5.2. Дейности по осигуряване на ЗБУТ

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

ЛИРЕКС.КОМ	Инструкция: Осигуряване на здравословни и безопасни условия на труд на работните места	Версия 4
	LRI004	2 от 7

	Работно място/дейност	Вид на инструктажите	Инструкции за безопасност при работа	Приложени мерки за защита
	Работно място в офис - помещение	Начален инструктаж, съвместен с инструктаж на работното място Периодичен инструктаж Извънреден инструктаж	1. Инструкция за безопасна работа с видеодисплеи; 2. Инструкция за безопасна работа с копирна машина; 3. Инструкция за безопасна работа с машина за унищожаване на документи; 4. Инструкция за безопасна работа при експлоатация на електрически уреди и апарати; 5. Инструкция за пожарна и аварийна безопасност; 6. Инструкция за оказване на първа долекарска помощ.	1. Въвеждане на физиологичен режим на труд и почивка 2. Периодични медицински прегледи 3. Обучение за оказване на първа долекарска помощ 4. Обучение за работа с наличните средства за пожарогасене 5. Управление на отпадъците от дейността
	Извършване на сервизна дейност в сервизен център	Начален инструктаж, съвместен с инструктаж на работното място Периодичен инструктаж Извънреден инструктаж	1. Инструкция за безопасна работа с видеодисплеи; 2. Инструкция за безопасна работа при експлоатация на електрически уреди и апарати; 3. Инструкция за пожарна и аварийна безопасност; 4. Инструкция за оказване на първа долекарска помощ.	1. Обучение и придобиване на квалификационна група по електробезопасност. 2. Въвеждане на физиологичен режим на труд и почивка 3. Периодични медицински прегледи 4. Обучение за оказване на първа долекарска помощ 5. Обучение за работа с наличните средства за пожарогасене 6. Управление на отпадъците от дейността
	Извършване на сервизна дейност в обект на клиент	Начален инструктаж, съвместен с инструктаж на работното място Периодичен инструктаж Извънреден инструктаж	1. Инструкция за безопасна работа с видеодисплеи; 2. Инструкция за безопасна работа при експлоатация на електрически уреди и апарати; 3. Инструкция за пожарна и аварийна безопасност; 4. Инструкция за оказване на първа долекарска помощ.	1. Обучение и придобиване на квалификационна група по електробезопасност. 2. Обучение и придобиване на правоспособност за използване на ЛПС за работа на височина и на други технически средства за достъп/подвижни платформи, скелета и др./ със същата цел. 3.При работа на височина провеждане на ежедневен инструктаж от Отговорния инструктор по ЗБУТ.

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

				4. При необходимост, инструктаж от длъжностно лице по ЗБУТ на клиента и точно спазване на инструкциите за безопасна работа на обекта на клиента. 5.Извършване на ежемесечна проверка за изправността на ръчните електрически инструменти. 6.Обучение за оказване на първа долекарска помощ. 7. Управление на отпадъците от дейността.
	Извършване на монтажна дейност на системи за сигурност в обект на клиент	Начален инструктаж, съвместен с инструктаж на работното място Периодичен инструктаж през 3 месеца Ежедневен инструктаж Извънреден инструктаж	1. Инструкция за пожарна и аварийна безопасност 2. Инструкция за безопасна работа с перфоратор 3. Инструкция за безопасна работа с бормашина 4. Инструкция за безопасна работа със строително монтажни пистолети 5. Инструкция за безопасна работа с подвижни електрически съоръжения и удължители 6. Инструкция за безопасна работа с ръчни механични и електрически инструменти 7. Правила за безопасна експлоатация на стълби подвижни, стационарно монтирани, преносими и раздвижни стълби 8. Инструкция за безопасна работа при експлоатация на електрически уреди и апарати 9. Инструкция за оказване на първа долекарска помощ	1. Обучение и придобиване на квалификационна група по електробезопасност 2. Обучение и придобиване на правоспособност за използване на ЛПС за работа на височина и на други технически средства за достъп/подвижни платформи, скелета и др./ със същата цел. 3. Провеждане на ежедневен инструктаж от отговорния инструктор по ЗБУТ за мерките за безопасност при работа на височина 4. Осигуряване на изправни технически средства за достъп/стълби, платформи, скелета и др./ за достигане до мястото за извършване на работата на височина. 5. Осигуряване на работещите с ЛПС /предпазни колани, защитни каски, въжета, обувки, ръкавици, очила и др./ и провеждане на инструктаж за правилното им използване.

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

				6. Осигуряване на работещите със средства за електробезопасност в зависимост от вида на извършваната работа. 7. Проверка за наличие на напрежение в електрическата мрежа преди започване на работа. 8. Извършване на ежемесечна проверка за изправността на ръчните електрически инструменти. 9. Управление на отпадъците от дейността
	Водач на служебен автомобил	Начален инструктаж, съвместен с инструктаж на работното място Периодичен инструктаж Ежедневен инструктаж Извънреден инструктаж	1.Инструкция за водачите на служебни автомобили 2. Инструкция за оказване на първа долекарска помощ 3. Инструкция за пожарна и аварийна безопасност	1. Спазване на изискванията на Закона за движение по пътищата и на Правилника за неговото прилагане. 2. Провеждане и документиряне на ежедневен инструктаж 3. Осигуряване постоянна техническа изправност на МПС от оторизиран сервиз 4. Периодични медицински прегледи 5. Редовни годишни прегледи на МПС 6. Управление на отпадъците от дейността
	Служител в склад	Начален инструктаж, съвместен с инструктаж на работното място Периодичен инструктаж Извънреден инструктаж	1.Инструкция за безопасност на труда при извършване на товарно - разтоварни работи 2. Инструкция за безопасна работа на товаро-разтоварни площадки и складове 3. Инструкция за безопасна работа при работа с транспалетна количка 4. Инструкция за безопасна работа с видеодисплей 5. Инструкция за пожарна и аварийна безопасност 6. Инструкция за оказване на първа долекарска помощ	1. Осигуряване на служителите с работно облекло и ЛПС (обувки с метално бомбе и ръкавици) 2. Работа с изправни технически средства за извършване на товаро-разтоварни работи 3. Въвеждане на физиологичен режим на труд и почивка 4. Обучение за оказване на първа долекарска помощ 5. Периодични медицински прегледи

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

ЛИРЕКС.КОМ	Инструкция: Осигуряване на здравословни и безопасни условия на труд на работните места	Версия 4
	LRI004	5 от 7

				6. Управление на отпадъците от дейността
	Работа в опасна среда (пожароопасна; взривоопасна; наличие на опасни химични вещества или задушливи газове) на обект на клиент	Начален инструктаж на работното място; Периодичен инструктаж Ежедневен инструктаж Извънреден инструктаж	1.Инструкция за оказване на първа долекарска помощ 2. Инструкция за пожарна и аварийна безопасност 3. Инструкция за безопасна работа с перфоратор 4. Инструкция за безопасна работа с бормашина 5. Инструкция за безопасна работа със строително монтажни пистолети 6. Инструкция за безопасна работа с подвижни електрически съоръжения и удължители 7. Инструкция за безопасна работа с ръчни механични и електрически инструменти 8. Правила за безопасна експлоатация на стълби подвижни, стационарно монтирани, преносими и раздвижни стълби 9. Инструкция за безопасна работа при експлоатация на електрически уреди и апарати	1. Задължителен инструктаж от длъжностно лице по ЗБУТ на клиента и точно спазване на инструкциите за безопасна работа на обекта на клиента 2. Ежедневен инструктаж от Отговорния инструктор преди започване на работа и регистриране в книгата за инструктажите 3. Осигуряване на служителите с необходимите за конкретната работа ЛПС 4. Периодични медицински прегледи 5. Управление на отпадъците от дейността
	Извършване на строителни и монтажни работи на обект на клиента	Начален инструктаж на работното място; Периодичен инструктаж Ежедневен инструктаж Извънреден инструктаж	1.Инструкция за безопасна работа при подготовката и дейностите на строителна площадка 2.Инструкция за оказване на първа долекарска помощ 3. Инструкция за пожарна и аварийна безопасност 4. Инструкция за безопасна работа с перфоратор 5. Инструкция за безопасна работа с бормашина 6. Инструкция за безопасна работа със строително монтажни пистолети 7. Инструкция за безопасна работа с подвижни електрически съоръжения и удължители	1. Обучение и придобиване на квалификационна група по електробезопасност 2. Обучение и придобиване на правоспособност за използване на ЛПС за работа на височина и на други технически средства за достъп /подвижни платформи, скелета и др./ със същата цел. 3. Задължителен инструктаж от длъжностно лице по ЗБУТ на клиента и точно спазване на инструкциите за безопасна работа на обекта на клиента

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

			8. Инструкция за безопасна работа с ръчни механични и електрически инструменти 9. Правила за безопасна експлоатация на стълби подвижни, стационарно монтирани, преносими и раздвижни стълби 10. Инструкция за безопасна работа при експлоатация на електрически уреди и апарати	4. Ежедневен инструктаж от Отговорния инструктор преди започване на работа и регистриране в книгата за инструктажите 5. Осигуряване на служителите с работно облекло и необходимите за конкретната работа ЛПС 6. Периодични медицински прегледи 7. Управление на отпадъците от дейността

6. Блок схеми

Не се изисква блок-схема .

7. Термини и съкращения

Лирекс.ком	Дружествата Лирекс БГ, Лирекс БС, Лирекс Хай Тех, Беолик, Лирекс Скопие и Теза.
Здравословни и безопасни условия на труд	Условия и фактори, които влияят или могат да повлияят върху здравето и безопасността на персонала (включително временно наетия персонал и персонала на контрагентите), посетителите и всички други хора на дадено работно място.
Система за управление на здравословни и безопасни условия на труд (СУЗБУТ)	Част от СУКИС, която разработва и внедрява своята политика по здравословни и безопасни условия на труд и управлява рисковете за здравето и безопасността при работа.
Работно място	Всяко физическо местоположение, където се извършват дейности, свързани с работата, управлявани от организацията.
Служба по трудова медицина (СТМ)	Звена с превантивни функции, което консултира и подпомага работодателя, комитетите и групите по условия на труд в планирането и организирането на дейностите по осигуряване и поддържане на ЗБУТ.
Орган по безопасност и здраве (ОБЗР)	Служител на Лирекс.ком, на когото е възложено изпълнението на дейностите по организация, координация и контрол на дейностите по осигуряване на ЗБУТ.

8. Препратки към документи

ID на документа	*наименование на документа*
LRP004	Процедура: Управление на здравословните и безопасни условия на труд

9. Оценки

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

Оценките, свързани с изпълнението на дейностите по настоящия документ, се представят на Годишния преглед от ръководството.

10. Документирана информация

Началният инструктаж на работното място, периодичните и извънредните инструктажи (след злополука или авария) се регистрират в Книгата за инструктаж на съответното дружество.

За документиране на началния инструктаж на всеки служител, ОБЗР попълва Служебна бележка по образец за съответното дружество, която се съхранява в личното трудово досие на служителя.

Ежедневните инструктажи се записват в съответната Книга за ежедневен инструктаж. След нейното изписване се предава за съхранение на Техническия организатор на АСД. Останалите книги за инструктаж се съхраняват от ОБЗР на дружествата и от отговорниците на офиси извън София.

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

1. История на редакциите

редакция	описание на промяната	автор	проверил	утвърдил	дата въвеждане
3	Промени в съответствие с OREP0135	Цв.Цифудин	Б.Йорданов	Д.Илиева	08.06.2007
4	Въвеждане на изискванията на ISO 9001:2008 и ISO/IEC 27001:2005	Цв.Цифудин	Б.Йорданов	Д.Илиева	30.01.2009
5	Актуализиране на документите от СУКИС	М. Йончева	Д. Маринов	Д. Илиева	09.07.2019

2. Предназначение

Инструкцията определя реда за изпълнение на сервиз на технически и базови програмни средства от Сервизните Центрове на дружествата *Лирекс.ком,* и реда за ескалация на проблемите във връзка с изпълнението на задължения за сервизно обслужване.

3. Приложимост

Регламентираният в инструкцията ред се прилага при всички форми за сервизно обслужване, предлагани на клиентите от дружествата *Лирекс.ком*. Изключения в реда за изпълнение на сервизните дейности и за документиране на сервизните операции се прави само в случаите на специфични изисквания за управление на проекти, регламентирани от процедура *LPP006 Управление на програми и проекти,* или в договорните отношения с клиента.

Инструкцията е задължителна за изпълнение от всички функционални звена на *Лирекс.ком*, които осъществяват сервизни дейности на технически и базови програмни средства.

Сервизно обслужване за инсталиране на технически и базови програмни средства, и за обучение се осъществява съгласно изискванията на договор/споразумение с клиент, а не по реда от настоящата процедура.

Взаимодействието на процеса за сервиз, регламентиран с реда от настоящата инструкция, с другите процеси за сервизно обслужване на технически и базови програмни средства се осъществява съгласно изискванията на процедура *LPP601 Организация и управление на сервизната дейност.*

Практическата реализация на сервизни дейности на технически и стандартни програмни средства се осъществява в съответствие с техническата документация за съответните устройства, операционни системи, програми.

4. Отговорности

4.1. Ръководител на Главен сервизен център

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

- определя структурата на записите в Дневника за Сервизни Дейности за всички сервизни центрове;
- контролира сервизното обслужване по проекти, реализирани от организацията;
- създава организация за правилно изпълнение на реда за ескалация на проблемите от всички сервизни центрове и контролира съблюдаването й;

4.2. Ръководител на Сервизен център

- организира и контролира изпълнението на сервизните дейности от служителите на Сервизния Център;
- планира изпълнението на сервизните операции, в съответствие с потребностите и квалификацията на сервизните специалисти;
- определя структурата на записите в Дневника за Сервизни Дейности и контролира коректността на записите в дневника.

4.3. Сервизен специалист

- изпълнява качествено и в срок възложените му за изпълнение сервизни операции, в съответствие с изискванията на настоящата инструкция;
- своевременно докладва на длъжностните лица за възникнали проблеми по изпълнението на сервизното обслужване, съгласно изискванията за ескалация на проблемите.

4.4. Диспечер на сервизен център

- поддържа информационните фондове на сервизния център за реализацията на сервизните операции;
- координира изпълнението на сервизните операции, съгласно разпорежданията на ръководителя на сервизния център;
- следи за правилното и своевременно документиране на сервизните дейности;
- уведомява клиентите за изпълнени ремонти;
- посреща клиентите в приемната на сервизния център и им оказва пълно съдействие за изясняване на техните потребности;
- попълва заявки за сервизно обслужване /ЗСУ/ за изпълнение на задължения за сервизно обслужване в обектите на клиенти;
- докладва на ръководителя на сервизния център за възникнали проблеми.

5. Процедура

5.1. Общи принципи за организация на сервизните дейности

- Организацията и управлението на всички операции за сервиз на технически и базови програмни средства се основават на принципа за работа със *сервизна услуга*. Услугата, независимо от повода за нейното иницииране, се свързва със *заявка за сервизна услуга /ЗСУ/,* която е обект на регистрация, планиране на изпълнението и контрол от момента на пораждането до окончателното й изпълнение (приключване).

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

- За планиране и управление на сервизните операции, в сервизния център се поддържа *Дневник за Сервизните Дейности /*ДСД/, в който се правят записи за: регистрацията на всяка *заявка за сервизно обслужване /ЗСУ/*, отговорните за изпълнението й, етапите (състоянието) на изпълнение;
- Структурата на записите в *дневника за сервизни дейности /ДСД/* се определя от ръководителя на главния сервизен център;
- Всички документи /записи във връзка с изпълнението на дадена *заявка за сервизно обслужване /ЗСУ/* се съхраняват в *пакета на ЗСУ*. В пакета се съхраняват оригиналите на документите или копие, ако е предвиден друг ред за съхранение на оригиналите;

По разпореждане на ръководителя на главния сервизен център, за клиент на абонаментно обслужване се поддържа *досие на клиента* или за обект на клиента, ако има повече такива. В досието се включват опис на всички *заявки за сервизно обслужване /ЗСУ/*, изпълнени в даден обект.

- За проучване степента на удовлетвореност на клиентите от качеството на осъществяваното сервизно обслужване, ръководителят на Сервизния Център следи за осъществяване на проучвания в съответствие с изискванията на процедура *LAP001 Измерване степента на удовлетвореност на клиентите.*
- При изпълнение на сервизните операции се съблюдават следните общосистемни изисквания:
    - манипулирането, съхранението и опаковането на технически средства се осъществява съгласно процедури *LPP002 Идентификация и проследимост на продукти и услуги, LPP003 Работа с продукти на клиент* и *LPP004 Манипулиране, съхранение, опаковане и доставка на продукти*;
    - работа с продукти, които не отговарят на изискванията се осъществява съгласно процедура *LAP004 Работа с продукти, несъответстващи на определените изисквания.*
- Изписване на резервни части от складове *Резервни части* и *Оборотна техника,* и предаването в складовете на дефектирали части се осъществява съгласно инструкция *LPI604 Управление на резервни части за технически сервиз;*
- Поръчка на резервни части за изпълнение на ремонтна дейност се осъществява съгласно инструкция *LPI604 Управление на резервни части за технически сервиз;*
- За извършените срещу заплащане сервизни услуги се издават финансово-отчетни документи със средствата на автоматизираната система *MS Dynamics NAV.*

5.2. Реализация на операциите

Изпълнимите операции от процеса и тяхната взаимовръзка са показани на блок-схемите от *Раздел 6* на инструкцията.

5.3. Ескалация на проблемите

В изпълнение на декларираната политика на организацията за осигуряване изискваното качество на предлаганото на клиентите сервизно обслужване, се прилагат следните правила за ескалация на проблемите:

За категоризация на реакциите относно постъпили от клиент съобщения за възникнал проблем, изискващ сервизно обслужване, се прилагат следните определения:

време за реакция	времето от момента на получаване на съобщение от клиент за възникнал проблем до началото на първоначална диагностика от сервизен специалист за идентификацията на причините за проблема;
срок за отстраняване на проблем	периодът от време, в течение на който Лирекс.ком е поел ангажимент за отстраняване на проблем, считано от момента на получаване на съобщение от клиент. Може да се регламентира в абсолютни или относителни стандартно приетото работно време единици – часове, дни.

За възникнал проблем, изискващ сервизно обслужване, клиентът определя приоритет в зависимост от важността за неговите бизнес-функции.

Приоритетите се определят по следната схема:

Приоритет 1	Системата (хардуер и базов софтуер) на клиента е в нефункционално състояние, което е критично за клиента, ако работоспособността на системата не се възстанови бързо. Не съществува алтернатива за изпълнение на нефункциониращите компоненти на системата. *Дружествата Лирекс.ком* и клиентът трябва да ангажират всички необходими ресурси за решаване на проблема в договореното време за отстраняване на проблем, без да се има предвид стандартно приетото работно време.
Приоритет 2	Системата (хардуер и базов софтуер) на клиента е частично нефункционираща, което засяга важни аспекти на бизнес операциите. Не съществува алтернатива за изпълнение на нефункциониращите компоненти на системата. *Дружествата Лирекс.ком* и клиентът трябва да ангажират всички необходими ресурси за решаване на проблема в

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

	договореното време за отстраняване на проблем, с отчитане на стандартно приетото работно време.
Приоритет 3	Системата (хардуер и базов софтуер) на клиента е частично нефункционираща, но повечето бизнес операции се изпълняват.
Приоритет 4	Клиентът иска информация или консултации относно функционалните възможности на продуктите, направени инсталации и настройки.

Приоритет 1 е приложим за договорено сервизно обслужване 7 (дни в седмицата) x 24 (часа в денонощието).

Приоритети 2, 3 и 4 са приложими за договорено сервизно обслужване в рамките на стандартно приетото работно време - 5 (дни в седмицата) x 9 (часа в денонощието).

При искане за сервизно обслужване, клиентът съобщава определения според него приоритет.

В процеса на изпълнение на заявката за сервизно обслужване /ЗСУ/, категоризирана с приоритет за обслужване, се уведомяват длъжностни лица от организацията за естеството на възникналия проблем, взетите мерки и състоянието на работата по отстраняване на проблема по схема от *Приложение 1*.

Доклад за проблема осъществява сервизният специалист, на когото е възложено изпълнението на заявката за сервизно обслужване /ЗСУ/.

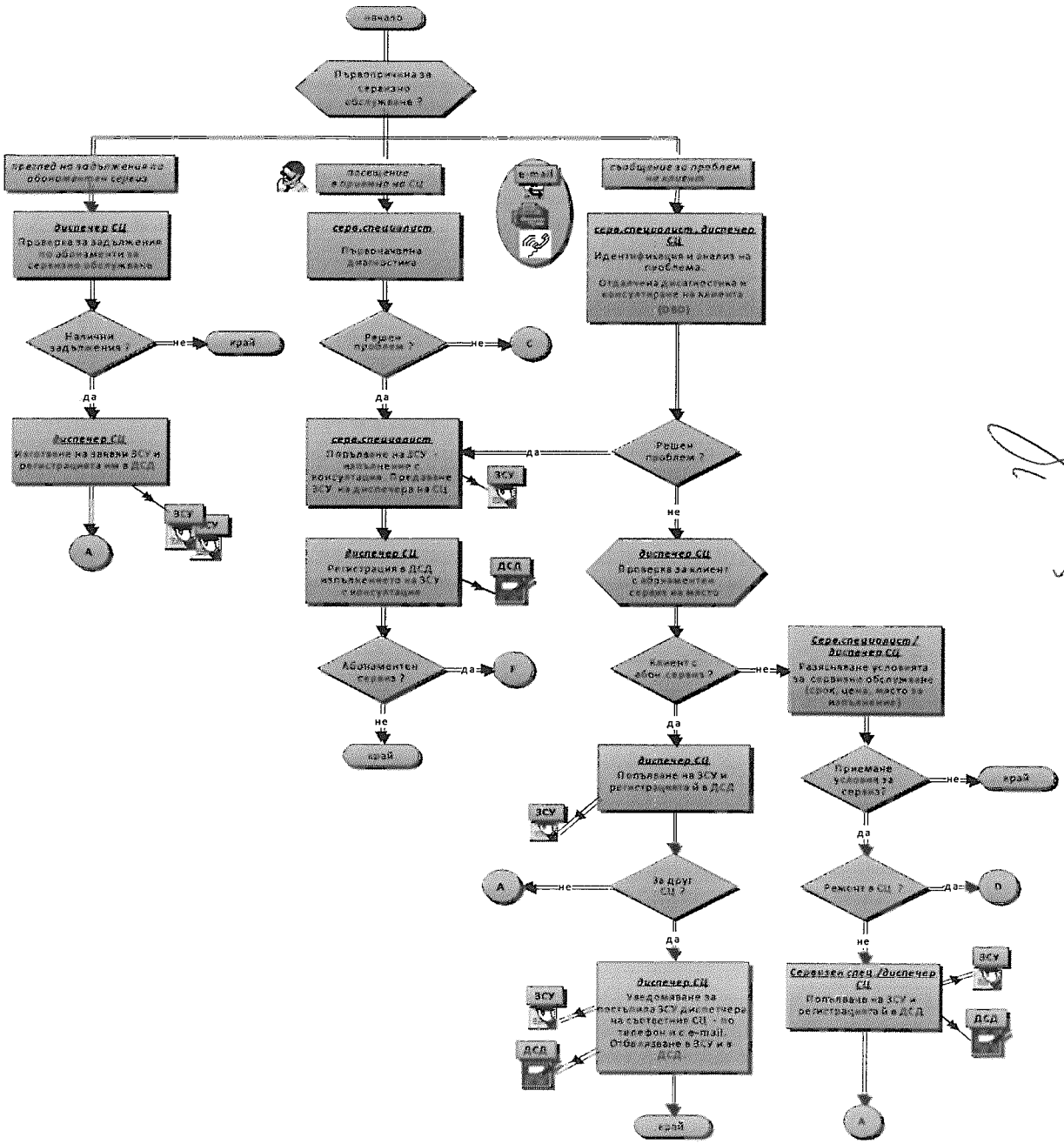
Процесът за ескалиране на проблем към висшето ръководство на организацията – управители и директори, може да се преустанови само по тяхно разпореждане.

За предприетите мерки за отстраняване на възникнал проблем, изискващ сервизно обслужване, ръководителят на сервизния център уведомява лично оторизираните представители на клиента. По негово устно разпореждане уведомяването може да осъществи и друг служител от сервизния център.

При необходимост, ръководителят на главния сервизен център уведомява и търси съдействието на сервизната организация на съответния вендор.

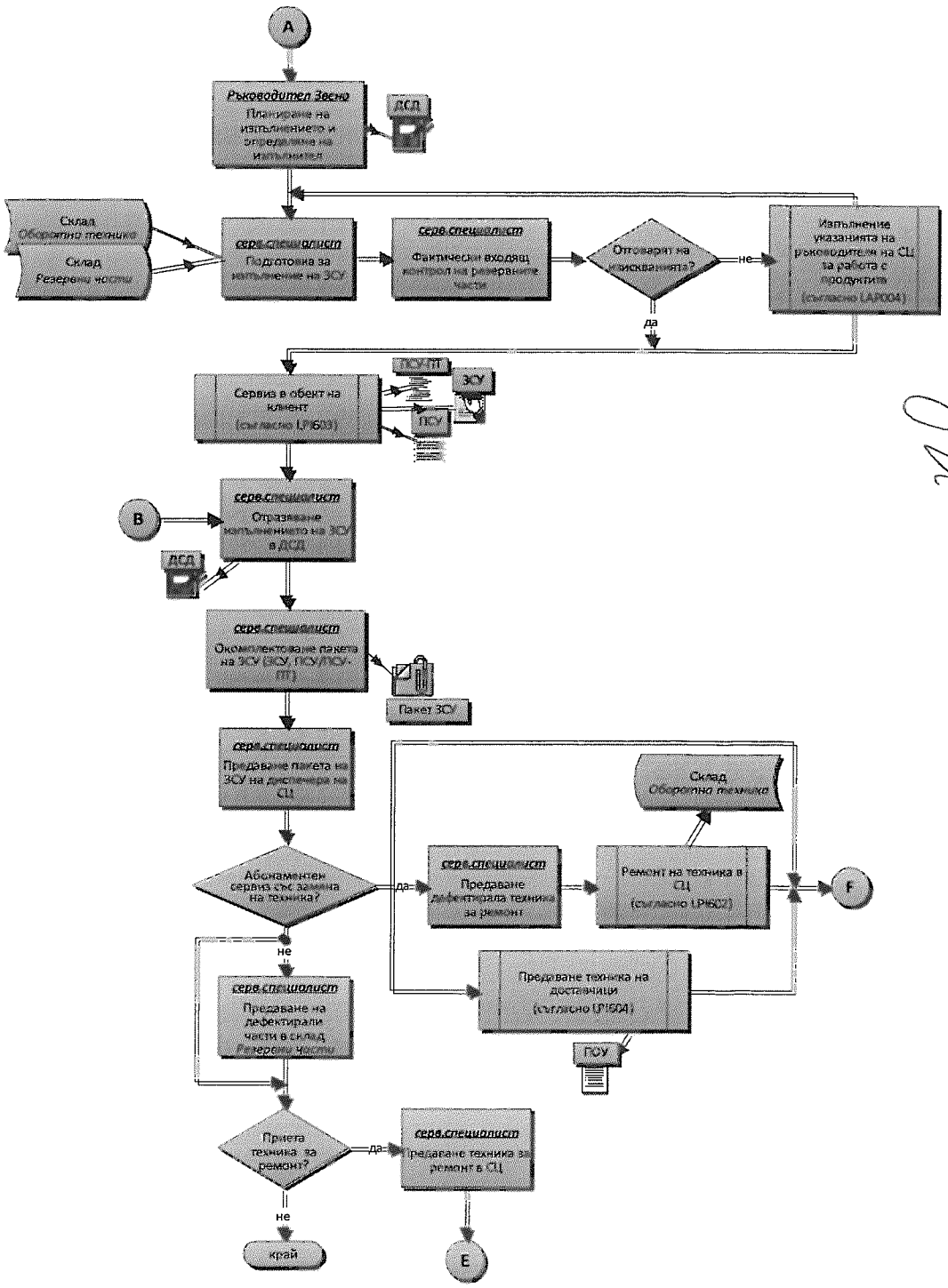
чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

6. Блок схеми



чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

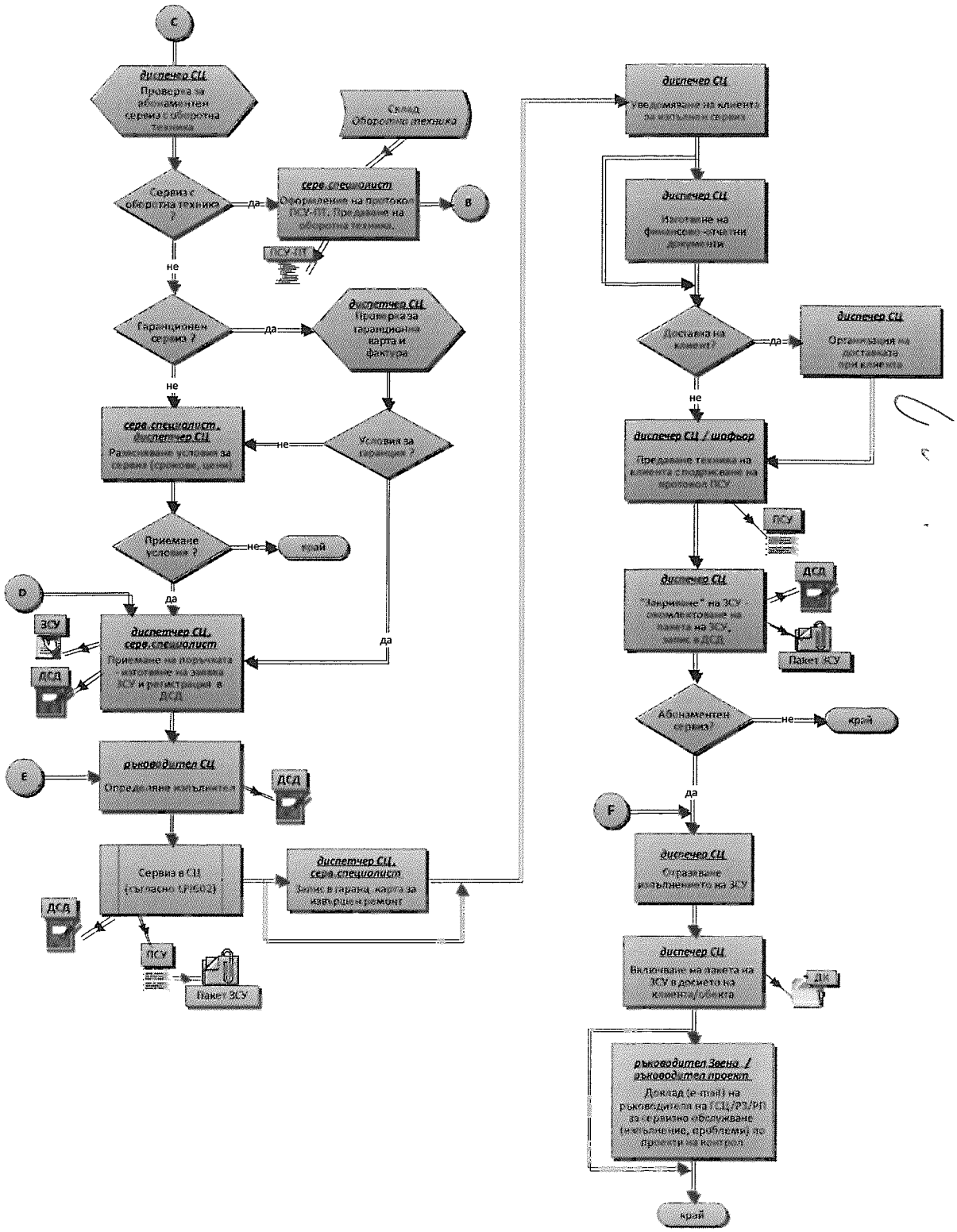
чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679



За актуалната редакция и съдържание на процедурата проверете в *LODIS*.

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

ЛИРЕКС.КОМ	Инструкция: Сервиз на технически и базови програмни средства	Версия 5
	LPI601	8 от 12



За актуалната редакция и съдържание на процедурата проверете в *LODIS*.

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

7. Термини и съкращения

Ръководител на ГСЦ	Служител на *Лирекс.ком*, отговарящ за организацията и управлението на сервизните дейности в цялата фирма.
Ръководител на СЦ	Служител на Лирекс.ком, отговарящ за организацията на сервизните дейности в СЦ и за тяхното качество.
Диспечер на СЦ	Служител, отговарящ за: • контактите с клиенти; • координацията на действията между служителите в СЦ, съгласно разпорежданията на ръководителя на СЦ; • координацията на действията между СЦ чрез диспечери; • поддържане на информационните фондове за сервизно обслужване.
Ескалация на проблем	Политика на дружеството за своевременно уведомяване на съответни ръководни нива за възникнал проблем, с цел: • контрол за състоянието на работата по отстраняване на проблема; • ангажиране на необходимите за решаване на проблема ресурси; • участие на всички ръководни нива за осигуряване на декларираното ниво на качеството на продукти и услуги; • осведомяване на клиента за вземаните мерки за отстраняване на проблем;
Резервна част	Фабрично произведен компонент или устройство, което не подлежи на ремонт в СЦ.
Оборотна техника	Технически средства, които се предоставят на клиента в замяна на дефектирали технически средства.
СЦ	Сервизен Център
ГСЦ	Главен Сервизен Център
ДП	Диспечерски пункт. Специализирано функционално звено на клиента, контролиращо състоянието на техническите средства и координиращо сервизното обслужване.
ЦП	Център за Поддържане. Център за регистрация и контрол изпълнението на сервизно обслужване на комплексни проекти, в които участва *Лирекс.ком*. По правило Центърът не е функционална структура на *Лирекс.ком*.

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

Service Case Tracking System (SCTS)	Web-базирана система за проследяване на сервизните заявки – http://svccases.lirex.com.

8. Препратки към документи

ID на документа	*наименование на документа*
LMP002	Процедура: Управление на документи и записи за реализация на фирмените дейности
LMP003	Процедура: Преглед на СУКИС от Ръководството
LPP002	Процедура: Идентификация и проследимост на продукти
LPP003	Процедура: Работа с продукти на клиент
LPP004	Процедура: Манипулиране, съхранение, опаковане и доставка на продукти
LPP006	Процедура: Управление на програми и проекти
LPP013	Процедура: Управление на външни ИТ услуги
LPI601	Инструкция: Сервиз на технически и базови програмни средства
LPI602	Инструкция: Реализация на сервизни операции в СЦ
LPI603	Инструкция: Сервизно обслужване в обект на клиент
LPI604	Инструкция: Управление на резервни части за технически сервиз
LAP001	Процедура: Измерване степента на удовлетвореност на клиентите
LAP003	Процедура: Коригиращи и превантивни действия
LAP004	Процедура: Работа с продукти, несъответстващи на определените изисквания
MSD NAV	Документация, инструкции, промени по системата – eportal/Внедряване NAV
SCTS_Use	Ръководство за работа на потребителя с SCTS
SCTS_Adm	Ръководство за администриране на SCTS

9. Оценки

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

Оценките, свързани с изпълнението на дейностите по настоящия документ, се представят на Годишния преглед от ръководството.

10. Документирана информация

За контрол на сервизните операции в сервизния център се поддържа *дневник за сервизните дейности* /ДСД/, видим on-line в SCTS. В дневника се регистрира всяка *заявка за сервизни услуги /ЗСУ/* и нейният изпълнител. В записите от дневника се отразява всяка промяна в изпълнението на сервизните услуги. Записи в *дневника на сервизните дейности /ДСД/* се правят съгласно инструкции *LPI601 Сервиз на технически и базови програмни средства* и *LPI602 Реализация на сервизни операции в СЦ.*

Сигурността на информацията, свързана с изпълняваните дейности се осигурява от процедурите и инструкциите на въведената *Система за управление на качеството и информационната сигурност /СУКИС/.*

Информацията, свързана с личните данни и търговската дейност на клиентите се събира и използва само във връзка с точното и навременно изпълнение на техните заявки и осигуряване на необходимото качество на обслужването.

10.1. Форми и бланки

ID на формата	*наименование на формата*
	Заявка за сервизна услуга
L-TS-004-PEU	Предавателен протокол за изпълнение на сервизно обслужване

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679

Приложение 1

СХЕМА

за доклад при ескалация на проблемите

период за доклад (в часове)	*приоритет 1*	*приоритет 2*	*приоритет 3*	*приоритет 4*
1	Ръководител СЦ			
4	Ръководител ГСЦ	Ръководител СЦ	Ръководител СЦ	
12	Търговски директор	Ръководител ГСЦ		
24	Управител	Търговски директор	Ръководител ГСЦ	Ръководител СЦ
48		Управител		
72			Търговски директор	
96				Ръководител ГСЦ

За актуалната редакция и съдържание на процедурата проверете в *LODIS*.

чл. 36а, ал. 3 от ЗОП,
във вр. с чл. 5, параграф 1,
буква "в" от Регламент (ЕС) 2016/679