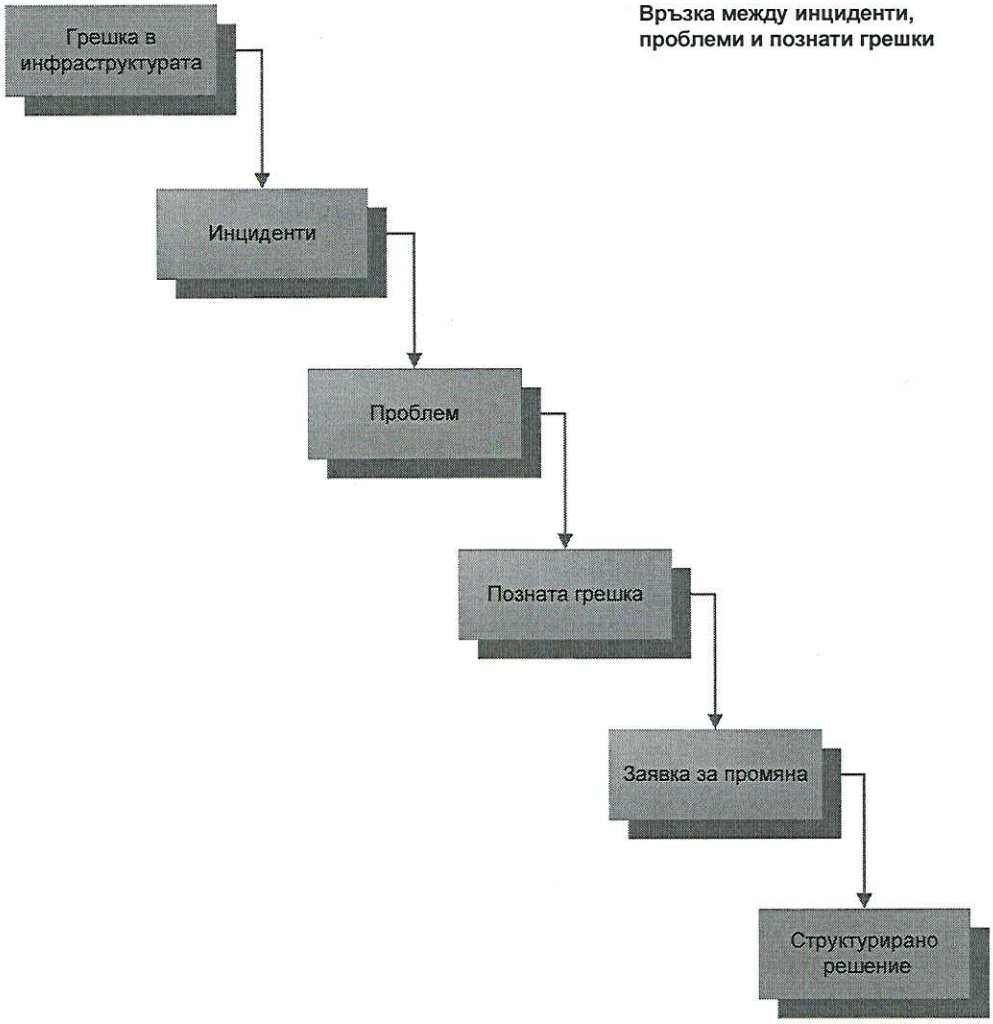
Управлението на проблемите се фокусира върху трансформиране на проблемите в познати грешки.

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.

Връзка между инциденти, проблеми и познати грешки



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).

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.

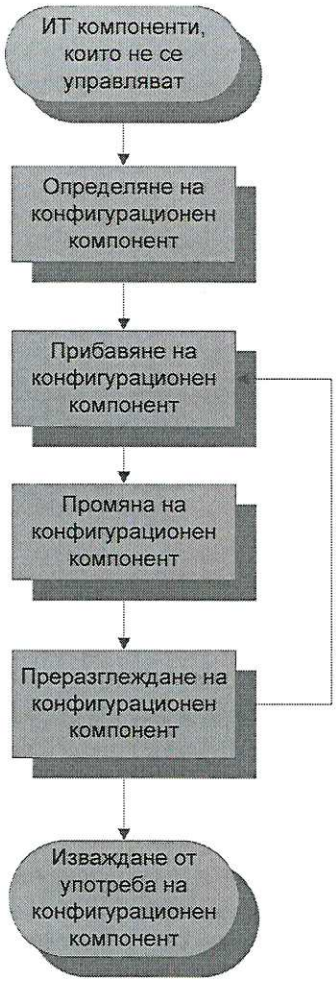
Управление на конфигурацията

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.

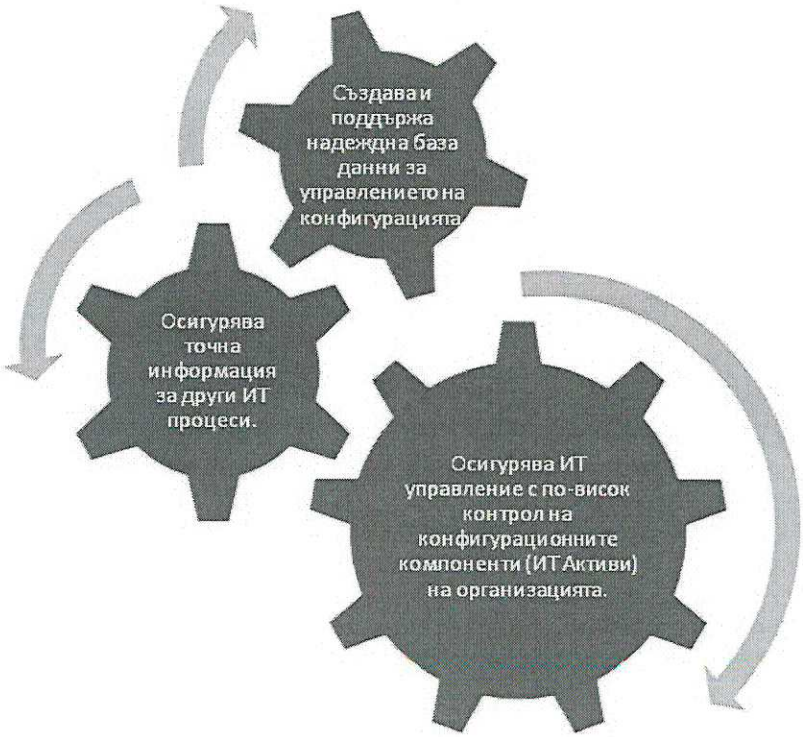
Процесът на управление на конфигурацията може да се счита като основен за всички други (особено за поддръжка на услугите) процеси. Управлението на конфигурацията се счита за централен и поддържащ останалите.

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.



Основните цели на процеса на управление на конфигурацията:

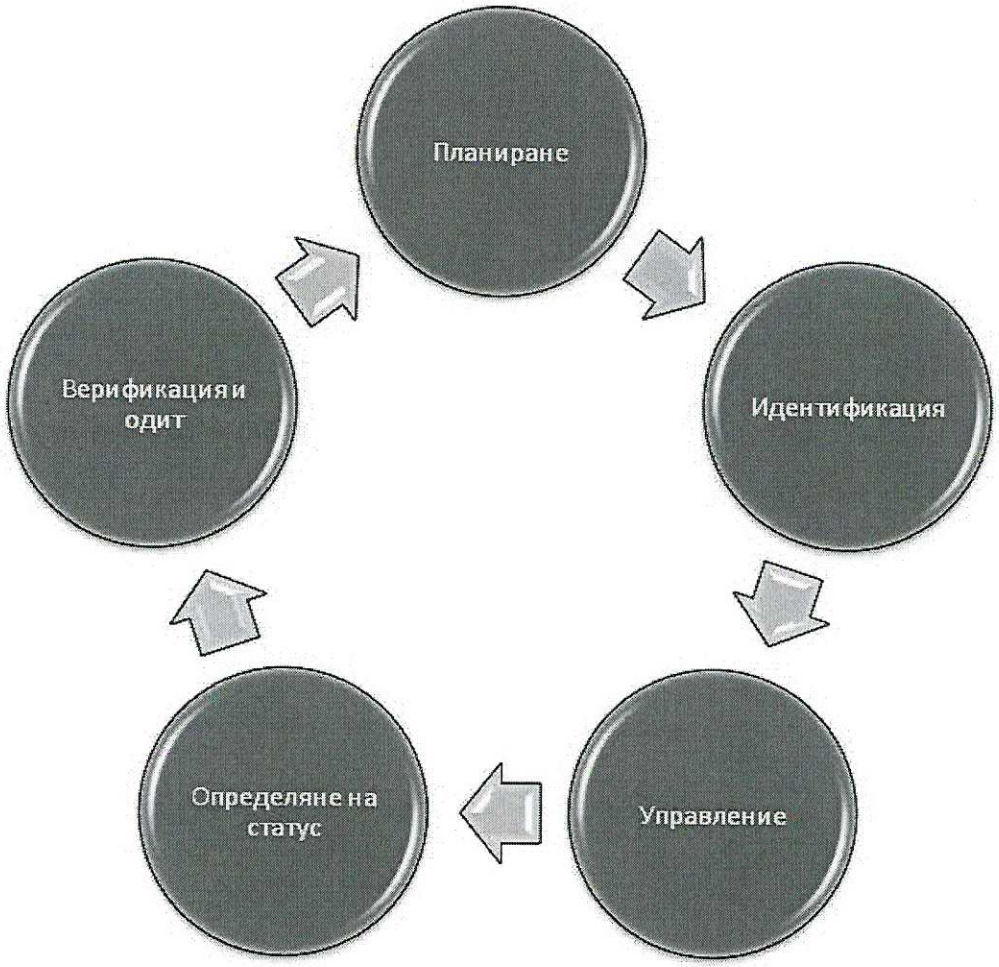


Голяма част от входната информация идва от управлението на промените и изисква информация относно компонентите, които ще въздействат на статуса на променените компоненти.

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.

Дейности на процеса на управление на конфигурацията са:



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 й. 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:
  - Нови версии на интернет/доставчици
  - 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 клиента.

Друг катализатор на промяна може да бъде предварителния план на промените FSC (Forward Schedule of Changes). Планът предварително се съгласува с представител на клиента. 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 процесът на управление на промените трябва да направи за влиянието (потенциално или не) или предложената промяна.

След съгласуване и приемане от Възложителя (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.

Управление на версиите

След като една или повече промени са утвърдени, тествани и представени във версии за разработване, управлението на версиите е отговорно за реализирането на тези промени и управление на техните версии. Управлението на версиите също спомага за ефективното въвеждане на промените чрез комбинирането им в една версия и чрез разработването им заедно.

Основна цел на управлението на версиите е да планира и наблюдава успешното разработване на софтуера и съответния хардуер.

Управлението на версиите може да се използва и за:

- Важни софтуерни разработки;
- Свързване или групиране на близки промени;
- Актуализиране на разработките.

Управлението на версиите управлява изцяло софтуера от закупуването или разработването до тестването и евентуалната миграция в продукта.

Процесът стартира с планиране на нови версии, независимо дали са за хардуер или софтуер и завършва с документиране, сигурно съхранение и внедряване с възможно най-малко влияние върху текущите дейности в организациите.

Отговорности:

- Планиране, предвиждане и успешно разработване на нов или променен софтуер и документиране на свързания хардуер;
- Взаимодействие с управлението на промените, за да се съгласува точното съдържание и плана за разработване на версията;
- Гарантира, че всички компоненти, които са разработени или променени са защитени и проследени чрез базата данни за управление на конфигурацията.

Целта на процеса за управление на версиите е да гарантира, че всички промени са внедрени успешно в ИТ средата по най-безвреден начин. Следователно, управлението на версиите е отговорно за:

- Стратегията на версиите, която включва проектиране, планиране и определяне на подход за разгръщане на промените със съдействието на консултативния борд на промените;
- Определяне на готовността на всяка версия на базата на определени критерии.

Управлението на версиите извършва следното:

- Осигурява цялостна версия на всички направени промени, одобрени от управлението на промените;
- Процесът на управление на версиите е зависим от процеса на управление на промените, тъй като последния одобрява и проследява промените по време на управление на версиите;
- Гарантира, че колкото и промени да са направени, те са предадени на управлението на конфигурацията за въвеждане в базата данни за управление на конфигурацията;

- Нуждае се от информация от управлението на конфигурацията, за да построи и провери валидността на тестовата среда във фазата на развитие на нова версия;
- Нуждае се от управлението на конфигурацията, за да оцени влиянието на промените върху ИТ средата и да осигури окончателно съхранение на версията.

Внедряването на процес на управление на версиите осигурява следните предимства:

- Издават се версии на софтуера, които се тестват и разработват по контролиран начин, така се понижава шансът за грешки;
- Издават се версии на софтуера, които се тестват и разработват по контролиран начин, така се понижава шанса за грешки;
- Софтуерът на (източника, товарите и изпълнимите файлове) организацията се намира на защитено място наречено дефинирана софтуерна библиотека DSL (Definitive Software Library);
- Възможност за внедряване на много на брой едновременни промени в софтуера без да се въздейства на качеството на ИТ средата;
- Софтуерът в отдалечени места може да се управлява ефективно и икономично от централна точка;
- Възможността да се използват нелегални копия е драстично намалена;
- Влиянието на новия хардуер се тества предварително чрез инсталиране в инфраструктурата;
- Крайните потребители са информирани за новите версии и включени в тестването им, в резултат рискът от нестабилност в ИТ средата се понижава драстично.

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 гарантирани 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;
- Изработва, преглежда и поддържа каталог на услугите.

1.7 Схема на ескалация

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 на партньора (напр. Cisco TAC). 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 ръководител 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	Ръководител проект	Ръководител 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.
		Ръководител 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 на партньора (напр. Cisco TAC). 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 ръководител 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	Ръководител проект	Ръководител 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.
		Ръководител 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 на партньора (напр. Cisco TAC). 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.
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	Ръководител проект	Ръководител 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.
		Ръководител 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.

1.8 План за управление и осигуряване 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.

Изпълнителят е сертифициран по системата за управление на качеството ISO 9001:2009 и ще прилага нея при работата по проекта.

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

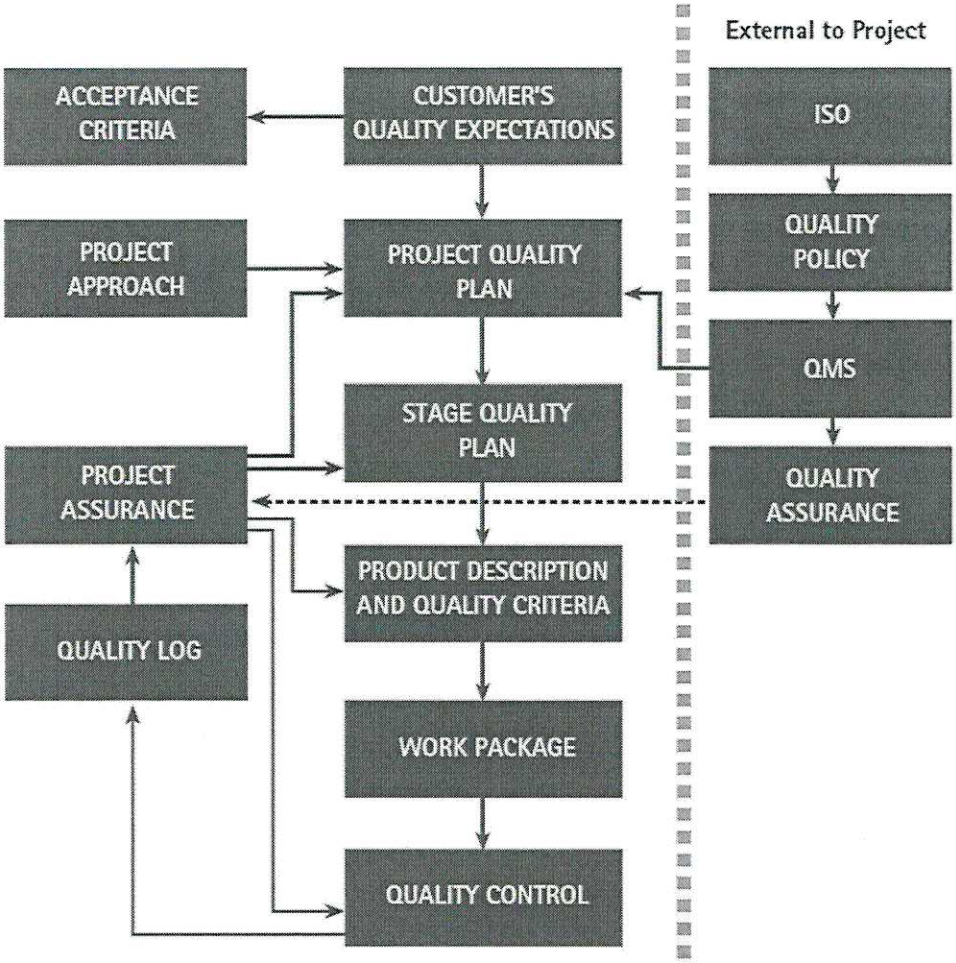
Гарантирането на качеството в проекта се управлява чрез План за осигуряване на качество на проекта (ПКП). Този план се добавя към Плана на проекта.

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.



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;
- 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

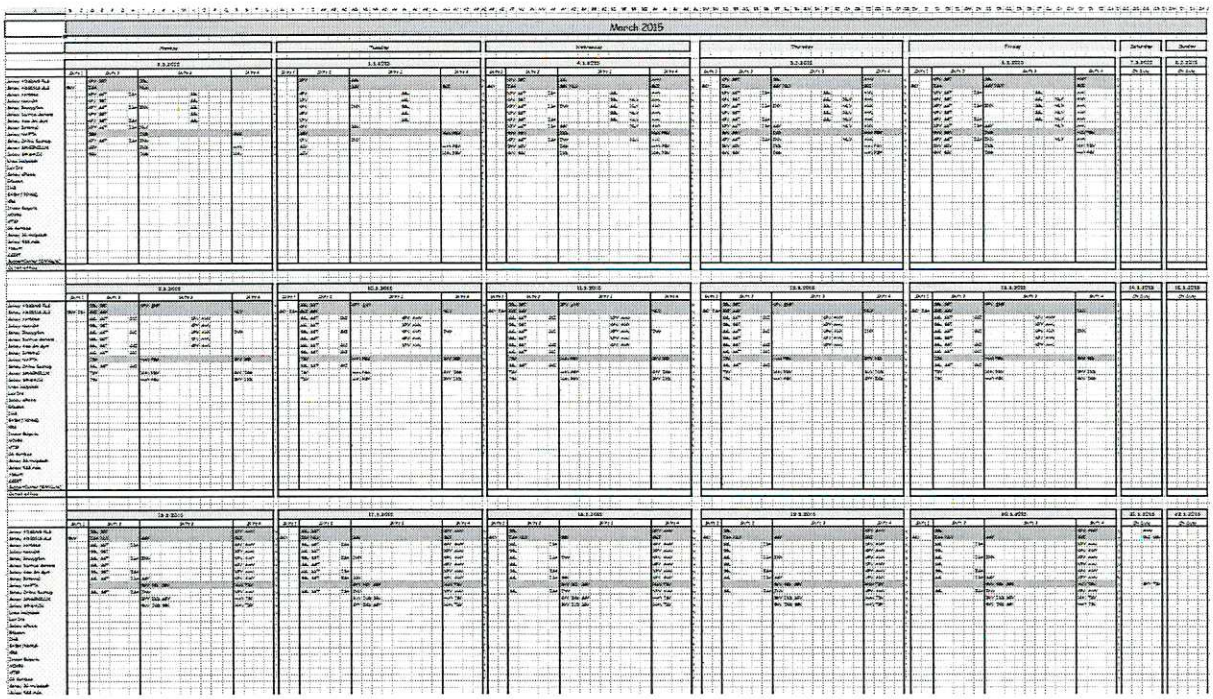
Важно значение за гарантиране качеството на изпълнението на проекта са внедрените системи за управление на качеството по международно признати стандарти от Изпълнителя, както следва:

- ISO 9001;
- ISO 20000-1;
- ISO 27001;
- ISO 14001;
- OHSAS 18001.

1.9 План за управление на непрекъснатостта и наличността на услуга

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

Наличността на услугата се обуславя от наличността на персонала съгласно Attendance форма.



2 Техническо предложение съгласно Техническа спецификация на Възложителя

2.1 Общи характеристики при изпълнение на услугата

Лирекс БГ се ангажира да извършва със свои средства (включително транспорт) поддръжката на локалната информационна инфраструктура (услуга тип 1) и поддръжка на единен център за предоставяне на информация на граждани (услуга тип 2). Разходите за транспорт, комуникации, такси, трудови възнаграждения на екипа на Изпълнителя, абонаментни договори с производители на хардуер и софтуер и резервни части за услуга тип 2, и всички други присъщи разходи, свързани с предоставяне на комплексната услуга по поддръжка в описания по-долу обхват са изцяло за сметка на Изпълнителя и са калкулирани в предложената цена.

За изпълнение на настоящата поръчка компанията разполага с експертен екип от технически компетентни лица, които са преминали съответните курсове на обучение и покриват поставените от Възложителя минимални изисквания.

Лирекс БГ разполага с капацитет да осигури необходимите решения за:

1. Отдалечено наблюдение на статуса на устройствата;
2. Мониторинг на основните системи и програми;
3. 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.
4. Възможност за подаване на заявки 24 часа в денонощието, 365 дни в годината;
5. Осигуряване на минимум 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. 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 Helpdesk система на 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.

Услугата по поддръжка ще включва минимум следните дейности:

- 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;
- Попълване на сервизен протокол;
- Диагностика на повреденото устройство (за услуги тип 2);
- Ремонт/възстановяване работоспособността на устройството (за услуги тип 2);
- Отчитането на сервизната дейност за услуги тип 2 ще се осъществява чрез изготвяне на протоколи за всеки ремонт, които се подписват от упълномощени от МТСП лица и от съответните сервизни инженери и съдържат: имената на специалистите, извършили ремонта, причината за повредата, вложените резервни части и материали.

2.2 Място за изпълнение:

Местата за изпълнение предмета на поръчката са, както следва:

- за услуга тип 1 – МТСП, ул. „Триадица“ 2;
- за услуга тип 2 – МТСП, ул. „Триадица“ 2;

2.3 Спецификации на оборудването за поддръжка:

Видът и броят на подлежащите на поддържане технически устройства и софтуер за съответния тип услуга са както следва:

Таблица 1. Описание на техническата и програмна среда в информационната инфраструктура на МТСП за услуга тип 1

Оборудване	**Брой**
HP Proliant BL460c G1	7
HP Proliant ML150 G6	1
HP ProLiant DL360 G5	1
HP ProLiant DL380 G5	3
HP ProLiant ML350 G5	1
HP Blade Chassis c7000	1
HP EVA 4400	1
Cisco UCSC-BSE-SFF-C200	2
Други	9
Виртуални машини	14
Enterprise Grade UPS	3
Сървър Lenovo IBM System x3550 M5, тип 1	5
Сървър Lenovo IBM System x3550 M5, тип 3	2
Сървър Lenovo IBM System x3630 M4	1
Споделен дисков масив Huawei OceanStor 5500	1
SAN комутатор Lenovo Brocade 6505 FC	2
Лентово устройство за архивиране HP StorEver 1/8 G2	1
UPS APC SRT10kxli	1
Комутатор Cisco C6800IA-48TD	7
Комутатор Cisco C6880-X-LE	1
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
Сървърни операционни системи	**Брой**
Microsoft Windows 2000/2003/2008/2012	30
Linux/Unix	8

От 300 до 350 работни места(всяко работно място е с персонален компютър, свързан с принтер и/или скенер).

Таблица 2. Списък на хардуер и софтуер за единен център за предоставяне на информация за услуга тип 2.

№	Наименование, параметри	Количество
	Хардуер	
1	Сървър Марка Cisco Systems/ Модел UCSC-BSE-SFF-C200 - (C200 M2 SFF Rack Srvr w/2PSU, 2CPU, mem, 4HDD, PCIe, DVD), 2 броя A01-X0111 процесори; 4 x A03-D1TBSATAтвърд диск; 2 x UCS-MR-1X082RX-A памет; RC460-PL001 контролер, резервирано захранване R2X0-PSU2-650W-SB, UCSC-DVD-SFF-C200.	2
2	Комутатор Марка Cisco Systems/ Модел WS-C2960S-24PS-L - (Catalyst 2960S 24 GigE PoE 370W, 4 x SFP LAN Base), 1x GLC-LH-SM=	2
3	Маршрутизатор Марка Cisco Systems/ Модел C2911-VSEC/K9 - (Cisco 2911 UC Sec. Bundle, PVDM3-16, UC and SEC License), VIC2-2BRI-NT/TE, VIC3-4FXS/DID,VWIC2-1MFT-T1/E1, 3xFL-CME-SRST-5, FL-CME-SRST-25, PVDM3-16, PVDM3-16U32	1
4	Компютърни Работни Места Марка HP / Модел Compaq 8200 Elite Microtower Business PC ;	25
5	Монитори Марка HP / Модел LA2405wg 24-inch Widescreen LCD - Monitor 24" Widescreen	25
6	IP Телефони Cisco Systems/ CP-7942G= (Cisco UC Phone 7942)	15
7	Операторски телефонни слушалки Марка Plantronics / Модел Entera HW111	25
8	Мобилни Компютърни работни места Марка HP / Модел ProBook 6560b Notebook PC	10
9	Сървърен шкаф: Марка Rittal / Модел TS8, 42U	1
	Софтуер	
	CCX-85-SRVRS-MEDIA	1
	L-CCX-85-NEW-LIC, 25x L-CCX-85-N-CR-LIC, 25x L-CCX-85-N-P-LIC	1
	CUCM-USR-LIC	1
	CUCM-USR-LIC, 50x LIC-CUCM-USR-A	1
	UNITYCN8-K9, 25x UNITYCN8-USR, 16x UNITYCN8-PORT	1
	VS5-ESSL-BUN-C	1

2.4 Обхват на услугите – дейности и резултати

2.4.1 Услуга тип 1 – Поддръжка на локалната информационна инфраструктура

Услугата се отнася за информационните системи разположени в сградата на МТСП на адрес: София, ул. „Триадица“ № 2 и описани в таблица 1. Услугата включва дейности по

системна администрация, системна и експертна помощ и диагностика на възникнали проблеми и включва обслужване на следните елементи на ИТ инфраструктурата:

- Системен и общ приложен софтуер;
- Специализиран приложен софтуер;
- Бази от данни;
- Хардуер;
- Комуникационно оборудване;

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

Лирекс БГ предлага процесно - ориентиран подход на комплексно обслужване, включително експертна и системна помощ, базиран на стандартите за управление на качеството, сигурността на информацията – ISO 9001, ISO 20000-1, ISO 27001 и добрите ИТ практики.

По отношение на сървърите Лирекс БГ ще осигури следните дейности:

2.4.1.1 Мониторинг на Windows базирани сървъри:

2.4.1.1.1 Дейности по предоставяне на услугата:

- 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.

2.4.1.1.2 Очакван резултат от извършените дейности:

- Непрекъснато наблюдение на състоянието на сървърните операционни системи и вземане на проактивни мерки за нормалната им работа;
- Наблюдение на основни процеси и параметри на сървърни операционни системи, сравняване с еталонни стойности, наблюдение за наличие на тесни места (Bottlenecks) при работата на сървърни операционни системи;

2.4.1.2 Мониторинг на Unix/Linux базирани системи:

2.4.1.2.1 Дейности по предоставяне на услугата:

- 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;

2.4.1.2.2 Очакван резултат от извършените дейности:

- Непрекъснато наблюдение на състоянието на сървърните операционни системи и вземане на проактивни мерки за нормалната им работа;
- Наблюдение на основни процеси и параметри на сървърни операционни системи, сравняване с еталонни стойности, наблюдение за наличие на тесни места (Bottlenecks) при работата на сървърни операционни системи;

2.4.1.3 Наблюдение на системните съобщения за грешки:

2.4.1.3.1 Дейности по предоставяне на услугата

- 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;

2.4.1.3.2 Очакван резултат от извършените дейности:

- Регулярен преглед на системните журнали (SysLog, System Log, Application Log, etc.) за наличие на записи за грешки, предупредителни записи и други обезпокоителни записи;
- Регулярен преглед на системните журнали по сигурността за опити за нерегламентиран достъп;

2.4.1.4 Наблюдение на състоянието на архивите:

2.4.1.4.1 Дейности по предоставяне на услугата

- 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;

2.4.1.4.2 Очакван резултат от извършените дейности

- Наблюдение на статуса на задачите за архивиране;
- Диагностика и отстраняване на проблеми;
- Постигане на възможно най-висока наличност на архивите клоняща към 100%;
- Своевременно отстраняване на всички проблеми с архивните задачи и възстановяване на процеса по архивиране;
- Осъществяване и поддържане на връзка с внедрителите на други услуги и разработчиците на Уеб съдържание за архивиране и възстановяване на данни, услуги и системи.

2.4.1.5 Наблюдение на планираните задачи:

2.4.1.5.1 Дейности по предоставяне на услугата

- Наблюдение на състоянието на Scheduled tasks;
- Наблюдение на състоянието на Crontab jobs;

2.4.1.5.2 Очакван резултат от извършените дейности

- Наблюдение на статуса на планираните задачи;
- Диагностика и отстраняване на възникнали проблеми с планираните задачи;

2.4.1.6 Наблюдение на състоянието на хардуера:

2.4.1.6.1 Дейности по предоставяне на услугата

- 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;

2.4.1.6.2 Очакван резултат от извършените дейности

- Проактивно следене на състоянието на сървърния хардуер и прилагане на превантивни мерки с цел избягване на проблеми с него и минимизиране на времето за отстраняването им;
- Предоставяне на възможно най-голямо количество полезна информация на представителите на оторизираните сервизи за по-бърза реакция от тяхна страна;

2.4.1.7 Администриране на Windows базирани системи:

2.4.1.7.1 Дейности по предоставяне на услугата:

- 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;

2.4.1.7.2 Очакван резултат от извършените дейности:

- Поддръжка на сървърните операционни системи чрез прилагане на добрите практики (Best practices), които са посочени от производителите на операционните системи и в съответствие със стандартите ISO 9001, ISO 20000-1 и ISO 27000, като по този начини се цели непрекъснатата и безаварийна им работа и се спазват гарантираните параметри;
- Непрекъснато наблюдение на състоянието на сървърните операционни системи и вземане на проактивни мерки за нормалната им работа;
- Инсталирани обновления, кръпки по сигурността и сервизни пакети (service packs) на операционните системи;
- Поддръжка на набор от актуални архиви и наличие на процедури за възстановяване на операционните системи от архив, чрез които да се гарантира възстановяването им в случай на срив в рамките на гарантираните параметри.

2.4.1.8 Администриране на Unix/Linux операционни системи:

2.4.1.8.1 Дейности по предоставяне на услугата:

- 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;

2.4.1.8.2 Очакван резултат от извършените дейности

- Поддръжка на сървърните операционни системи чрез прилагане на добрите практики (Best practices), които са посочени от производителите на операционните системи и в съответствие със стандартите ISO 9001, ISO 20000-1 и ISO 27000, като по този начини се цели непрекъснатата и безаварийна им работа и се спазват гарантираните параметри;
- Непрекъснато наблюдение на състоянието на сървърните операционни системи и вземане на проактивни мерки за нормалната им работа;
- Инсталирани обновления, кръпки по сигурността и сервизни пакети (service packs) на операционните системи;
- Поддръжка на набор от актуални архиви и наличие на процедури за възстановяване на операционните системи от архив, чрез които да се гарантира възстановяването им в случай на срив в рамките на гарантираните параметри.

2.4.1.9 Администриране на виртуална инфраструктура:

2.4.1.9.1 Дейности по предоставяне на услугата

- Администриране на виртуалната инфраструктура и всички прилежащи към нея компоненти;
- Администриране на виртуалните машини. Създаване, изтриване и администриране на ресурсите на виртуалните машини;

2.4.1.9.2 Очакван резултат от извършените дейности

- Администриране на услугата по виртуализация на ресурси чрез прилагане на добрите практики (Best practices), които са посочени от производителя на компонентите на услугата и в съответствие със стандартите ISO 9001, ISO 20000-1 и ISO 27000 като по този начини се цели непрекъснатата и безаварийна работа на услугата и се спазват гарантираните параметри;
- Непрекъснато наблюдение на състоянието на услугата и вземане на проактивни мерки за гарантиране на наличността ѝ;
- Консолидиране на системите и услугите за по-оптимално използване на наличните ресурси;
- Повишаване на надеждността и отказоустойчивостта на услугите;
- Администриране на виртуалния хардуер чрез централна конзола ако са налични лицензи;
- Поддръжка на набор от актуални архиви и наличие на процедури за възстановяване на услугата от архив, чрез които да се цели възстановяването на услугата в случай на срив в рамките на гарантираните параметри.

79

2.4.1.10 Администриране на архивите:

2.4.1.10.1 Дейности по предоставяне на услугата

- 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.

2.4.1.10.2 Очакван резултат от извършените дейности

- Разработване и внедряване на процедури за архивиране и възстановяване от архив, които са базирани на добрите практики и в съответствие със стандартите ISO 9001, ISO 20000–1 и ISO 27000, чрез които да се гарантира възстановяването на системи и данни в случай на срив в рамките на гарантираните параметри.
- Поддържане на набор от актуални архиви на конфигурации на сървърни операционни системи, приложения и услуги, прилежащи данни от приложения и услуги, потребителски данни от споделени ресурси и потребителски компютри;
- Постигане на възможно най-висока наличност на архивите клоняща към 100%;
- Своевременно отстраняване на всички проблеми с архивните задачи и възстановяване на процеса по архивиране;
- Осъществяване и поддържане на връзка с внедрителите на други услуги и разработчиците на Уеб съдържание за архивиране и възстановяване на данни, услуги и системи.

2.4.1.11 Администриране на кръпки по сигурността (Security Patches Management):

2.4.1.11.1 Дейности по предоставяне на услугата

- 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;

2.4.1.11.2 Очакван резултат от извършените дейности

- Осигуряване на високо ниво на защитеност на ИТ системите на МТСП;
- Свеждане до минимум на фронтовете за атака на ИТ системите на МТСП от хакери и зловред код.

2.4.1.12 Възстановяване на работоспособността на ОС в случай на срив

2.4.1.13 Възстановяване на работоспособността на СУБД в случай на срив

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

2.4.1.14 Наблюдение на инфраструктурни услуги:

2.4.1.14.1 Дейности по предоставяне на услугата

- 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 2010;

2.4.1.14.2 Очакван резултат от извършените дейности

- Наблюдение на процесите, които са необходими за нормалната работа на услугите;
- Наблюдение на основни процеси и параметри на услугите, сравняване с еталонни стойности, наблюдение за наличие на тесни места (Bottlenecks) при работата на услугите;

2.4.1.15 Администриране на MS Active Directory:

2.4.1.15.1 Дейности по предоставяне на услугата

- 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;

2.4.1.15.2 Очакван резултат от извършените дейности

- Администриране на Active Directory чрез прилагане на добрите практики (Best practices), които са посочени от производителя на компонентите на услугата и в съответствие със стандартите ISO 9001, ISO 20000-1 и ISO 27000, като по този начини се цели непрекъснатата и безаварийна работа на услугата и се спазват гарантираните параметри;
- Непрекъснатост в работата на услугата;
- Автоматизиране на дейностите по администриране на услугата;
- Поддържане в актуално състояние на информацията за потребителски акаунти и групи;
- Изготвяне на специализирани справки за конкретен обект или група обекти (акаунти, групи и други) при поискване от ръководството на Възложителя;
- Непрекъснато наблюдение на състоянието на услугата и вземане на проактивни мерки за гарантиране на наличността ѝ;
- Актуално състояние на служебната информация за всеки потребителски акаунт;
- Поддръжка на набор от актуални архиви и наличие на процедури за възстановяване на услугата от архив, чрез които да се гарантира възстановяването в случай на срив в рамките на гарантираните параметри.

2.4.1.16 Администриране на DNS услугата:

2.4.1.16.1 Дейности по предоставяне на 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;

2.4.1.16.2 Очакван резултат от извършените дейности

- Администриране на DNS услугата чрез прилагане на добрите практики (Best practices), които са посочени от производителя на компонентите на услугата и в съответствие със стандартите ISO 9001, ISO 20000-1 и ISO 27000, като по този начини се цели непрекъснатата и безаварийна работа на услугата и се спазват гарантираните параметри;
- Лесен достъп до споделени ресурси и интернет съдържание чрез познати „приятелски" имена;
- Автоматично идентифициране на предлаганите услуги във вътрешната мрежа чрез записи като Service Point Records и процеси като Outlook Autodiscover;

- Непрекъснато наблюдение на състоянието на услугата и вземане на проактивни мерки за гарантиране на наличността ѝ;
- Поддръжка на набор от актуални архиви и наличие на процедури за възстановяване на услугата от архив, чрез които да се гарантира възстановяването в случай на срив в рамките на гарантираните параметри.

2.4.1.17 Администриране на DHCP услугата:

2.4.1.17.1 Дейности по предоставяне на услугата

- Поддръжка на DHCP сървъри;
- Създаване, конфигуриране и поддръжка на DHCP scopes;
- Управление на записите;
- Архивиране и възстановяване от архив на DHCP услугата;

2.4.1.17.2 Очакван резултат от извършените дейности

- Администриране на DHCP услугата чрез прилагане на добрите практики (Best practices), които са посочени от производителя на компонентите на услугата и в съответствие със стандартите ISO 9001, ISO 20000-1 и ISO 27000, като по този начини се цели непрекъснатата и безаварийна работа на услугата и се спазват гарантираните параметри;
- Непрекъснато наблюдение на състоянието на услугата и вземане на проактивни мерки за гарантиране на наличността ѝ;
- Поддръжка на набор от актуални архиви и наличие на процедури за възстановяване на услугата от архив, чрез които да се гарантира възстановяването в случай на срив в рамките на гарантираните параметри;

2.4.1.18 Администриране на файлови сървъри:

2.4.1.18.1 Дейности по предоставяне на услугата

- Поддръжка на Windows File Sharing файлови сървъри;
- Поддръжка на SAMBA File Sharing файлови сървъри;
- Администриране на структурата на папките със споделени файлове;
- Администриране на правата за достъп до папките със споделени файлове;
- Архивиране и възстановяване от архив на информацията в папките със споделени файлове;

2.4.1.18.2 Очаквани резултати от извършените дейности:

- Администриране на файлови сървъри чрез прилагане на добрите практики (Best practices), които са посочени от производителя на компонентите на услугата и в съответствие със стандартите ISO 9001, ISO 20000-1 и ISO 27000, като по този начини се цели непрекъснатата и безаварийна работа на услугата и се спазват гарантираните параметри;
- Служителите имат достъп единствено до споделените ресурси, които са необходими за извършване на ежедневната им работа като достъпът се контролира чрез конфигурирането на права за достъп до всеки ресурс;
- Контролиране на достъпа до споделените ресурси (сигурност на информацията);
- Непрекъснато наблюдение на състоянието на услугата и вземане на проактивни мерки за гарантиране на наличността ѝ (Наличност на информацията);
- Поддръжка на набор от актуални архиви и наличие на процедури за възстановяване на услугата от архив, чрез които да се гарантира възстановяването в случай на срив в рамките на гарантираните параметри.

По отношение на специализирания приложен софтуер Лирекс БГ ще осигури следните дейности:

2.4.1.19 Инсталиране на специализиран приложен софтуер (на сървърите) при закупуване или подмяна на технически и програмни средства;

2.4.1.20 Обновяване на инсталирания специализиран приложен софтуер;

2.4.1.21 Периодично наблюдение и осигуряване на нормално функциониране на специализираните приложни системи;

2.4.1.22 Администриране на приложен софтуер - поддържане на актуални потребители и други административни функции;

2.4.1.23 Оказване на системна помощ на потребителите на специализираните приложни системи;

2.4.1.24 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 сигурността начин;

2.4.1.25 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;

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.

По отношение на базата от данни Лирекс БГ ще осигури следните дейности:

2.4.1.26 Архивиране на базите данни на МТСП;

2.4.1.27 Администриране на наличните бази от данни по установени еталони и модели;

2.4.1.28 Ежедневно архивиране на статистическите файлове;

2.4.1.29 Промяна на системни настройки - след съгласуване с Възложителя;

2.4.1.30 Отстраняване на възникнали проблеми, като в случай на необходимост действията се съгласуват с външни организации;

По отношение на поддръжката на потребителски компютри в ИТ инфраструктурата на МТСП Лирекс БГ ще подсигури:

2.4.1.31 Поддръжка на потребителски компютри

2.4.1.31.1 Дейности по предоставяне на услугата

- 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.

2.4.1.31.2 Очаквани резултати от извършените дейности

- Поддръжка на персоналните компютри на служителите чрез прилагане на добрите практики (Best practices), които са посочени от производителите на хардуера и софтуера и в съответствие със стандартите ISO 9001, ISO 20000-1 и ISO 27000, като по този начини се цели безпроблемната им работа и спазването на гарантираните параметри;
- Постигане на висока удовлетвореност на служителите МТСП чрез съдействие при възникване на въпроси относно или срещане на проблеми при работа с персоналните им компютри.

По отношение на сигурността на информацията Лирекс БГ ще осигури:

2.4.1.32 Прилагане на Политиката и процедурите за сигурност на информационните системи на МТСП;

2.4.1.33 Непрекъснат контрол и 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;

2.4.1.34 Вписване на инцидентите в „Регистър на събития и инциденти свързани с информационната сигурност", съгласно вътрешните правила за информационна сигурност в МТСП.

2.4.1.35 Лирекс БГ ще осигури поддържане на комуникационно оборудване със следните функции:

2.4.1.35.1 Дейности по поддръжка:

- 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;
- Наблюдение и анализ на функционирането на комуникационното оборудване. Измерване и анализ на параметрите на трафика и предложения за оптимизации на комуникационното оборудване;
- 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.

2.4.1.35.2 Очакван резултат от извършените дейности:

- Поддръжка на мрежовото оборудване чрез прилагане на добрите практики (Best practices), които са посочени от производителите на мрежово оборудване и в съответствие със стандартите ISO 9001, ISO 20000-1 и ISO 27000, като по този начини се цели непрекъснатата и безаварийна работа и се спазват гарантираните параметри;
- Непрекъснато наблюдение на състоянието на мрежовото оборудване и вземане на проактивни мерки за нормалната му работа;
- Проактивно следене на състоянието на мрежовото оборудване и прилагане на превантивни мерки с цел избягване на проблеми с него и минимизиране на времето за отстраняването им;
- Предоставяне на възможно най-голямо количество полезна информация на представителите на оторизираните сервизи за по-бърза реакция от тяхна страна.

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

- Всички връзки с външни доставчици на интернет свързаност.

2.4.1.37 За периода на договора Лирекс БГ ще поддържа в актуално състояние следните регистри в електронен вид и ще предоставя достъп до тях на директора на дирекция ПАОЧР или упълномощен от него служител:

- 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

84

компютри, мобилни устройства, мрежови принтери, многофункционални устройства и други;
- Регистър на адресите – съдържа политиката за раздаване на IPv4 адреси и адресната схема, използвана в МТСП;
- Регистър на Услугите – услуги използвани от клиенти, в това число инфраструктурни (DNS, DHCP);
- 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;
- 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;

2.4.1.38 Лирекс БГ ще представя на Възложителя **месечен отчет** за извършените дейности, който съдържа минимум 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.

Еднократни дейности свързани с предоставяне на услугите

2.4.1.39 Лирекс БГ ще извърши следните еднократни дейности свързани с предоставяне на услугите
- първоначална профилактика на сървърната, сторидж и виртуална инфраструктура базирана на преглед на системни логове с цел установяване на текущото състояние на информационната инфраструктура на МТСП;
- анализ на състоянието и нуждите от архивиране на сървърните приложения и изготвяне на схема за архивиране;
- разписване на процедура за създаване на годишен архив и еднократно архивиране на информацията от всички информационни системи в МТСП на външен носител, който да предостави на Възложителя за съхранение извън сървърните помещения; анализ на състоянието и представяне на препоръки за оптимизация на информационната инфраструктура на МТСП;
- анализ на състоянието на информационната сигурност в ИТ инфраструктурата на МТСП и предоставяне на доклад на ВЪЗЛОЖИТЕЛЯ с препоръки за подобряването и. Следва да се извърши от специалист със съответната квалификация;
- анализ на входящия и изходящия интернет трафика в МТСП и предоставяне на доклад включващ информация за количеството на нелегитимния трафик. Изпълнителят следва да предостави необходимите инструменти за извършване на анализа.

2.4.2 Параметри на услуга тип 1

	Параметър	Тип изискване	Описание / Изискване	Предложение на Лирекс БГ
	Обслужване и достъпност на каналите за заявяване на поддръжка (24 часа в денонощието, 7 дни в седмицата, 365 дни в годината)	Точно	Задължително	Лирекс БГ ще осигури обслужване и достъпност на каналите за заявяване на поддръжка (24 часа в денонощието, 7 дни в седмицата, 365 дни в годината)

	Параметър	Тип изискване	Описание / Изискване	Предложение на Лирекс БГ
	Време за реакция при критичен инцидент, застрашаващ работата на цялата система в рамките на работното време на Възложителя	Максимум	да се предложи от участника	**30 минути**
	Време за реакция при инцидент, застрашаващ работата на сегмент/част от системата в рамките на работното време на Възложителя	Максимум	2 часа	2 часа
	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
	Време за отстраняване на критичен инцидент, застрашаващ работата на цялата система в рамките на работното време на Възложителя	Максимум	4 часа	4 часа
	Време за отстраняване на инцидент, застрашаващ работата на сегмент от системата в рамките на работното време на Възложителя	Максимум	12 часа	12 часа
	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
	Осигуряване на минимум двама души, които ежедневно в рамките на работното време на Възложителя от 08:00 до 19:00 да се ангажират на място с поддръжка.	Точно	Задължително	Лирекс БГ ще осигури минимум двама души, които ежедневно в рамките на работното време на Възложителя от 08:00 до 19:00 да се ангажират на място с поддръжка.
	Възможност за приемане на заявки за поддръжка по телефон или други гласови канали	Точно	Задължително	Лирекс БГ ще осигури възможност за приемане на заявки за поддръжка по телефон или други гласови канали (тел. 02 488 06 66, GSM 0885 991 378)
	Възможност за приемане на заявки за поддръжка по e-mail.	Точно	Задължително	Лирекс БГ ще осигури приемането на заявки за поддръжка по e-mail (lirexss@lirex.com)
	Възможност за нотификация по e-mail при развитие на всеки „инцидент"	Точно	Задължително	Лирекс БГ ще осигури възможност за нотификация по e-mail при развитие на всеки „инцидент"
	Отчетност и статистика за постигнатите параметри на поддръжка (времена за реакция, времена за затваряне на „инцидента" и пр.)	Точно	Задължително	Лирекс БГ ще осигури отчетност и статистика за постигнатите параметри на поддръжка (времена за реакция, времена за затваряне на „инцидента" и пр.)
	Поддръжка на база данни с параметрите и серийните номера на оборудването и софтуера предмет	Точно	Задължително	Лирекс БГ ще осигури поддръжка на база данни с параметрите и серийните

	Параметър	Тип изискване	Описание / Изискване	Предложение на Лирекс БГ
	на поддръжка.			номера на оборудването и софтуера предмет на поддръжка
	Изисквания към извършването на еднократни дейности			
	Дейностите по тази точка трябва да бъдат завършени до 2 месеца след подписване на договора за изпълнение на услугата (удостоверява се с двустранен протокол)	Точно	Задължително	Лирекс БГ ще извърши еднократните дейности до 2 месеца след подписване на договора за изпълнение на услугата

2.4.3 Допълнителни услуги невключени в обхвата на услуга тип 1

Лирекс БГ ще приема от Възложителя за изпълнение дейности/допълнителни услуги по поддръжка на информационната инфраструктура на МТСП, неописани в точка 2.4.1, в това число и дейности извън работното време на Възложителя. Тези дейности се заплащат допълнително, извън стойността на поръчката, на база действително вложени ресурси от Изпълнителя и по ценови ставки, посочени в Ценовото предложение.

2.4.4 Услуга тип 2 - Поддръжка на единен център за предоставяне на информация на граждани (система Кол Център)

2.4.4.1 Обхват на услугата

Услуга се отнася за единния център за предоставяне на информация в сградата на МТСП на адрес: София, ул. „Триадица“ № 2 и описан в таблица 2 по-горе. Услугата включва дейности по:

- техническа поддръжка на хардуер и софтуер на единен център за предоставяне на информация на граждани,
- привеждане на устройствата в състояние на работоспособност, както и подмяна при необходимост на дефектирали елементи.
- оказване на техническа помощ и консултации;
- конфигуриране и настройка на оборудването при необходимост.

2.4.5 Параметри на услуга тип 2

2.4.5.1 Дейности по предоставяне на услугата

За периода на договора при възникване на проблем Лирекс БГ ще осигури:

- 12 (дванадесет) часа / 7 (седем) дни телефонна поддръжка;
- първоначална реакция в рамките на 2 часа в рамките на работното време на Възложителя (с изключение на официални празници и почивни дни);
- отстраняване на проблем до 2 работни дни в рамките на работното време на Възложителя (с изключение на официални празници и почивни дни);
- Отчетност и статистика за постигнатите параметри на поддръжка (времена за реакция, времена за отстраняване на „инцидента”);
- Поддръжка на база данни с параметрите и серийните номера на оборудването и софтуера предмет на поддръжка.

В случай на невъзможност за ремонтиране на повредена част или единица от оборудването в рамките на времето за отстраняване на проблем, Лирекс БГ ще предостави временно - оборотно оборудване за срока на ремонта, гарантирайки същата функционалност като тази на оборудването, което се ремонтира.

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

2.4.5.2 Очаквани резултати от извършените дейности

- Изпълнение на дейностите по предоставяне на услуга тип 2 чрез прилагане на добрите практики (Best practices), които са посочени от производителите на поддържаното оборудване и системи и в съответствие със стандартите ISO

9001, ISO 20000-1 и ISO 27000, като по този начини се цели непрекъснатата и безаварийна работа и се спазват гарантираните параметри;
- Постигане на възможно най-висока наличност на услугата чрез прилагане на проактивни мерки за предотвратяване възникването на инциденти;
- Бърза реакция при възникване на инцидент / проблем с работата на услугата;
- Ангажиране на екип от високо квалифицирани специалисти, които да работят по отстраняване на възникнали инцидент/проблеми за минимизиране на времето, през което услугата не е налична;
- Документиране на извършените дейности в Web базирана система, до която е предоставен достъп на Изпълнителя.

Дата: 25.11.2016 г.

Подпис и печат: _____
Димитринка Илиева
(име и фамилия)
Управител
(длъжност на представляващия участника)

Изготвил: А. Георгиев, В. Митева
Съгласувал: Б. Янчев, С.Джурелов

История на редакциите					
№ редакция	*описание на промяната*	*автор*	*проверил*	*утвърдил*	*дата въвеждане*
1	Начална редакция	Б.Янчев	Б.Йорданов	Д.Илиева	12.02.2009
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

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"

1 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.

2 Приложимост

Процедурата се прилага от всички служители в съответствие с изпълнение на изискванията на ISO 27001:2013 за управление на непрекъсваемостта на бизнес процесите.

3 Термини и съкращения

ИС	Информационни Системи
DRC	Виж Disaster Recovery Center
Disaster Recovery Center	Център за възстановяване след аварии
Recovery Time	Времето, необходимо за да се възстанови достъпността

Objective (RTO)	на дадена услуга след съществено прекъсване (бедствие или авария)
Recovery Point Objective (RPO)	Момент във времето, към който ще бъдат възстановени данните в системата
ВМ	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.
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, Лирекс Нет, 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.

4 Блок – схеми

Не се прилагат блок схеми.

5 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

6 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

7 Възможни аварии със сериозни негативни последици 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)
- 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.

8 Комуникации

За коректната комуникация в случай на бедствия и аварии са необходими надеждни комуникации. Наличните комуникационни канали са:

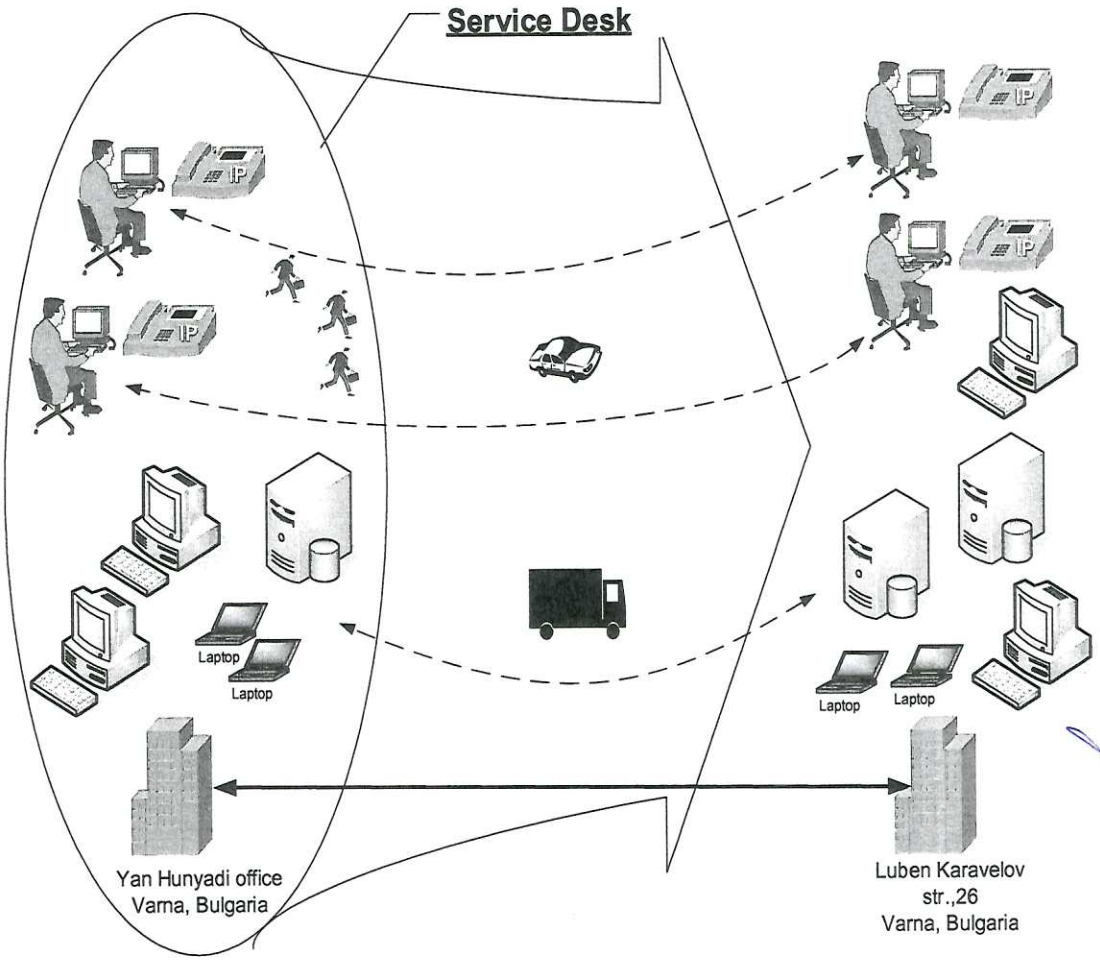
- IP телефони използваща
  - Стандартни гласови канали през БТК
  - IP свързаност
  - VoIP трънкове
  - Оптична свързаност с ТТК
  - Интернет свързаност и използване на Cisco IP Communicator
- Мобилни телефони
  - GSM апарати
  - Мобилни gateway
- Електронна поща
- Комуникатори тип messenger
  - Skype
  - ICQ

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

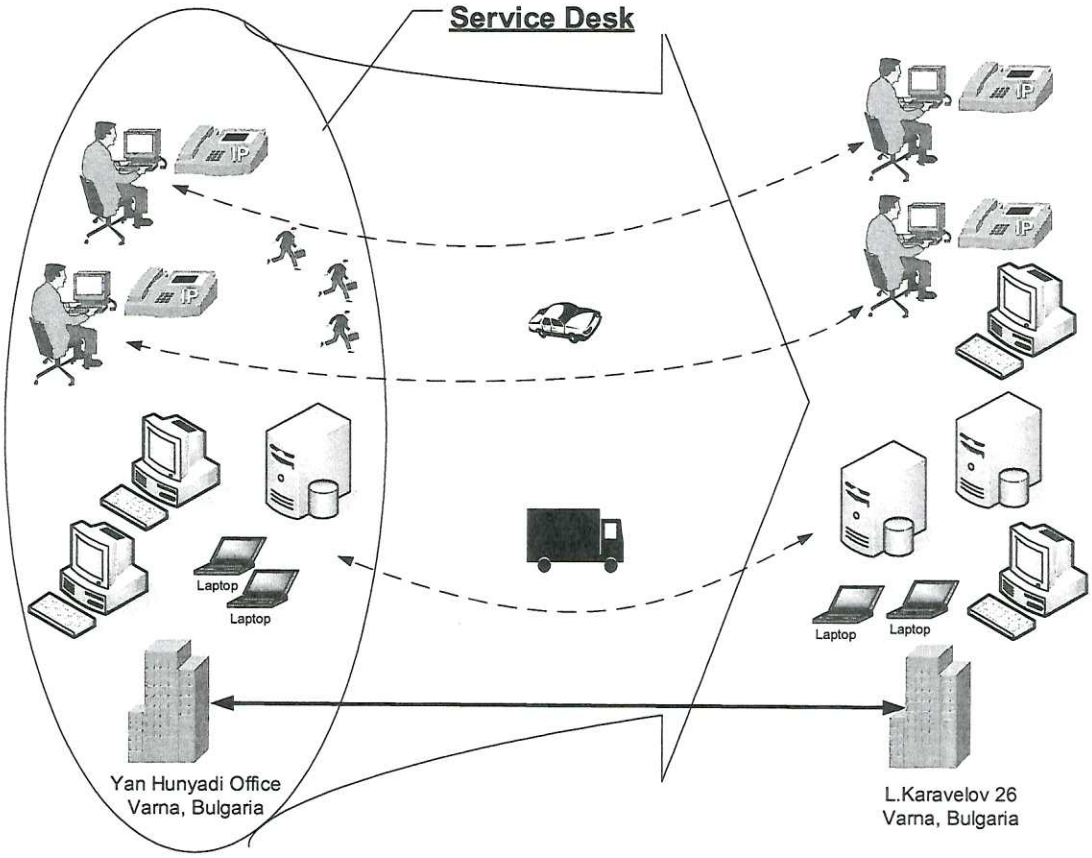
9 Планирана схема за реалокация на ресурси

9.1.1 Реалокация на екип по поддръжка на инфраструктурата



10 Непрекъснатост на Външни ИТ услуги

10.1 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

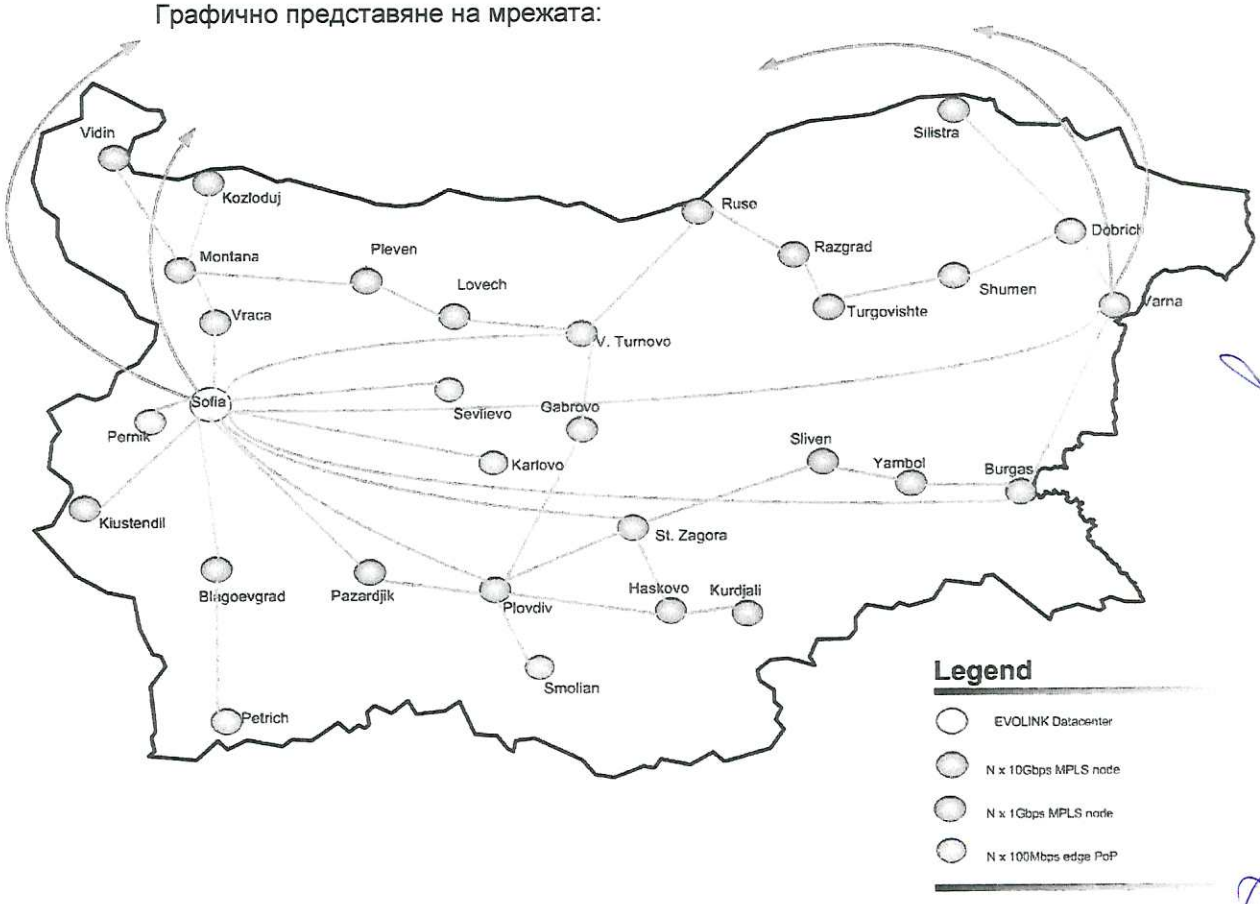
10.2 Сервизни услуги

Схемата за непрекъсваемост на сервизните услуги следва таблицата:

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

10.3 Интернет услуги

Графично представяне на мрежата:



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.

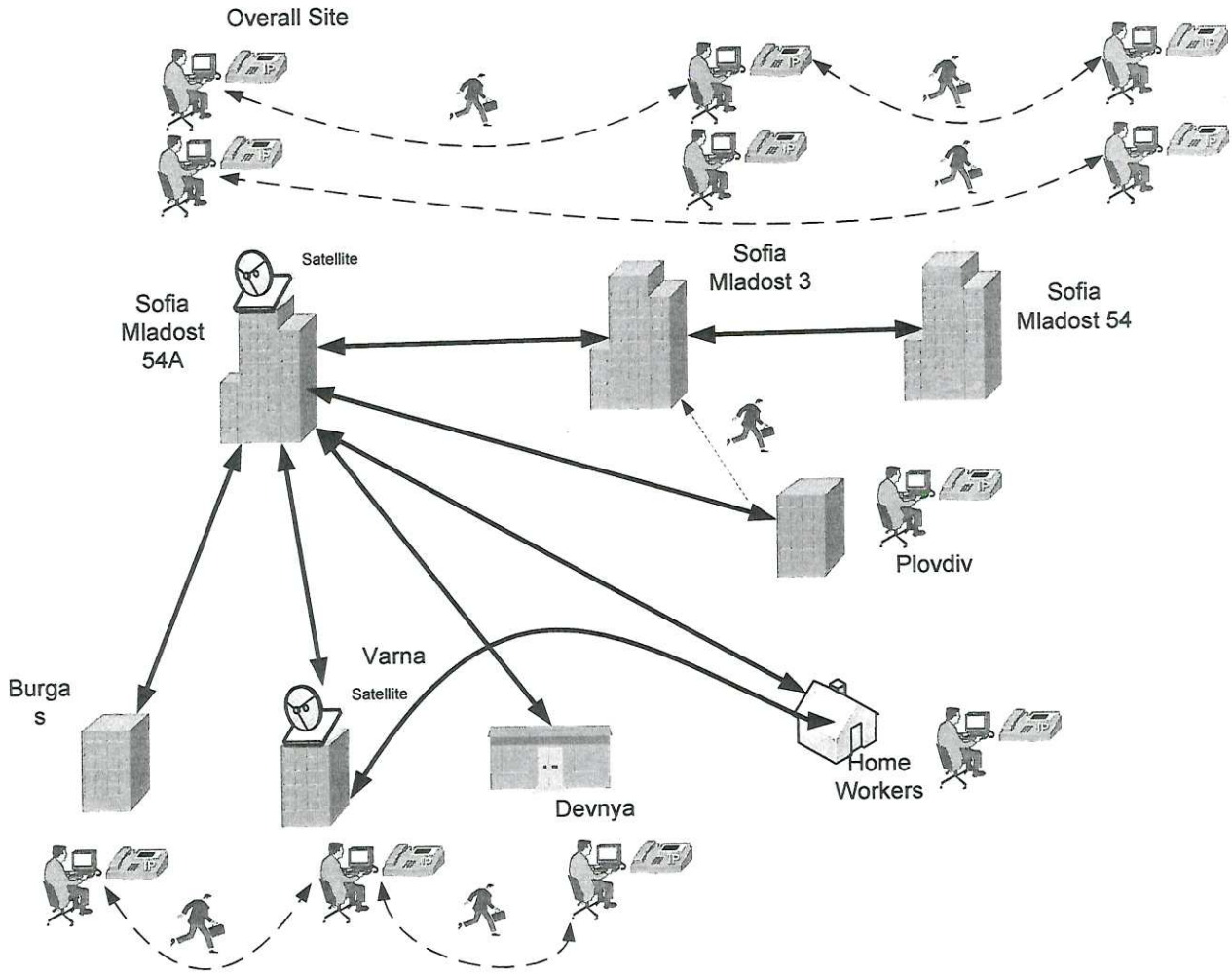
Чрез всяка от международните връзки може да се осигурява Интернет капацитет до всяка точка от мрежата на Лирекс нет.

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.

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, Множество MAN връзки	BGS2 – хл. България	UPS	Директна оптична връзка до BGS1, MAN връзки

Схема за реалокация на персонала



11 Възстановяване след сривове и аварии

11.1 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

11.2 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

11.3 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

12 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.

13 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

14 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.

15 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 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

16 Форми и бланки

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 БГ
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

Образец № 7.1

СПИСЪК

Долуподписаният /-ната/ Димитринка Иванова Илиева, с ЕГН 5912027611, в качеството ми на Управител *(посочете длъжността)* на «Лирекс БГ» ООД *(посочете наименованието на участника),* ЕИК/БУЛСТАТ 121057952 – участник в процедура за възлагане на обществена поръчка с *„ПОДДРЪЖКА НА ИНФОРМАЦИОННА ИНФРАСТРУКТУРА НА МТСП”*, заявяваме, че разполагаме с експертен екип за изпълнение на предмета на настоящата обществена поръчка, както следва:

№	Три имена на експерта	Образование / Квалификация	Професионален опит	Позиция в екипа за изпълнение
1	Петър Ганчев Ганчев	Технически университет – София, Магистър -Инженер компютърни системи, сериен № ТУ – А- 99 000693, Рег.№ 75005/07.12.99 **Сертификати**: Документ за членство в Project Management Institute (PMI) Project Manager Professional (PMP) PMP номер: 1815926 Дата на издаване:15.05.2015г. Дата на валидност: 14.05.2018г	Служител на Лирекс от 2004 г., заемал последователно длъжностите: Експерт по управление на проекти, Старши експерт по управление на проекти, Ръководител направление „Реализация на проекти”, Директор управление на проекти. Притежава над 10 г. професионален опит в областта на ръководенето на ИТ проекти. Притежава над 18 г. опит в областта на ИТ. Участва в следните проекти: - юли 2004 – септември 2011, Ръководител програма *Проектиране, изграждане и поддържане на системи за фиксирана телефония и VoIP сървърни решения*, Мобилтел АД - април 2005 – септември 2010, Ръководител програма Проектиране, изграждане и поддържане на системи за фиксирана телефония и VoIP сървърни решения, Транс телеком - октомври 2005 – януари 2006, Ръководител проект Надграждане на съществуваща VoIP система, Булгаргаз ЕАД	Ръководител на проекта

Бургас 056/ 811 902; Варна 052/ 681 881; Габрово 066/ 801 166; Пловдив 032/ 560 222;
Русе 082/ 877 092; Севлиево 0675/ 3 54 90; Стара Загора 042/ 621 114; Девня 0519/ 9 59 59; Козлодуй 0973/ 80 407, Скопие, Македония +389 (2) 322 4157

№	Три имена на експерта	Образование / Квалификация	Професионален опит	Позиция в екипа за изпълнение
			- октомври 2005 – януари 2006, Ръководител проект Надграждане на съществуваща VoIP система, Булгаргаз ЕАД - февруари 2006 – юни 2006, Ръководител проект Проектиране и изграждане на система за core VoIP, core WAN и WLAN, Хотел Кемпински Зографски - май 2006 – септември 2006, Ръководител проект Проектиране, конфигуриране и инсталиране на VoIP and fixed telephony voice recording , Булгаргаз ЕАД - януари 2007 – юни 2009, Ръководител програма Национална IP/MPLS мрежа с DWDM разширение, ДАИТС - март 2007 – септември 2007, Ръководител проект Изграждане на национална SDH мрежа, ДАИТС - септември 2010 – септември 2011, Ръководител проект Обновяване, настройка и препоръки за развитие на мрежата на агенция IDDEEA, Делегацията на ЕК в Босна и Херцеговина - юни - 2012 – ноември 2015, Ръководител проект Доставка на хардуер, софтуер и адаптирането им за нуждите за единен център за предоставяне на информация (кол-център), Министерство на труда и социалната политика	

№	Три имена на експерта	Образование / Квалификация	Професионален опит	Позиция в екипа за изпълнение
2	Станислав Иванов Мановски	Технически университет – Габрово Магистър Електроинженер, Специалност „Изчислителна техника", сериен № А9 000111, рег. № Е 1245 **Сертификати:** Microsoft Certified Systems Engineer Сертификационен № B395-3952 Дата на издаване: 31.08.2004 Сертификационна версия: Messaging on Windows Server 2003 Microsoft Certified Systems Engineer Сертификационен № B395-3946 Дата на издаване: 05.04.2004 Сертификационна версия: Windows Server 2003 Microsoft Certified Database Administrator Сертификационен № B395-3935 Дата на издаване: 15.12.2000 Сертификационна версия: Microsoft SQL Server 2000 CCIE Certification - Collaboration сертификационен № CSCO10277978, дата на издаване: 24.04.2006г. Дата на валидност: 24.04.2018 г.	Служител на Лирекс от 1998 г. Към момента заема длъжността Ръководител отдел R&D. Притежава над 15 години професионален опит в областта на анализ, проектиране, разработване, внедряване, поддръжка и на комплексни хетерогенни ИТ системи, комуникационни решения, системи за сигурност, приложни програмни продукти и др. Участва във реализираните от дружеството проекти в областта на ИК технологии, сред които: - Април 2010 Експерт предоставяне на ИТ услуги а Балкантекс, България, Проектиране и внедряване на корпоративни ИТ стандарти; *Изграждане на комплексна, хетерогенна, виртуална инфраструктура, системи за управление на комуникацията и решение за архивиране* - Юни 2012 – Септември 2012 Експерт предоставяне на ИТ услуги, Министерство на труда и социалната политика, Доставка на хардуер, софтуер и адаптирането им за нуждите за единен център за предоставяне на информация (кол-център) - Януари 2013 – Април 2013 Експерт предоставяне на ИТ услуги, Изграждане на IP телефонната система на Булгартранзгаз с капацитет над 600 IP телефона и над 1000 софтуерни клиенти за настолни/мобилни персонални компютри с функции IM/Presence и управление на настолни IP телефони; - 01.2008, Системен архитект, МВР, Система за видео-наблюдение и контрол – градска среда – София, интегрирана WEB базирана система за управление и контрол	Експерт Системна интеграция – 1бр.

№	Три имена на експерта	Образование / Квалификация	Професионален опит	Позиция в екипа за изпълнение
			- 12.2008, Системен архитект ДАИТС, Национална комуникационна система на образованието – изграждане, инсталация, поддръжка и мониторинг - 01.2009, Системен архитект, Държавен Фонд Земеделие, Изграждане на система за IP базирана телефония - 01.2009, Системен архитект Министерство на Финансите, IT Communication Infrastructure System - 2009, Системен архитект АЕЦ Козлодуй – IP базирана система за оповестяване при бедствия и аварии на площадката на АЕЦ и 12 км зона, интегрирана система за управление, мониторинг и контрол. - 2009, Системен архитект, Печатница на БНБ – Внедряване на система за управление на бизнеса - 2011, Системен архитект, Столична община – изграждане на система за наблюдение на общински площи – паркове, градинки и подлези - 2011, Системен архитект, Градско строителство Дупница – изграждане на система за видео-наблюдение в градска среда - 2011, Системен архитект, АЕЦ Козлодуй – проектиране на ИТ базирани технически системи за сигурност	
3	Светослав Иванов Манев	Технически университет – Габрово, Специалност: Системи и управление, сериен №ВД -96 0013851, рег. № E96175/12.07.96 **Сертификати:** Microsoft Certified Solutions Expert Сертификационен № E735 -4636 Дата на издаване: 25.02.2014	Служител на Лирекс от 2000 г. Притежава над 10 г. опит в проектирането , интегрирането и поддръжката на комплексни хетерогенни ИТ системи и инфраструктура в държавната администрация и корпоративния сектор. Участва във реализираните от дружеството проекти в областта на ИК технологии сред които: - Октомври 2011- Ноември 2011, Ключов експерт , "Провеждане одит на услугите	Експерт Предоставяне на ИТ услуги

№	Три имена на експерта	Образование / Квалификация	Професионален опит	Позиция в екипа за изпълнение
		Сертификационна версия: Server Infrastructure Microsoft Certified Solutions Associate Сертификационен № E184 – 6937 Дата на издаване: 28.02.2013 Сертификационна версия: Windows Server 2012 (MCSA) Charter Member Microsoft Certified IT Professional Сертификационен № A562-8201 Дата на издаване: 08.10.2010 Сертификационна версия: Enterprise Administrator or Windows Server 2008 Microsoft Certified Systems Administrator Сертификационен № A562 -8186 Дата на издаване: 02.02.2007 Сертификационна версия: Messaging on Windows Server 2003 Microsoft Certified Professional Сертификационен № E184-6938 Дата на издаване: 28.02.2013 Сертификационна версия: Microsoft Certified Professional Microsoft Certified Systems Engineer Сертификационен № A562-8182 Дата на издаване: 28.05.2004 Сертификационна версия: Windows Server 2003	и мрежовата инфраструктура на АЕЦ Козлодуй, предоставени от отдел "ИС и КТ" ", АЕЦ Козлодуй ЕАД Проектът включва преглед на мрежова и сървърна инфраструктура , анализ на защитеността и отказоустойчивостта на инфраструктурата, препоръки за подобрения както и методи за администриране и управление на информационната инфраструктура - Декември 2011- Февруари 2012, Архитект , "Разработване на решение ,тестване и внедряване на система за мониторинг на компютърни системи за Glob@l Libraries Bulgaria" – проект на UNPD (United Nations Development Programme) Разработване на техническото предложение за участие в търг и в последствие за реализацията му. - Февруари 2012 – Март 2012, Инсталиране и конфигуриране на виртуална инфраструктура базирана на VMware vSphere 5.0 , за нуждите на сървърна консолидация и виртуализация в Солвей – Девня - Юни 2012 – Декември 2013, ИТ Консултант , в проект включващ дизайн и внедряване на виртуална инфраструктура на VMware vSphere5 (вкл. конфигуриране на DRS и HA клъстер) за консолидиране на физическа и виртуална сървърна инфраструктура в регионите на Северна Америка (NAFTA) от инфраструктурата на Solvay S.A., Belgium	

№	Три имена на експерта	Образование / Квалификация	Професионален опит	Позиция в екипа за изпълнение
		Преминати изпити: - 414 Implementing an Advanced Server Infrastructure/ 25.02.2014 - 284 Implementing and Managing Microsoft Exchange Server 2003/ 02.02.2007 - 292 Managing and Maintaining a Microsoft Windows Server 2003 Environment for an MCSA Certified on Windows 2000/ 30.04.2004 - 068 Implementing and supporting NT 4.0 in the Enterprise/31.01.2001 - 073 Implementing and supporting NT 4.0 Workstation/ 19.01.2001 - 067 Implementing and supporting NT Server 4.0/07.12.2000	- Септември 2012- Април 2013 ИТ Консултант , в проект включващ „Изграждането на IP телефония, контактен център и интегриране на телефонни услуги с информационните системи на Разплащателна Агенция , предназначена за по –добро изпълнение на мерките по ПРСР" (European Project), Държавен Фонд „Земеделие" , София - Септември 2012- Ноември 2013 ИТ Консултант , в проект WICP на SIS отдела в Solvay S.A., Belgium Проектът включва фазата на сливането и преструктурирането на Активна Директория на Solvay, така че да се отрази придобиването на компанията Rhodia. Това включва процеса на трансформиране на двете AD forest-и на двете компании в една нова Solvay S.A., Belgium - Септември 2013- - Октомври 2013 ИТ Консултант , в проект Интеграция на система за е-обучение на базата на Moodle в Министерство на Правосъдието , EuropeAid/133148/C/SUP/BA Lot 5, Босна и Херцеговина - Октомври 2013- Ноември 2013Ключов експерт , "Модернизиране и интеграция на (НСРПО) и на системите за предупреждение и оповестяване на АЕЦ Козлодуй на (ЗНЗМ), както и изграждане на единна РК система за спасителни дейности с цел поддържане на взаимодействието между	

№	Три имена на експерта	Образование / Квалификация	Професионален опит	Позиция в екипа за изпълнение
			МВР,МИЕТ,МЗ,АЕЦ,АЯР и БЕХ ", АЕЦ Козлодуй ЕАД, София, България - Май 2014 – Юни 2014 ИТ Консултант , в проект включващ дизайн, план и мигриране на виртуална инфраструктура на VMware vSphere4.0 към vSphere5.5 (вкл. конфигуриране на DRS и HA клъстер) за сайт NOH от инфраструктурата на Солвей в Брюксел Solvay S.A., Belgium - Юли 2014-Август 2014 ИТ Консултант, в проект "Проучване и анализ на ИТ инфраструктурата и услугите в ЕНЕРГО-ПРО Варна ЕООД и препоръки за оптимизирането им ", ЕНЕРГО-ПРО , ВАРНА, България - Януари 2015-Февруари 2015 ИТ Консултант, в проект – „Дизайн на отказоустойчива виртуална инфраструктура на базата на VMware vSphere 5.5 за Щрак ООД Щрак ООД, Варна - Март 2015-Март 2015 ИТ Консултант, в проект – „Одит и анализ на физическата ИТ инфраструктура на община Оряхово във връзка с новия проект за дигитални архиви „Община Оряхово, гр. Оряхово - Май 2015-Юни 2015 ИТ Консултант, в проект – „Одит на състоянието на системите и връзките в Община Стара Загора и нейните изнесени центрове „Община Стара Загора, гр. Стара Загора - Септември 2015-Октомври 2015 ИТ	

№	Три имена на експерта	Образование / Квалификация	Професионален опит	Позиция в екипа за изпълнение
			Консултант, в проект – „ Одит на мрежовата инфраструктура и информационни технологии на „Система за контрол на достъпа" и „Телевизионна система за наблюдение и контрол" „ Отдел „Сигурност", АЕЦ Козлодуй ЕАД, София, България	
4	Петър Василев Петров	Технически Университет София, Магистър, Специалност: Топлинна и хладилна техника и технологии, сериен № ТУ – СФ – 2000, рег. № 76806 **Сертификати:** Cisco Certified Network Professional Security Сертификационен номер: CSCO 11463328 Дата на издаване: 20.09.2011 Дата на валидност: 23.05.2017 Cisco Certified Network Associate Routing and Switching Сертификационен номер: CSCO 11463328 Дата на издаване: 20.11.2008г. Дата на валидност: 23.05.2017г. CCIE Certification Routing & Switching Сертификационен номер: CSCO 11463328 Дата на издаване: 09.02.2015г. Дата на валидност: 09.02.2017 г.	Служител на Лирекс от 2010 г. Към момента заема длъжността Мрежови инженер. Като такъв притежава над 6 г. опит в конфигуриране, мониторинг и поддръжка на мрежово оборудване и инфраструктура. Участва като мрежови инженер в следните проекти, реализирани от дружеството: - 01.2010-11.2010 Експерт поддръжка на мрежи Министерство на външните работи. Изграждане на непрекъсната, високоскоростна, дублирана и защитена комуникационна връзка между Национален визов център – МВнР, Резервен визов център – Бояна, Основния компютърно – комуникационен център и Резервния център на МВР, съгласно изискванията към Националния компонент за връзка с визовата информационна система на ЕС и мрежата за консултиране на визи VISION. - 07.2012 – 01.2013 Експерт поддръжка на мрежи, ДФ Земеделие. Доставка, инсталация и конфигурация на комуникационно оборудване Изграждане на безжична мрежа с криптирана комуникация между АП-та и контролера. Осигуряване на комуникация на VoIP устройствате през безжичната мрежа. Осигуряване на CCKM автенетикация през Cisco ACS Server за VoIP клиентите.	Експерт Поддръжка на мрежи

№	Три имена на експерта	Образование / Квалификация	Професионален опит	Позиция в екипа за изпълнение
			- 04.2013, Експерт поддръжка на мрежи, SG Express Bank, Доставка, инсталация и конфигурация на комуникационно оборудване. Изграждане на безжична мрежа с криптирана комуникация между АП-та и контролера. - 09.2013 – 11.2013, АДРА България, Мрежови инженер, Доставка, инсталация и конфигурация на комуникационно оборудване. Изграждане на LAN мрежата на клиента. Изграждане на VPN Crypto тунели между отделните офиси на клиента. Осигуряване на Remote Access VPN достъп за клиентите. - 01.2012 – 07.2013, МТСП Мрежови инженер, Поддръжка, инсталация и конфигурация на комуникационно оборудване - 10.2012 – 11.2012, АББ България, Мрежови инженер, Доставка, инсталация и конфигурация на комуникационно оборудване. Изграждане на безжична мрежа с криптирана комуникация между АП-та и контролера. - 09.2012 – 10.2012, Фаизер България, Мрежови инженер Доставка, инсталация и конфигурация на комуникационно оборудване - 01.2012г – до момента, Kaufland България Мрежови инженер Поддръжка, инсталация и конфигурация на комуникационно оборудване - 01.2011г – до момента, МОМН, Мрежови инженер Поддръжка, инсталация и конфигурация на комуникационно оборудване - 10.2010г. – до момента, Лев Инс, Мрежови инженер Поддръжка,	

111

№	Три имена на експерта	Образование / Квалификация	Професионален опит	Позиция в екипа за изпълнение
			инсталация и конфигурация на комуникационно оборудване	
5	Здравко Георгиев Ножаров	Технически университет, гр.София Магистър инженер – Комуникационни Технологии Специалност: Телекомуникации, сериен № А09 035347, рег. № 12601-88/ 12.06.09 **Сертификати:** CCNP Voice Сертификационен номер: CSCO 12339046 Дата на издаване: 28.01.2015 Дата на валидност: 28.01.2018	Служител на Лирекс от 2013 г. Към момента заема длъжността Инженер гласови комуникации. Притежава над 3 г. опит в конфигуриране , инсталиране и поддръжка на решения за IP телефония, вкл. Cisco Call Manager, Участва като такъв в следните проекти, реализирани от дружеството: - 2013 цялостна инсталация, конфигурация и поддръжка на телефонна централа Cisco Call Manager 9.1 Business Edition за ЛЕМ България - 2013 инсталация, конфигурация и поддръжка на софтуер за запис на обаждания Zoom Call Recording за Булгартрансгаз - 2013, АЕЦ Козлодуй – Внедряване и поддръжка на ASP.NET Web базирана система за мониторинг на IP телефония - 2013 Държавна агенция "Национална сигурност", Внедряване и поддръжка на билинг система за IP базираната им телефонна централа	Експерт Поддръжка на софтуерни телефонни централи
6	Денислав Маринов Братоев	Технически Университет - Варна Магистър по информатика; Компютърна техника и технологии, Сериен № ТУВ – 99 079424, рег. № 23314/ 24.11.99 **Сертификати:** Удостоверение вътрешен одитор по ISO 9001 и ISO 27001 , удостоверение № 7007 Дата на издаване: 02.02.2009 Издаден от: Алфа Куолити Сертификат за одитор по ISO 27001:2015 №106681	Служител на Лирекс от 2001 г. до настоящия момент, към момента заема длъжността Регионален координатор, Варна и Ръководител обособено звено Аутсорсинг. Притежава над 15 г. опит в областта на информационните технологии. Участва в следните проекти като ключов експерт Одитор по качество: - 2003 – текущ Оперативен ръководител, Ст. одитор по качество на продукта (вкл. на разработката и внедряването) „Изграждане и поддръжка на система за отчитане на товари – автоматичен и ръчен авто кантар", Солвей Соди АД, Девня, България; Системата е в	Експерт Ръководител по качеството

№	Три имена на експерта	Образование / Квалификация	Професионален опит	Позиция в екипа за изпълнение
		Дата на издаване: 29 ноември 2013 г. Издаден от: Intertek Сертификат по ITIL Foundation Certificate in IT Service Management Сертификационен номер: GR750134382DB Дата на издаване: 20.11.2014 Сертификат за моделиране на бизнес процеси Дата на издаване: 09.10.2008 Издаден от: Тен Степ Инк., Проджекта	поддръжка до настоящия момент. - 2004 – текущ Оперативен ръководител, Ст. одитор по качество на продукта (вкл. на разработката и внедряването) „Изграждане и поддръжка на система за отчитане на заявки за хранене“, Солвей Соди АД, Девня, България. Системата е в поддръжка до настоящия момент. - От 2001 – текущ – Ръководител проект, Ст. одитор по качество „Разработване, внедряване и поддръжка на система за контрол на достъпа, поддръжка на техническите системи за сигурност – видеонаблюдение, СОТ“, Солвей Соди АД, Девня, България. - 2011 – 2012, Одитор по качество „Консултантски услуги по разработване и интеграция на SharePoint базирани системи за управление на качеството и информационната сигурност съгласно ISO 9001:2008 и ISO 27001:2005.”, Бизнес софт, София Като Одитор качество извършва дейности по проверка и контрол на качеството на предлаганите от дружеството проекти и решения, съответствие с изискванията на клиента и с международните стандарти за информационна сигурност и качество.	

Заявяваме, че разполагаме с екип от неключови Хелпдеск специалисти за изпълнение на предмета на настоящата обществена поръчка, както следва:

- Андрей Витанов Георгиев
- Филип Михайлов Митов
- Николай Ангелов Георгиев
- Васил Кръстев Малинков
- Мартин Минчев Сабинов

24.11.2016 г.
(дата на подписване)

ДЕКЛАРАТОР: _____
(Димитринка Илиева – Управител)

Изготвил: Р. Каралашева
Съгласувал: С. Джурелов

113