РЕПУБЛИКА БЪЛГАРИЯ
МИНИСТЕРСТВО НА ЗДРАВЕОПАЗВАНЕТО
РЕГИОНАЛНА ЗДРАВНА ИНСПЕКЦИЯ-СЛИВЕН

С ЛИЦЕ КЪМ ХОРАТА

УТВЪРДИЛ:
Д-Р ПЕТЯ БАЛУЛОВА
ДИРЕКТОР РЗИ СЛИВЕН

ЗАПОВЕД ЗА УТВЪРЖДАВАНЕ № РД-19-263/01.11.2019г.

ВЪТРЕШНИ ПРАВИЛА

ЗА МРЕЖОВАТА И ИНФОРМАЦИОННА СИГУРНОСТ

В РЕГИОНАЛНА ЗДРАВНА ИНСПЕКЦИЯ - СЛИВЕН

Регионална здравна инспекция-Сливен; ул. „Пейо Яворов" № 1; гр. Сливен
тел. 044 616 200; 044 616 201; факс 044 667 330
e-mail: rzi-sliven@mbox.contact.bg
web site: www.rzi-sliven.org

РАЗДЕЛ I
ОБЩИ ПОЛОЖЕНИЯ

Чл. 1. Настоящите правила имат за цел осигуряването на контрол и управление на работата на информационните системи в РЗИ-Сливен. В този смисъл понятието информационна система се определя като съвкупност от компютърна и периферна техника, програмни продукти, данни и обслужващ персонал, като компютрите могат да бъдат свързани в локална мрежа или по друг начин, както и да обменят информация чрез съответните устройства и програми. Програмните продукти и бази данни могат да бъдат специфични за всяко звено от РЗИ-Сливен.

Чл. 2. Потребителите на информационни системи в РЗИ-Сливен са задължени с отговорни действия да гарантират ефективното и ефикасно използване на системите.

Чл. 3. Проектирането и изграждането на информационни и комуникационни системи се извършва така, че те да представляват компоненти с възможност за интеграция в единна потребителска среда и при спазване на Наредба за минималните изисквания за мрежова и информационна сигурност.

Чл.4. Настоящите вътрешни правила само пояснява част от Наредбата за минималните изисквания за мрежова и информационна сигурност в случай на противоречие с нея тя следва да има предимство, като всички служители в Инспекцията следва да са запознати с нея.

РАЗДЕЛ II

КОНТРОЛ НА ДОСТЪПА И ПРАВИЛА ЗА РАБОТА С НОСИТЕЛИ

Чл. 5. Защитата и контролът на информационните и компютърните системи се извършва при спазване на следните основни принципи:

(1) разделяне на потребителски от администраторски функции;

(2) установяване на нива и достъп до информация;

(3) регистриране на достъпа, въвеждането, промяната и заличаването на данни и информация;

(4) осъществяването на контрол от специализирани звена и служители на РЗИ-Сливен.

Чл. 6. Всеки служител има точно определени права на достъп и използва уникален потребителски профил за вход в системата и достъп до данните, за които е оторизиран, така че да може да бъде идентифициран. Не е разрешено използването на групови профили;

Чл. 7. Контрол на управлението и защитата на достъпа до мрежови връзки и мрежови услуги се извършва чрез средствата на активна директория с конкретно потребителско име, мрежи и мрежови услуги.

Чл. 8. Предоставянето на достъп става по дефиниран вътрешен ред, като се задават определени права на достъп до конкретни информационни ресурси, според заемната длъжност и функция. Не се задава и не се осигурява достъп на неоторизирани лица.

Чл. 9. Лицата, които обработват лични данни, използват уникални пароли с достатъчно сложност, които не се записват или съхраняват онлайн;

Чл. 10. Всички пароли за достъп на системно ниво се променят периодично.

Чл. 11. Всички носители на лични данни се съхраняват в безопасна и сигурна среда - в съответствие със спецификациите на производителите, в заключени шкафове, с ограничен и контролиран достъп.

Чл. 12. На служителите на РЗИ-Сливен, които използват електронни бази данни и техни производни (текстове, разпечатки, карти и скици) се забранява:

(1) да ги изнасят под каквато и да е форма извън служебните помещения преди извеждане от деловодството (извършване на услуга);

(2) да ги използват извън рамките на служебните си задължения;

(3) да ги предоставят на външни лица без да е заявена услуга.

Чл. 13. За нарушение целостта на данните се считат следните действия:

(1) унищожаване на бази данни или части от тях;

(2) повреждане на бази данни или части от тях;

(3) вписване на невярна информация в бази данни или части от тях.

Чл. 14. При изнасяне на носители извън физическите граници на РЗИ-Сливен, те се поставят в подходяща опаковка и в запечатан плик.

Чл. 15. На служителите е строго забранено да използват мобилни компютърни средства на места, където може да възникне риск за средството и информацията в него. Потребителите на мобилни компютърни средства и мобилни телефони отговарят за защитата им от кражба и не ги оставят без наблюдение.

Чл. 16. Служителите са длъжни да избягват всякакъв риск от достъп до информация от неупълномощени лица, както и до злоумишлен софтуер. Забранено е съобщаването на тайна и чувствителна информация по мобилни телефони на места, където може да стане достъпна за трети страни.

Чл. 17. След като повече не са необходими, носителите се унищожават сигурно и безопасно за намаляване на риска от изтичане на чувствителна информация към неупълномощени лица. Физическото унищожаване на информационните носители става със счупване. Предварително се проверят, за да е сигурно, че необходимата информация е копирана и след това цялата информация е изтрита от тях преди унищожаване.

Чл.18. Събирането, подготовката и въвеждането на данни на страницата се извършва от администратора на сайта на РЗИ-Сливен и от служители на РЗИ-Сливен.

Чл.19. Събирането и подготовката на данните се извършва от служители в техния ресор, след което данните се изпращат в електронен вид (на файлове) на служителите отговорни за качването им на интернет страницата на РЗИ-Сливен.

РАЗДЕЛ III

РАБОТНО МЯСТО

Чл.20. Работното място се състои от работно помещение, работна маса и стол, компютърна и периферна техника, комуникационни средства.

Чл.21. Работното място се оборудва при спазване на изискванията на Наредба № 7 от 15.08.2005 г. за минималните изисквания за осигуряване на здравословни и безопасни условия на труд при работа с видеодисплеи (Издадена от министъра на труда и социалната политика и министъра на здравеопазването, обн., ДВ, бр.70 от 26.08.2005 г.).

Чл.22. Всеки служител на РЗИ-Сливен отговаря за целостта на компютърната и периферна техника, програмните продукти и данни, инсталирани на компютъра на неговото работно място или ползвани от него на сървъра на локалната компютърна мрежа съобразно дадените му права.

Чл.23. Служителят има право да работи на служебен компютър, като достъпът до съхраняваните данни се осъществява от него с въвеждането на потребителско име и парола;

Чл.24. Забранява се на външни лица работата с персоналните компютри на РЗИ-Сливен, освен за упълномощени фирмени специалисти в случаите на първоначална инсталация на компютърна и периферна техника, програми, активни и пасивни компоненти на локални компютърни мрежи, комуникационни устройства и сервизна намеса на място, но задължително в присъствие на администратора на РЗИ-Сливен.

Чл.25. След края на работния ден всеки служител задължително изключва компютъра.

Чл.26. Забраняват се опити за достъп до компютърна информация и бази данни, до които не са предоставени права, съобразно заеманата от служителя длъжност, както и извършването на каквито и да е действия, които улесняват трети лица за несанкциониран достъп.

Чл.27. Инсталиране и разместване на компютърни конфигурации и части от тях, на периферна техника, на активни и пасивни компоненти на локални компютърни мрежи, на комуникационни устройства се извършва само след съгласуване с администратора на РЗИ-Сливен.

Чл.28. Забранява се използването на преносими магнитни, оптични и други носители с възможност за презаписване на данни за прехвърляне на файлове между компютри, свързани в компютърната мрежа на РЗИ-Сливен.

Чл.29. Служителите имат право да обменят компютърна информация посредством вътрешна компютърна мрежа само във връзка с изпълнение на служебните си задължения и само със служителите, с които имат преки служебни взаимоотношения.

Чл.30. Архивирана компютърна информация се предоставя само на служители, които имат право на достъп, съгласно заеманата от тях длъжност и изпълнявана задача, при спазване на принципа „необходимост да се знае."

Чл.31. Достъпът до компютърна информация, бази данни и софтуер се ограничава посредством технически методи - идентификация на потребител, пароли, отчитане на времето на достъп, забрани за копиране, проследяване на несанкциониран достъп.

Чл.32. Достъпът до помещенията, където са разположени сървърите се ограничава по възможност само до специализиран по поддръжката им персонал.

РАЗДЕЛ IV

ПОЛЗВАНЕ НА КОМПЮТЪРНАТА МРЕЖА И ИНТЕРНЕТ

Чл.33. Упълномощеният администратор извършва необходимите настройки за достъп до интернет, създават потребителски имена и пароли за работа с компютърната мрежа и електронната поща на РЗИ-Сливен.

Чл.34. Ползването на компютърната мрежа и електронната поща от служителите става чрез получените потребителско име и парола.

Чл.35. Ползването на интернет и служебна електронна поща се ограничават съобразно скоростта на ползвания достъп до интернет, броя на откритите работни места и необходимостта от ползване на тези услуги съобразно служебните задължения на служителите.

Чл.36. Служителите на съответните работни места са длъжни да не споделят своите потребителски имена и пароли с трети лица и носят дисциплинарна отговорност, ако се установи неправомерно ползване на ресурсите на компютърната мрежа, достъпа до интернет или електронна поща при използване на предоставените им потребителски имена и пароли.

Чл.37. Компютрите, свързани в мрежата на РЗИ-Сливен използват интернет само от доставчик, с когото РЗИ-Сливен има сключен договор за доставка на интернет.

Чл.38. Забранява се свързването на компютри едновременно в мрежата на РЗИ-Сливен и в други мрежи, когато това позволява разкриване и достъп до IP адреси от мрежата на РЗИ-Сливен и/или е в противоречие с изискванията на Закона за електронното управление (ЗЕУ) и Наредба за общите изисквания за оперативна съвместимост и информационна сигурност.

Чл.39. Забранява се инсталирането и използването на комуникатори (като icq, skype и др. подобни), осигуряващи достъп извън рамките на компютърната мрежа на РЗИ- Сливен и създаващи предпоставки за идентифициране на IP адрес на потребителя и за достъп на злонамерен софтуер и мобилен код до компютрите, свързани в компютърната мрежа на РЗИ-Сливен.

Чл.40. Забранява се съхраняването на сървърите на РЗИ-Сливен на лични файлове с текст, изображения, видео и аудио.

Чл.41. Забранява се отварянето без контрол от страна на администратор:

(1) получени по електронна поща или на преносими носители изпълними файлове, файлове с мобилен код и файлове, които могат да предизвикат промени в системната конфигурация, напр. файлове с разширения .exe, .vbs, .reg и архивни файлове;

(2) получени по електронна поща съобщения, които съдържат неразбираеми знаци.

РАЗДЕЛ V

ЗАЩИТА

ОТ

КОМПЮТЪРНИ ВИРУСИ И ДРУГ ЗЛОВРЕДЕН СОФТУЕР

Чл.41. С цел антивирусна защита се прилагат следните мерки:

(1) Всички персонални компютри имат инсталиран антивирусен софтуер в реално време, който се обновява ежедневно.

(2) Администратора извършва следните дейности:

2.1 активира защитата на съответните ресурси - файлова система, електронна поща и извършва първоначално пълно сканиране на системата;

2.2 настройва антивирусния софтуер за периодични сканирания през определен период;

2.3 проверява за правилно настроен софтуер за автоматично обновяване на операционната система и инсталирания софтуер;

(3) При поява на съобщение от антивирусната програма за вирус в локалната мрежа, всеки служител от съответното работно място задължително информира администратора.

НЕОТОРИЗИРАНО ИЗПОЛЗВАНЕ НА УСТРОЙСТВА

42.Личните технически средства се използват само от лицата на които се водят по ведомост и отговарят за тях.

43.Преносимите записващи устройства се ползват само от лицата на които се водят по ведомост, като се забранява споделено ползване от цяла дирекция или няколко служители.

АДМИНИСТРИРАНЕ НА ИНФОРМАЦИОННИТЕ И КОМУНИКАЦИОННИТЕ СИСТЕМИ

44. РЗИ-Сливен прилага следните мерки за защита на профилите с административни права за информационните и комуникационните системи и техните компоненти:

1. преди въвеждане в експлоатация задължително се сменят идентификационните данни на администратора, въведени по подразбиране или инсталирани от производителя/доставчика на информационния актив;

2. администраторските профили са персонални;

3. администраторските профили се използват само за административни цели;

4. администраторските профили се създават само на служители, които извършват административни операции (инсталиране, конфигуриране, управление, поддръжка и т. н.);

5. правата на всеки администраторски акаунт са ограничени във възможно най-голяма степен до функционалния и техническия периметър на всеки администратор;

6. данните за автентикацията на администраторските акаунти:

а) са различни за всяка система;

б) са с възможно най-голяма сложност, позволена от системата или нейния компонент;

в) се съхраняват подходящо физически и логически защитени, като достъп до тях има само оторизиран представител на РЗИ-Сливен

7. поддържа списък на администраторските профили за информационните и комуникационните системи и техните компоненти;

8. при невъзможност на администратор да изпълнява пълноценно функциите си поради обективни причини правата на административния му акаунт се спират за съответния период;

9. поне веднъж годишно се прави преглед на администраторските профили с цел удостоверяване на актуалността им.

(2) Паролите за автентикация на администраторските профили се сменят задължително:

1. периодично - най-малко веднъж в годината;

2. при прекратяването на договорните отношения със служители или трети страни, на които тези данни са били известни;

3. при пробив в мрежовата и информационната сигурност.

ЗАЩИТА НА ХАРДУЕРНИ УСТРОЙСТВА

45.За намаляване на риска от инциденти, предизвикани от технически повреди, РЗИ-Сливен:

1. осигурява климатико-механичните условия, указани от производителя;
2. осъществява наблюдение на параметрите на условията по т. 1;
3. провежда планирана регулярна техническа профилактика на устройствата в съответствие с политиката му за жизнения им цикъл.

(2) За намаляване на риска от неоторизиран достъп РЗИ-Сливен е длъжена да разполага устройствата в зони, които са физически и логически защитени в съответствие с класификацията на информацията, с която работят.

РАЗДЕЛ VI

НЕПРЕКЪСНАТОСТ НА РАБОТАТА

Чл.42. Мерките, които се прилагат с цел антивирусна защита са:

1. Всички сървъри и устройства за съхранение на данни да са свързани към устройство за непрекъсваемост на ел. снабдяването.
2. При липса на ел. захранване за повече от 10 мин., администратора започва процедура по поетапно спиране на сървърите.
3. При срив в локалната компютърна мрежа, всеки потребител следва да запише файловете, които е отворил на локалния си компютър, за да се избегне загуба на информация. При възстановяване на мрежата, всички локално запазени файлове следва да се преместят отново на сървъра и да се изтрият локалните копия.

РАЗДЕЛ VII

СЪЗДАВАНЕ НА РЕЗЕРВНИ КОПИЯ

Чл. 43. Всеки служител на РЗИ-Сливен е длъжен да създава резервни копия на документацията която изготвя или съхранява.

Чл. 44. Информацията, включително тази, съдържаща лични данни, се архивира по следния начин:

(1) Архивирането на данните се извършва по начин, който позволява, при необходимост данните да бъдат инсталирани на друг сървър/ компютър и да се продължи работният процес без чувствителна загуба на данни;

(2) Базите данни на всички програми се архивират всеки месец.

(3) Резервните копия се съхраняват на носител, различен от този, на който са разположени данните или електронните документи.

(4) Съхраняват се най-малко последните три резервни копия.

РАЗДЕЛ VIII

Управление на инциденти с мрежовата и информационната сигурност

Чл. 45. (1) В тези вътрешните правила се регламентират всички дейности при обработката на сигнали и реакция при инциденти.

(2) Вътрешните правила по ал. 1 съдържат:

1. реда за подаване на сигнали за настъпили или потенциални събития, оказващи негативно влияние върху мрежовата и информационната сигурност;
2. информация за лицата, отговорни за регистъра на инцидентите;
3. реда за регистриране на сигнала, проверката на неговата достоверност, класифицирането му, приоритизирането му и последващото уведомяване за това на подателя;
4. реда за уведомяване за инцидента (функционална и йерархична ескалация);
5. реда за подаване на информация за начина за разрешаване на инцидента;
6. реда за приключване на инцидента;
7. процеса за събиране, съхраняване и предаване на доказателства, когато инцидентът предполага извършването на процесуални действия срещу лице или организация, включително необходимите за това записи;
8. правата на достъп до регистъра на инцидентите.

(3) Субектът разработва, проверява и поддържа в актуално състояние планове за справяне с инцидентите, които биха имали най-сериозно въздействие върху мрежовата и информационната сигурност. Плановете съдържат информация за:

1. отговорника за организацията при настъпване на инцидент;
2. реда за информиране;
3. мерките, които следва да се предприемат и отговорното за това лице;
4. реда за консултиране;
5. реда за следене на параметрите по време на инцидента;
6. лицето, което ще събира и съхранява необходимата информация, и др.

(4) Субектът разработва стратегия за комуникация, която определя реда за споделяне на информацията за инцидента със служители, партньори, доставчици, клиенти, медии, държавни органи.

РАЗДЕЛ IX

РЕД ЗА ДОКЛАДВАНЕ

Всеки служител, който има съмнение за инцидент с мрежовата и информационната сигурност в РЗИ-Сливен незабавно докладва на прекия си ръководител и на главния секретар – Деян Петров на Инспекцията, както и на председателя на комитета по информационна сигурност д-р Николина Иванова – зам.-директор РЗИ-Сливен при тяхно отсъствие на Диман Тачев – главен експерт, д-я "АПФСО", като не прави никакви опити за отстраняване на проблема сам.

Посочените лица се свързват с лицето с което РЗИ-Сливен има сключен договор за поддръжка на компютърни системи и периферни устройства, като обяснява за настъпилата ситуация и осигурява достъп до помещението, където е проблема.

Във времеви диапазон **2 часа** от възникване на инцидент Деян Петров или Диман Тачев при отсъствие на друг член на комитета за информационна сигурност в РЗИ-Сливен докладват на Националният център/екип за реакция при инциденти в компютърната сигурност на адрес cert@govcert.bg, като използва формата за докладване за инцидент – Приложение 7 към чл. 31, ал 2 на НМИМИС., тел. 02 949 2212, 0878 908

РАЗДЕЛ X

ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

§ 1. Ръководителите и служителите в РЗИ-Сливен са длъжни да познават и спазват разпоредбите на тези правила.

§ 2. Контролът по спазване на правилата се осъществява от главния секретар на РЗИ-Сливен и директорите на дирекции в инспекцията.

§ 3. Настоящите вътрешни правила се разглеждат и оценяват периодично с оглед ефективността им, като РЗИ-Сливен може да приема и прилага допълнителни мерки и процедури, които са целесъобразни и необходими с оглед защитата на информацията получени с указателни писма от ДАЕУ или Министерство на здравеопазването.

§ 4. Тези правила са разработени съгласно Наредбата за минималните изисквания на мрежова и информационна сигурност, обн.ДВ.бр.59/ 26.06.2019г.