ИЗОТСЕРВИЗ СТАРА ЗАГОРА

ПОЛИТИКА ПО УПРАВЛЕНИЕ НА ИНФОРМАЦИОННАТА СИГУРНОСТ

Въведение

Ръководството и екипът на **ИЗОТСЕРВИЗ - СТАРА ЗАГОРА ЕООД** утвърждава в ежедневната си работа висок професионализъм, дисциплина и отговорност, спазва стриктно изискванията на законодателството и насочва своите усилия към постоянно усъвършенстване и утвърждаване на престижа на компанията като предпочитан партньор за търговия с компютърни системи, компоненти, софтуер; асемблиране, ремонт и поддръжка на компютри и ИТ компоненти; структурно окабеляване и изграждане на компютърни мрежи. Изхождайки от убеждението, че търговските отношения с клиента започват със съответната продажба, а не приключват с нея, ръководството на **ИЗОТСЕРВИЗ - СТАРА ЗАГОРА** си дава сметка, че в съвременния високотехнологичен и динамичен свят, неоспоримо преимущество за бизнеса е достоверната и актуалната информация, както и нейната успешна защита. Управлението на информацията и информационните активи е от особена важност, както за нормалното обезпечаване на дейността на фирмата така и за опазване на личните (конфиденциалните) данни на клиентите и в тази връзка дейностите: **Производство, продажба, гаранционен и извънгаранционен сервиз на електронни компоненти и компютърни системи. Разработване и поддръжка на софтуерни системи. Изработка, монтаж и гаранционна и извънгаранционна поддръжка на резервоари и инсталации за продажба на светли горива и газоснабдителни станции** е основен приоритет и личен ангажимент на Управителя на ИЗОТСЕРВИЗ - СТАРА ЗАГОРА ЕООД.

Обхват

Основен момент в Политиката на СУСИ е създаването на Система за Управление на Сигурността на Информацията (СУСИ), която да изпълнява изискванията на ISO/IEC 27001:2013. На тази основа и с тази цел са формулирани всички изисквания в **ИЗОТСЕРВИЗ - СТАРА ЗАГОРА ЕООД** по отношение на сигурността на информацията. Тези аспекти се разглеждат в зависимост от особеностите в дейността на дружеството, нейното местоположение, използваните технологии и информационни активи, действащото законодателство, културната и социална среда. Настоящата политика е приложима във всички дейности, обхваща всички активи, направления и обособени структурни единици на ИЗОТСЕРВИЗ - СТАРА ЗАГОРА. Обхватът на системата е описан в документ **Обхват на СУСИ**, част от Приложенията на Наръчника по ИС (mISMS), според изискванията на Стандарт ISO/IEC 27001:2013. В обхвата на СУСИ се включва офиса и търговската част, на която се осъществява дейността с адрес: **гр. Пловдив, п.код. 4000, ул. „Граф Игнатиев" №5.**

Този документ е създаден в рамките на проект „Развитие на управленския капацитет и растеж на ИЗОТСЕРВИЗ - СТАРА ЗАГОРА ЕООД" в изпълнение на договор № BG16RFOP002-2.002-0506-C01 с финансовата подкрепа на Оперативна програма „Иновации и конкурентоспособност" 2014-2020, съфинансирана от Европейския съюз чрез Европейския фонд за регионално развитие. Цялата отговорност за съдържанието се носи от "ИЗОТСЕРВИЗ - СТАРА ЗАГОРА" ЕООД и при никакви обстоятелства не може да се приема, че този документ отразява официалното становище на Европейския съюз и Управляващия орган

Цели на информационната сигурност

Ръководството на **ИЗОТСЕРВИЗ - СТАРА ЗАГОРА ЕООД** си поставя следните **общи цели** по отношение на информационната сигурност :

- осигуряване на **съответствие с приложимото законодателство** и договорните изисквания
- осигуряване на **непрекъснатост на процесите** при запазване на **цялостност** (вярност и пълнота) **и достъпност** (само от упълномощени лица) **на информацията**, по време на нейното съхранение, обработка и предаване на други заинтересовани страни;
- **минимизиране на рисковете за сигурността на информацията**, причиняващи загуби или вреди на дружеството, неговите клиенти, партньори и други заинтересовани страни
- **минимизиране на степента на загуби или вреди**, причинени при пробиви в информационната сигурност;
- **осигуряване на необходимите ресурси** за поддържане на СУСИ и непрекъснатото й подобряване и повишаване нейната ефективност;
- **информираност на служителите за техните отговорности и задължения** по отношение на информационната сигурност;

Отговорности

В **Организационната структура** на **ИЗОТСЕРВИЗ - СТАРА ЗАГОРА ЕООД**, която е част от Приложенията към настоящия Наръчник, свързаните с информационната сигурност дейности са в правомощията на Мениджър ИС, който се назначава със Заповед на Управителя. Координацията на дейностите по създаване и поддържане на СУСИ извършва от Мениджър ИС съвместно със Системния администратор и компетентни служители от екипа на **ИЗОТСЕРВИЗ - СТАРА ЗАГОРА ЕООД**. Задълженията са регламентирани в **Права и задължения на Мениджър ИС** и в **Права и задължения на Системен Администратор** (в Приложенията на Наръчника по ИС).

Всеки актив на организацията, имащ отношение към ИС има определен **Отговорник на актив**, по смисъла, вложен в понятието "притежание на активи" в контрола А.8.1.2 на Приложение А, на Стандарт ISO 27001:2013. Правомощията на **Отговорника на актив** са документирани в **Права и задължения на Отговорник на актив** (в Приложенията на Наръчника по ИС)**.**

Ръководството и служителите на ИЗОТСЕРВИЗ - СТАРА ЗАГОРА ЕООД поемат ангажимент за осигуряване необходимото ниво на сигурност за данните, с които се работи, включително и при ползването на услуги от трети страни. В този смисъл, на договаряне със заинтересованите страни подлежат и всички необходими изисквания по отношение на информационната сигурност, в това число начините на размяна на данни,

Този документ е създаден в рамките на проект „Развитие на управленския капацитет и растеж на ИЗОТСЕРВИЗ - СТАРА ЗАГОРА ЕООД" в изпълнение на договор № BG16RFOP002-2.002-0506-C01 с финансовата подкрепа на Оперативна програма „Иновации и конкурентоспособност" 2014-2020, съфинансирана от Европейския съюз чрез Европейския фонд за регионално развитие. Цялата отговорност за съдържанието се носи от "ИЗОТСЕРВИЗ - СТАРА ЗАГОРА" ЕООД и при никакви обстоятелства не може да се приема, че този документ отразява официалното становище на Европейския съюз и Управляващия орган

степента на поверителност, методи за криптиране, изясняване на актуални законови изисквания, клаузи за конфиденциалност и други.

Основни принципи при разработване, внедряване и поддържане на СУСИ:

1. От законова гледна точка:

- защита на данни и неприкосновеност на лична информация;
- опазване на архивите на организацията;
- защита на авторски права, търговска информация и други права върху интелектуална собственост.

2. От общоприетите добри практики за информационна сигурност:

- разработване на политика по информационна сигурност;
- разпределяне на отговорностите по информационна сигурност;
- обучение по информационна сигурност;
- докладване на инциденти, свързани със сигурността;
- управление непрекъснатостта на работа;
- дисциплинарен процес вследствие от нарушенията на политиката по сигурността.

Усилията на Ръководството са насочени към:

- критичната (чувствителната) информация и системи да бъдат подлагани на редовен анализ на риска;
- за критичните (чувствителни) информационни ресурси и системи да бъдат определени „собственици" - служители отговорни за конкретните бизнес приложения, компютри и мрежи;
- информацията да бъде класифицирана по начин, който показва нейната критичност и чувствителност по отношение на организацията;
- персоналът да осъзнава проблемите на информационната сигурност;
- организацията да се съобразява с лицензите за софтуер, авторските и други свързани права, както и с други правни, регулаторни и договорни задължения;
- нарушаването на политиката по сигурността и евентуалните недостатъци в системата за информационна сигурност да бъдат докладвани;
- информационните ресурси да бъдат защитавани от гледна точка на изискванията за конфиденциалност, цялостност и достъпност.

Въвеждането и спазването на политиката по информационна сигурност цели да се забранят:

- • използването на информацията и системите на организацията без оторизация или за цели, които не са свързани с дейността й;

Този документ е създаден в рамките на проект „Развитие на управленския капацитет и растеж на ИЗОТСЕРВИЗ - СТАРА ЗАГОРА ЕООД" в изпълнение на договор № BG16RFOP002-2.002-0506-C01 с финансовата подкрепа на Оперативна програма „Иновации и конкурентоспособност" 2014-2020, съфинансирана от Европейския съюз чрез Европейския фонд за регионално развитие. Цялата отговорност за съдържанието се носи от "ИЗОТСЕРВИЗ - СТАРА ЗАГОРА" ЕООД и при никакви обстоятелства не може да се приема, че този документ отразява официалното становище на Европейския съюз и Управляващия орган

- • изнасяне на оборудване или информация от офисите и производствените помещения на организацията без оторизация;
- • неоторизирано копиране на информация и софтуер;
- • компрометиране на пароли (например със записване или разпространяване);
- • използване на персонална информация за бизнес цели, освен ако няма изрична оторизация;
- • фалшифициране на доказателства в случай на инцидент.
- • правене на порнографски/неприлични, дискриминационни или нападателни изявления, които могат да бъдат противозаконни (например с използване на електронна поща или интернет);
- • разпространение на незаконни материали (например с неприлично или дискриминационно съдържание).

Политика по оценка на риска

Системата за Управление на Информационната Сигурност на **ИЗОТСЕРВИЗ - СТАРА ЗАГОРА ЕООД** се изгражда на основата на оценката на риска, с което на практика се прилагат основните принципи за информационна сигурност, а именно принципите за **Целесъобразност** и **Основаване върху анализа на риска**.

Оценката на риска позволява на **ИЗОТСЕРВИЗ - СТАРА ЗАГОРА ЕООД** да съсредоточи противодействащите защити върху заплахите асоциирани с активите с най-висока степен на въздействие на риска.

Критериите за оценка на риска са - **Стойност на активите (A); Сериозност на потенциалната заплаха за информационната сигурност (B); Вероятност за протичане на инцидента (C); Потенциална честота на инцидента (D)**, като стойността на риска за конкретния актив по отношение на всяка конкретна заплаха и уязвимост за информационната сигурност се пресмята по формулата **R=AxBxCxD**.

След пресмятане степента на риска за информационните активи, **ИЗОТСЕРВИЗ - СТАРА ЗАГОРА ЕООД** идентифицира и обръща специално внимание на тези активи, които са с много висок или с висок риск. Същите се отразяват в Плана за намаляване (третиране) на риска, като **всяка изчислена степен на въздействие на риска по-голяма от 361 се изследва незабавно.**

Всяка изчислена степен на въздействие на риска **по-малка от 181 се третира като „приемлив риск"** и тези рискове не се отразяват в **Плана за третиране на риска.**

Политика по вътрешна организация на информационната сигурност

Ръководството провежда политика за координиране на дейностите по внедряването и поддържането на мерките за защита.

Този документ е създаден в рамките на проект „Развитие на управленския капацитет и растеж на ИЗОТСЕРВИЗ - СТАРА ЗАГОРА ЕООД" в изпълнение на договор № BG16RFOP002-2.002-0506-C01 с финансовата подкрепа на Оперативна програма „Иновации и конкурентоспособност" 2014-2020, съфинансирана от Европейския съюз чрез Европейския фонд за регионално развитие. Цялата отговорност за съдържанието се носи от "ИЗОТСЕРВИЗ - СТАРА ЗАГОРА" ЕООД и при никакви обстоятелства не може да се приема, че този документ отразява официалното становище на Европейския съюз и Управляващия орган

В **ИЗОТСЕРВИЗ - СТАРА ЗАГОРА** са разпределени отговорностите по сигурността на информацията в съответствие с Политиката по сигурност на информацията. Ангажиментите на служителите са дефинирани в длъжностните им характеристики и/или са документирани като приложения към Наръчника по ИС, включително и конкретните отговорности за изпълнението на следните дейности:

- собственост и защита на активите;
- поддръжка на ключови ресурси на организацията - мрежа, сървъри, клиентски поръчки;
- закупуване, изменения и поддръжка на софтуерните ресурси;
- закупуване, изменения и поддръжка на хардуерни компоненти;
- правилата за поддръжка на инфраструктурата, вътрешния ред и контактите с външни организации;
- управление на инциденти;
- непрекъснатостта на дейността;
- сключване на споразумения за поверителност с трети страни и изисквания за защита на поверителната информация на организацията.

Политика по управление на активите

Политиката се отнася до служители, договарящи страни, консултанти, временно работещи за фирмата и други, включително и персонал на трети страни. Тази политика се отнася до цялото информационно оборудване, собственост или използвано от **ИЗОТСЕРВИЗ - СТАРА ЗАГОРА**.

Политиката на фирмата за използване на активите цели не да налага ограничения, противоречащи на установената фирмена култура на откритост и доверие, а да защитава служителите на **ИЗОТСЕРВИЗ - СТАРА ЗАГОРА**, нейните партньори и самата фирма от незаконни и увреждащи действия, извършени предумишлено или несъзнателно.

Системите свързани с Интернет, Локална мрежа, включително компютърното оборудване, приложния софтуер, операционните системи, средствата за съхранение на информация, електронната поща и други са собственост на **ИЗОТСЕРВИЗ - СТАРА ЗАГОРА**. Тези системи са предназначени да се използват за целите на бизнеса в интерес на фирмата, на нашите клиенти и потребители, което налага въвеждане на правила за употреба.

Данните, които потребителите обработват и съхраняват в корпоративната система са собственост на фирмата и/или на клиентите на организацията. Поради необходимостта да се защитава информационната система на **ИЗОТСЕРВИЗ - СТАРА ЗАГОРА**, Ръководството на фирмата не гарантира конфиденциалност на личната информация, съхранявана на което и да е устройство, принадлежащо на **ИЗОТСЕРВИЗ - СТАРА ЗАГОРА ЕООД**.

Този документ е създаден в рамките на проект „Развитие на управленския капацитет и растеж на ИЗОТСЕРВИЗ - СТАРА ЗАГОРА ЕООД" в изпълнение на договор № BG16RFOP002-2.002-0506-C01 с финансовата подкрепа на Оперативна програма „Иновации и конкурентоспособност" 2014-2020, съфинансирана от Европейския съюз чрез Европейския фонд за регионално развитие. Цялата отговорност за съдържанието се носи от "ИЗОТСЕРВИЗ - СТАРА ЗАГОРА" ЕООД и при никакви обстоятелства не може да се приема, че този документ отразява официалното становище на Европейския съюз и Управляващия орган

Служителите са задължени да правят добра преценка относно разумността на личната употреба.

За целите на сигурността и поддръжката на мрежата, системните администратори наблюдават оборудването, системите и мрежовия трафик по всяко време.

ИЗОТСЕРВИЗ - СТАРА ЗАГОРА си запазва правото, чрез Системните администратори да деинсталира всякакъв софтуер или файлове, които не са свързани със служебните задължения на потребителя. Примери за такъв софтуер или файлове включват, но не се ограничават до, игри, музикални файлове, файлове с изображения, споделени и свободни програми, и др.

ИЗОТСЕРВИЗ - СТАРА ЗАГОРА си запазва правото периодично да одитира мрежите и системите, за да провери спазването на тази политика.

Потребителите, имащи достъп до информацията разположена в системите свързани с Интернет/Локална мрежа, са длъжни да спазват Политиката за чисто бюро, чист екран и защита на ненадзиравани устройства.

Служителите трябва да прилагат изключително внимание когато работят с електронната поща, за да се предпазят от вируси, бомби, троянски коне, червеи и друг вреден софтуер.

Изброените по-долу дейности са забранени. Служителите могат да бъдат освободени от тези ограничения само в резултат на техните утвърдени служебни задължения:

- Служителите на **ИЗОТСЕРВИЗ - СТАРА ЗАГОРА** нямат право при никакви обстоятелства да участват в каквато и да е дейност, която е незаконна спрямо националното или международното законодателство, когато използват ресурсите на **ИЗОТСЕРВИЗ - СТАРА ЗАГОРА**;
- Нарушение на правата на личност или организация, защитени от законите или разпоредбите за авторско право, търговски тайни, патенти или друга интелектуална собственост, включително и инсталирането или разпространението на „пиратски" или друг софтуерен продукт, който не е лицензиран за нуждите на **ИЗОТСЕРВИЗ - СТАРА ЗАГОРА** (вж. Лицензионна политика).
- Копиране на материали, защитени с авторско право, в т.ч. дигитализиране и разпространение на фотографии от списания, книги, музика или други защитени източници и инсталиране на софтуер, за който **ИЗОТСЕРВИЗ - СТАРА ЗАГОРА** или крайния потребител нямат активен лиценз.
- Въвеждане на вреден софтуер в мрежата или сървъра (напр. вируси, троянски коне, e-mail бомби и др.)
- Разкриване на паролите или допускане на друг човек да използва акаунтите. Това включва членове на семейството или други, живеещи в дома, когато се работи вкъщи.

Този документ е създаден в рамките на проект „Развитие на управленския капацитет и растеж на ИЗОТСЕРВИЗ - СТАРА ЗАГОРА ЕООД" в изпълнение на договор № BG16RFOP002-2.002-0506-C01 с финансовата подкрепа на Оперативна програма „Иновации и конкурентоспособност" 2014-2020, съфинансирана от Европейския съюз чрез Европейския фонд за регионално развитие. Цялата отговорност за съдържанието се носи от "ИЗОТСЕРВИЗ - СТАРА ЗАГОРА" ЕООД и при никакви обстоятелства не може да се приема, че този документ отразява официалното становище на Европейския съюз и Управляващия орган

- Представяне на фалшиви оферти за продукти или услуги на **ИЗОТСЕРВИЗ - СТАРА ЗАГОРА**.
- Въвеждане на пробиви и разриви в мрежовите комуникации. Пробивите включват достъп до данни, до акаунт или до сървър, за които служителят не е оторизиран.
- Извършване на каквато и да е форма на наблюдение на мрежата, която ще прихваща данни, които не са предназначени за работните станции на служителите, с изключение на случаите, когато тази дейност е част от нормалните служебни задължения.
- Проваляне на автентификацията на потребителя или сигурността на която и да е станция, мрежа или акаунт.
- Използване на програма/скрипт/акаунт или изпращане на съобщения от всякакъв вид с намерение да се попречи или да се прекъсне сесията на потребителя, чрез всякакви средства локално или чрез Интернет/Локална мрежа.
- Предоставяне на информация за служителите и клиентите на **ИЗОТСЕРВИЗ - СТАРА ЗАГОРА** на страни извън организацията.

Политика по сигурността, свързана с човешките ресурси

Човешките ресурси са основен елемент от СУСИ. Политиката по сигурността на човешките ресурси на **ИЗОТСЕРВИЗ - СТАРА ЗАГОРА** е насочена основно към осъзнаване на необходимостта от осигуряване на информационната сигурност чрез адекватно дефиниране на отговорности и обучение.

Администрирането на човешките ресурси обхваща целия процес - проучване на кандидатите, назначаване, определяне на задълженията, промяна на длъжността и прекратяване на договорите, и се извършва в съответствие с разработена, документирана и внедрена процедура **Сигурност на човешките ресурси (ИС А7).**

Контролът по връщането на активите на организацията се осъществява чрез подписване на декларация за поверителност, протокол за предоставяне на достъп до информационните ресурси при постъпване на работа и отнемане на достъп при напускане на работа. Правата за достъп се дават в съответствие с **Сигурност на човешките ресурси (ИС А7).**.

Всички служители на организацията, и където е уместно, доставчиците и потребителите от трета страна, в съответствие с техните функции на работа, преминават подходящо обучение и редовно актуализиране на знанията по политиката и процедурите на СУСИ.

Всички служители на **ИЗОТСЕРВИЗ - СТАРА ЗАГОРА** и други физически лица, които използват ресурси и активи на Дружеството, подписват Декларация за поверителност.

В случаи на сериозно нарушение на политиката и правилата за сигурност се прилага дисциплинарен процес, който включва отнемане на права за достъп до информационни ресурси, на активи и, ако е необходимо, отстраняване от работа.

Този документ е създаден в рамките на проект „Развитие на управленския капацитет и растеж на ИЗОТСЕРВИЗ - СТАРА ЗАГОРА ЕООД" в изпълнение на договор № BG16RFOP002-2.002-0506-C01 с финансовата подкрепа на Оперативна програма „Иновации и конкурентоспособност" 2014-2020, съфинансирана от Европейския съюз чрез Европейския фонд за регионално развитие. Цялата отговорност за съдържанието се носи от "ИЗОТСЕРВИЗ - СТАРА ЗАГОРА" ЕООД и при никакви обстоятелства не може да се приема, че този документ отразява официалното становище на Европейския съюз и Управляващия орган

Политика по физическа сигурност и сигурност на заобикалящата среда

ИЗОТСЕРВИЗ - СТАРА ЗАГОРА провежда политика на защита на средствата за обработка и съхранение на информацията чрез определяне на граници на физическа сигурност и организация на зони за сигурност.

Работните помещения и техниката се защитават от физическо влизане чрез система за сигурност с различни зони за достъп и определени права за достъп до всяка зона, посочени в процедура **Физическа сигурност и сигурност на заобикалящата среда (ИС А11)**.

Прилагат се механизми за контрол на физическото влизане, които ограничават достъп до зоните с чувствителна или критична информация само на упълномощени служители.

Определени са местата за достъп на клиенти, доставки и зареждане. За да се избегне неразрешен достъп, не се допуска присъствие на външни лица в работните помещения без придружител.

Политиката на **ИЗОТСЕРВИЗ - СТАРА ЗАГОРА** по отношение на защита на устройствата цели намаляване на риска от неразрешен достъп до информацията с всички възможни последствия, загуба, повреда, кражба, прекъсване на дейността. Прилагат се технически мерки за защита от пожар и прекъсване в електрозахранването, защита на окабеляването и комуникационните връзки.

Изнасянето на устройства и работа извън офисите на фирмата, начините за поддръжка на информационните ресурси, както и за тяхното унищожаване или повторно използване, се извършва само и единствено с разрешение от Управителя.

ИЗОТСЕРВИЗ - СТАРА ЗАГОРА провежда и целенасочена политика за осигуряване на условия за безопасна работа в съответствие със Закона за здравословни и безопасни условия на труд.

Политика по контрол на достъпа

Политиката на **ИЗОТСЕРВИЗ - СТАРА ЗАГОРА** за контрол на достъпа е базирана на принципите „необходимо да знае" или „необходимо да се ограничи", „всеки достъп, който не е изрично разрешен е забранен" и минимализиране на привилегиите.

Ръководството на **ИЗОТСЕРВИЗ - СТАРА ЗАГОРА ЕООД** прилага мерки на контрол на достъпа, които да осигуряват:

- физическа защита на информационните ресурси;
- достъп до съответните информационни ресурси в съответствие с политиката на собственика на ресурса и на ръководството на организацията;
- определяне на нивата на достъп в съответствие с ролята, която трябва да изпълняват служителите на организацията и нивата на класификация на информацията;

Този документ е създаден в рамките на проект „Развитие на управленския капацитет и растеж на ИЗОТСЕРВИЗ - СТАРА ЗАГОРА ЕООД" в изпълнение на договор № BG16RFOP002-2.002-0506-C01 с финансовата подкрепа на Оперативна програма „Иновации и конкурентоспособност" 2014-2020, съфинансирана от Европейския съюз чрез Европейския фонд за регионално развитие. Цялата отговорност за съдържанието се носи от "ИЗОТСЕРВИЗ - СТАРА ЗАГОРА" ЕООД и при никакви обстоятелства не може да се приема, че този документ отразява официалното становище на Европейския съюз и Управляващия орган

- механизми за контрол на физическото влизане;
- определяне на зони за обществен достъп, доставки и зареждане;
- контрол на нивото на достъп за всеки служител от регистрирането до крайната де-регистрация;
- разделяне на ролите за контрол на достъпа;
- минимизиране на необходимостта от специални привилегии;
- спазване на правилата за „чисто бюро и чист екран";
- защита на ненадзиравани устройства;
- ограничаване нивата на достъп на външни потребители на информационната система
- отнемане на права на достъп при напускане;
- периодичен преглед на достъпа;
- ъпргрейд на контрола на достъп в отговор на нови заплахи, възможности, изисквания на бизнеса или изводи от инциденти.

Политика по разработване, внедряване и поддържане на информационните системи

Политиката на **ИЗОТСЕРВИЗ - СТАРА ЗАГОРА** по разработване, внедряване, изменение и поддържане на информационните системи е базирана на принципа на превантивната оценка на риска от измененията, включително ъпгрейд на съществуващи и внедряване на нови елементи от системата, разделение на средата за изпитване от действащата информационна система и планирана поддръжка на цялата информационна система.

С цел предотвратяване на грешки, загуба, неразрешено изменение или използване на информация в приложни системи се прилагат механизми за контрол върху входните данни, вътрешната обработка, изходните данни и данните за изпитването на системата.

Всички изменения в хардуера и в софтуера на системата се извършват само с предварително разрешение и в съответствие с процедура **Придобиване, разработване и поддържане на системите (ИС А14).**

Приложени са мерки за управление на технически уязвимости, които включват приложенията, операционните системи и оценка на риска, свързан с техническите уязвимости.

Организацията определя изискванията за сигурност, които трябва да се спазват при придобиване, разработване и поддържане.

Този документ е създаден в рамките на проект „Развитие на управленския капацитет и растеж на ИЗОТСЕРВИЗ - СТАРА ЗАГОРА ЕООД" в изпълнение на договор № BG16RFOP002-2.002-0506-C01 с финансовата подкрепа на Оперативна програма „Иновации и конкурентоспособност" 2014-2020, съфинансирана от Европейския съюз чрез Европейския фонд за регионално развитие. Цялата отговорност за съдържанието се носи от "ИЗОТСЕРВИЗ - СТАРА ЗАГОРА" ЕООД и при никакви обстоятелства не може да се приема, че този документ отразява официалното становище на Европейския съюз и Управляващия орган

Политика по управление на инциденти и подобряване на сигурността на информацията

С цел намаляване на риска и произтичащите от появата на инциденти разходи **ИЗОТСЕРВИЗ - СТАРА ЗАГОРА ЕООД** е разработила и внедрила политика за управление на инциденти, която е насочена към разработване и внедряване на процедури и средства за ефективно третиране на слабостите и пробивите, свързани със сигурността на информацията. Мерките обхващат непрекъснато наблюдение, реагиране, оценяване, подобряване и цялостно управление на слабостите и инцидентите.

Всички потребители на информационните системи са задължени да докладват за наблюдавани събития и слабости в информационната сигурност в съответствие с **Управление на инциденти по информационната сигурност (ИС А16)**.

Действията свързани с управление на инциденти включват докладване, анализ на причината, планиране на коригиращи и превантивни мерки за предотвратяване от повторна поява, възстановяване на системата и съобщаване за инцидента.

Действията за възстановяване след нарушение на сигурността и за коригиране на грешки на системата се извършват от определен и упълномощен персонал и са документирани, и докладвани.

Където се изискват доказателства, те се събират и съхраняват, за да се гарантира съответствие с изискванията на нормативните актове при последващи правни действия срещу лице или организация след инцидент със сигурността на информацията.

В **ИЗОТСЕРВИЗ - СТАРА ЗАГОРА** се събират данни и се извършва анализ на вида и броя на инцидентите, и на направените разходи по разрешаване на инцидентите с цел да се идентифицират повтарящите се инциденти или инцидентите с голямо влияние, и да се ограничат честотата, щетите и загубите от появата им в бъдеще. Оценката на инцидентите е част от входните данни при Прегледа от ръководството.

Политика за осигуряване на непрекъснатостта на бизнеса

Ръководството на **ИЗОТСЕРВИЗ - СТАРА ЗАГОРА ЕООД** разбира необходимостта от планиране непрекъснатостта на бизнеса. То осъзнава, че има значителен риск за неговите критични процеси при потенциални и неочаквани разрушителни събития. Увеличаващото се развитие на процеси базирани на технологии и силната зависимост от информационните технологии е основание за създаване на план за непрекъснатост на работа.

В **ИЗОТСЕРВИЗ - СТАРА ЗАГОРА** е разработен План за непрекъснатост на работата, който гарантира работата на критичните ресурси на системата при настъпване на сериозни неблагоприятни условия и прекъсване по-голямо от 48 часа. Планът е разработен от Мениджър ИС и е съгласуван с ръководителите отдели и отговорниците на пряко подчинение на Управителя.

Планът за непрекъснатостта е разработен и приложен във всички отдели и направления с цел критичните бизнес задачи да бъдат възстановени в максимално кратък период от

Този документ е създаден в рамките на проект „Развитие на управленския капацитет и растеж на ИЗОТСЕРВИЗ - СТАРА ЗАГОРА ЕООД" в изпълнение на договор № BG16RFOP002-2.002-0506-C01 с финансовата подкрепа на Оперативна програма „Иновации и конкурентоспособност" 2014-2020, съфинансирана от Европейския съюз чрез Европейския фонд за регионално развитие. Цялата отговорност за съдържанието се носи от "ИЗОТСЕРВИЗ - СТАРА ЗАГОРА" ЕООД и при никакви обстоятелства не може да се приема, че този документ отразява официалното становище на Европейския съюз и Управляващия орган

време. Планът представлява неразделна част от всички процеси по управление. Планът по непрекъснатостта е съгласуван и утвърден по отношение на алтернативни офиси и възстановителни процеси, като определя специфичните отговорности на определените екипи, които да осигурят възобновяване и възстановяване на критичните информационни функции.

Планът осигурява придобиване и поддържане на резерв от информационни ресурси, необходими за осъществяването непрекъснатост на работа.

Планът се поддържа и тества, с цел установяване на пропуски и слабости.

Промените в информационната система на **ИЗОТСЕРВИЗ - СТАРА ЗАГОРА** се разглеждат и оценяват по отношение на влиянието и риска, свързани с плана за непрекъснатост.

Политиката и планът за непрекъснатост на работа са координирани с дейностите по информационна сигурност, включително физическа сигурност, човешки ресурси, архивиране.

Непрекъснатостта на поддържането на интернет връзката и на интернет страницата на **ИЗОТСЕРВИЗ** е споделена отговорност с доставчиците на услугите и се базира на двустранни договори.

Лицензионна политика

Политиката на организацията е създадена с цел да се спазват всички авторски права на компютърния софтуер, както и условията по софтуерните лицензи, по които тя е страна. Организацията предприема всички необходими действия за предотвратяване на копирането на лицензиран софтуер от потребителите, както и използването на свързана с него документация в офисите на организацията или на друго място, освен ако не съществува изрично разрешение за това съгласно договора с лицензодателя. Забранява се на служителите да използват софтуера по начин, който не съответства на лицензионния договор, включително предоставяне или получаване на софтуер или шрифтове от клиенти, изпълнители по договори, потребители и други.

Целият софтуер, придобит от организацията, трябва да бъде закупен след съгласуване със системните администратори и Отговорника по сигурността. Каналите за придобиване на софтуер са ограничени, за да гарантират, че организацията поддържа пълна документация за закупения софтуер и може да регистрира, поддържа и актуализира съответния софтуер. Това включва и софтуер, който може да бъде свален и/или закупен от интернет.

Компютрите на **ИЗОТСЕРВИЗ - СТАРА ЗАГОРА** са активи собственост на дружеството, използват се с лицензиран софтуер и са защитени от вируси. Забранява се на потребителите да внасят/свалят софтуер и да го инсталират на своите компютри. Притежаваният от организацията софтуер не може да бъде изнасян от потребителите и инсталиран на други компютри.

Този документ е създаден в рамките на проект „Развитие на управленския капацитет и растеж на ИЗОТСЕРВИЗ - СТАРА ЗАГОРА ЕООД" в изпълнение на договор № BG16RFOP002-2.002-0506-C01 с финансовата подкрепа на Оперативна програма „Иновации и конкурентоспособност" 2014-2020, съфинансирана от Европейския съюз чрез Европейския фонд за регионално развитие. Цялата отговорност за съдържанието се носи от "ИЗОТСЕРВИЗ - СТАРА ЗАГОРА" ЕООД и при никакви обстоятелства не може да се приема, че този документ отразява официалното становище на Европейския съюз и Управляващия орган

Всички потребители използват наличния софтуер при спазване на съответните лицензионни договори и са наясно, че не притежават този софтуер или свързаната с него документация, и освен ако изрично не са упълномощени от издателя на софтуера, не могат да правят допълнителни копия.

ИЗОТСЕРВИЗ - СТАРА ЗАГОРА няма да толерира използването на неоторизирани копия на софтуер. Всеки, който незаконно копира софтуер, може да бъде обект на граждански или наказателни санкции, включително налагане на глоби и съдебно производство. Никой потребител не трябва да толерира незаконното копиране на софтуер при никакви обстоятелства, а всеки който разработва, използва или придобива нелицензиран софтуер ще бъде наказан дисциплинарно.

При никакви обстоятелства в **ИЗОТСЕРВИЗ - СТАРА ЗАГОРА** не може да се използва софтуер, който е донесен от нелицензирано местонахождение, включително, но не само от интернет, дом, приятели и колеги.

Политика за защита на авторските права

Политиката на **ИЗОТСЕРВИЗ - СТАРА ЗАГОРА** за защита на авторските права е изцяло съобразена със Закона за авторското право и сродните му права.

Клиентът запазва всички авторски права върху информационните ресурси и материали, включително файлове, каталози и други готови изображения, върху техния дизайн, върху запазени знаци и марки, които предоставя на **ИЗОТСЕРВИЗ - СТАРА ЗАГОРА** с цел осъществяване на дейността.

ИЗОТСЕРВИЗ - СТАРА ЗАГОРА съхранява цялата информация, подадена от клиента, при строга конфиденциалност и пази търговската тайна на клиента и на неговите клиенти и потребители, като гарантира и поема задължение да не използва нито в свой интерес, нито в интерес на трети лица, запазени знаци, бази данни, лични данни, образи и друга информация на или за Клиента или неговите клиенти и потребители, станала известна при изпълнение на поетите професионални ангажименти.

Политика за защита на личните данни

Политиката на **ИЗОТСЕРВИЗ - СТАРА ЗАГОРА** за защита на личните данни е изцяло е съобразена съгласно изискванията на Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27.04.2016 относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни. **ИЗОТСЕРВИЗ - СТАРА ЗАГОРА е** администратор на лични данни към КЗЛД и обработва предоставените данни и персонална информация съобразно Закон за защита на личните данни и Общия регламент за защита на личните данни (ЕС) 2016/679. Правното съответствие се контролира от Управителя, а се управлява от Мениджър ИС.

В зависимост от конкретната ситуация, **ИЗОТСЕРВИЗ - СТАРА ЗАГОРА** може да обработва данни в качеството на администратор или обработващ. Обработването на лични данни означава всяка операция или съвкупност от операции, извършвана с лични

Този документ е създаден в рамките на проект „Развитие на управленския капацитет и растеж на ИЗОТСЕРВИЗ - СТАРА ЗАГОРА ЕООД" в изпълнение на договор № BG16RFOP002-2.002-0506-C01 с финансовата подкрепа на Оперативна програма „Иновации и конкурентоспособност" 2014-2020, съфинансирана от Европейския съюз чрез Европейския фонд за регионално развитие. Цялата отговорност за съдържанието се носи от "ИЗОТСЕРВИЗ - СТАРА ЗАГОРА" ЕООД и при никакви обстоятелства не може да се приема, че този документ отразява официалното становище на Европейския съюз и Управляващия орган

данни или набор от лични данни чрез автоматични или други средства като събиране, записване, организиране, структуриране, съхранение, адаптиране или промяна, извличане, консултиране, употреба, разкриване чрез предаване, разпространяване или друг начин, по който данните стават достъпни, подреждане или комбиниране, ограничаване, изтриване или унищожаване.

Обработването на лични данни се състои в осигуряване на достъп до определена информация само за лица, чиито служебни задължения или конкретно възложени задачи налагат такъв достъп.

Лични данни са всяка информация, отнасяща се до физическо лице, което може да бъде идентифицирано, пряко или непряко чрез нея (например име, ЕГН, данни за местонахождение, онлайн идентификатор) или по един или повече признаци, специфични за физическата, физиологичната, генетичната, психическата, умствената, икономическата, културната или социална идентичност на това физическо лице (пол, раса, етнически произход, политически убеждения, членство в синдикални организации, сексуална ориентация и др.).

ИЗОТСЕРВИЗ - СТАРА ЗАГОРА не продава, отдава, търгува с каквато и да е лична информация, получена от служителите си или от подизпълнителите.

Определените отговорни служители, обработващи лични данни, са задължени да третират информацията като конфиденциална.

Предприети са мерки за физическа и логическа защита на личните данни и са ограничени правата за достъп до тях.

Всеки служител, за когото се отнасят данните има право на достъп до своите данни, както и да изиска тяхното коригиране, което се изразява в писмено **съгласие** от негова страна за право на информация относно личните му данни, достъпа до тях и коректно съхраняване. Право да изисква коригиране, изтриване или ограничено обработване на личните му данни. Право да възразява срещу обработване поради причини, свързани с легитимни интереси, обществен интерес, или профилиране, освен ако Администраторът не докаже съществуването на защитени, обосновани причини, имащи приоритет пред неговите интереси, права и свободи, или че това обработване се извършва с цел предявяване, упражняване или защита по правни претенции. Право на преносимост на данните. Право на подаване на оплакване през Комисията за защита на личните данни. Право по всяко време да оттегли съгласието си за събирането, обработването и използването на личните данни с действие занапред всяко свободно изразено, конкретно, информирано и недвусмислено указание за волята на субекта на данни, посредством изявление или ясно потвърждаващо действие, което изразява съгласие за обработка на лични данни, свързани с него.

Заключение

Политиката по информационна сигурност е разпространена до трети страни, които имат достъп до информацията и системите на организацията.

Този документ е създаден в рамките на проект „Развитие на управленския капацитет и растеж на ИЗОТСЕРВИЗ - СТАРА ЗАГОРА ЕООД" в изпълнение на договор № BG16RFOP002-2.002-0506-C01 с финансовата подкрепа на Оперативна програма „Иновации и конкурентоспособност" 2014-2020, съфинансирана от Европейския съюз чрез Европейския фонд за регионално развитие. Цялата отговорност за съдържанието се носи от "ИЗОТСЕРВИЗ - СТАРА ЗАГОРА" ЕООД и при никакви обстоятелства не може да се приема, че този документ отразява официалното становище на Европейския съюз и Управляващия орган

Политиката по информационна сигурност се преглежда редовно на базата на установен процес.

Политиката по информационна сигурност се ревизира, за да се вземат под внимание променящите се обстоятелства.

Всеки служител, който прецени, че има злоупотреба с настоящата политика в организацията, трябва да уведоми Мениджър ИС.

Всеки служител, за когото е установено, че е нарушил тази политика, подлежи на дисциплинарна отговорност.

Персоналът на **ИЗОТСЕРВИЗ - СТАРА ЗАГОРА ЕООД** се задължава да спазва всички правила, свързани с информационната сигурност, описани в процедури, инструкции и други документи от СУСИ.

Ръководството на **ИЗОТСЕРВИЗ - СТАРА ЗАГОРА ЕООД** *декларира своята пълна ангажираност в процесите на развитие, поддържане и усъвършенстване на СУСИ.*

21.05.2018 *Управител: ……. инж. Илчо Илчев*

Този документ е създаден в рамките на проект „Развитие на управленския капацитет и растеж на ИЗОТСЕРВИЗ - СТАРА ЗАГОРА ЕООД" в изпълнение на договор № BG16RFOP002-2.002-0506-C01 с финансовата подкрепа на Оперативна програма „Иновации и конкурентоспособност" 2014-2020, съфинансирана от Европейския съюз чрез Европейския фонд за регионално развитие. Цялата отговорност за съдържанието се носи от "ИЗОТСЕРВИЗ - СТАРА ЗАГОРА" ЕООД и при никакви обстоятелства не може да се приема, че този документ отразява официалното становище на Европейския съюз и Управляващия орган