РЕПУБЛИКА БЪЛГАРИЯ
Министерство на околната среда и водите
Регионална инспекция по околната среда и водите – Стара Загора

ЗАПОВЕД

№ РД-08-29

Стара Загора, 14.02.2023 г.

На основание чл.6, ал.1, т.1 от Правилника за устройството и дейността на Регионалните инспекции по околната среда и водите и чл.5 ал. т. 6 от Наредба за минималните изисквания за мрежова и информационна сигурност

I.УТВЪРЖДАВАМ

Вътрешни правила за мрежова и информационна сигурност. Кибер сигурност

II.ОПРЕДЕЛЯМ:

Длъжностно лице за служител по информационни технологии Старши експерт, направление "Специализирани регистри" при дирекция „Превантивна дейност“, който да отговаря за мрежовата и информационна сигурност.

Длъжностното лице изпълнява следните функции:

1. Ръководи дейностите, свързани с постигане на високо ниво на мрежова и информационна сигурност;
2. Участва в изготвянето на политиките за мрежова и информационна сигурност и документираната информация;
3. Следи за спазването на вътрешните правила и прилагането на законите, подзаконовите нормативни актове, международните стандарти, политиките и правилата за мрежовата и информационната сигурност;
4. Ръководи периодичните оценки на рисковете за мрежовата и информационната сигурност;
5. Периодично, но не по-малко от веднъж годишно, прави преглед за състоянието на мрежовата и информационната сигурност в РИОСВ – Стара Загора, изготвя доклад за извършения преглед и го предоставя на директора на РИОСВ – Стара Загора;
6. Организира проверки за актуалността на плановете за справяне с инцидентите и плановете за действия в случай на аварии, природни бедствия или други форсмажорни обстоятелства като анализира резултатите от тях и организира изменение на плановете, при необходимост;
7. Поддържа връзки с други администрации, организации и експерти, работещи в областта на информационната сигурност;
8. Следи за точното водене на регистъра на инцидентите;
9. Уведомява за инциденти съответния секторен екип за реагиране при инциденти с компютърната сигурност в съответствие с изискването на чл. 31, ал. 1 от НМИМИС;
10. Организира анализ на инцидентите с мрежовата и информационната сигурност за откриване на причините за тях и предприемане на мерки за отстраняването им с цел намаляване на еднотипните инциденти и намаляване на загубите от тях;
11. Следи за актуализиране на използвания софтуер;

12. Следи за появата на нови Кибер заплахи (вируси, зловреден код, спам, атаки и др.) и предлага адекватни мерки за противодействието им;

13. Прави редовни прегледи на достъпите, но не по-рядко от веднъж в годината; при тези прегледи се установява дали всички, на които е даден достъп до мрежата, до отделните системи и/или приложения, имат право на него в съответствие със служебните им задължения, дали външни лица имат достъп и какъв е той (бивши служители, представители на трети страни) и предприема действия за извършване на необходимите промени;

14. Предлага за дисциплинарно наказание, служителите нарушили мерките за мрежова и информационна сигурност;

Всички служители се задължават да оказват съдействие на служителя, отговарящ за мрежовата и информационна сигурност за отстраняване на възникнали проблеми, диагностика и поддръжка на системите.

ДИАНА ИСКРЕВА-ИДИГО
Директор на РИОСВ – Стара Загора

УТВЪРЖДАВАМ:

Диана Искрева-Идиго

Директор на Регионална инспекция

по околната среда и водите – Стара Загора

ВЪТРЕШНИ ПРАВИЛА

ЗА МРЕЖОВА И ИНФОРМАЦИОННА СИГУРНОСТ.

КИБЕР СИГУРНОСТ.

1. Общи положения.

(1) Киберсигурност е състояние на обществото и държавата, при което чрез прилагане на комплекс от мерки и действия киберпространството е защитено от заплахи, свързани с неговите независими мрежи и информационна инфраструктура или които могат да нарушат работата им.

(2) Киберсигурността включва мрежова и информационна сигурност, противодействие на киберпрестъпността и киберотбрана.

(3) Мрежова и информационна сигурност е способността на мрежите и информационните системи да се противопоставят на определено ниво на въздействия, засягащи отрицателно наличието, истинността, целостта или поверителността на съхранявани, пренасяни или обработвани данни или на свързаните с тях услуги, предлагани от тези мрежи и информационни системи или достъпни чрез тях.

2. Целите на настоящите правила:

(1) прилагане на мерки за защита от кибератаки;

(2) осигуряване на непрекъснатост на работните процеси;

(3) минимизиране на рисковете за сигурността и интегритета на информацията, причинени от загуба на данни или външна намеса;

(4) информиране на служителите за техните отговорности и задължения по отношение на информационната сигурност;

(5) осигуряване на съответствие с нормативните изисквания.

3. Обхват на системата за управление на информационната сигурност

Управлението на информационната сигурност обхваща всички електронни документи, както и:

(1) бази данни и регистри;

(2) софтуерни активи;

(3) локална мрежа;

(4) всички WEB базирани и други информационни системи;

(5) носители на информация (дискови масиви, дискове, USB памети и др.);

(6) комуникационни устройства;

(7) инфраструктура (електрозахранване, кабели за локална мрежа и др.);

(8) служители;

4. Приоритети:

(1) създаване на условия служителите да бъдат информирани и да осъзнават проблемите на информационната сигурност;

(2) спазването на политиката по сигурността и евентуалните недостатъци в системата за информационна сигурност да бъдат докладвани;

(3) информационните ресурси да бъдат защитавани от гледна точка на изискванията за конфиденциалност, интегритет и достъпност;

(4) въвеждането и спазването на политиката по информационна сигурност;

(5) превенция при използването на информацията и системите на инспекцията без оторизация или за цели, които не са свързани с дейността й.

5. Отговорности:

Ръководството:

- планира необходимите ресурси за осигуряване на информационната сигурност;
- координира прилагането на мерки за защита и информационна сигурност;
- упражнява контрол върху нивото на мрежова и информационна сигурност чрез организирането на одити по смисъла на чл. 35, ал. 1, т.1 и 3 за доказване на съответствието на предприетите мерки.

Потребители:

- потребителите на информационни системи, се задължават да следват процедурите, инструкциите и заповедите, свързани с информационната сигурност и да докладват за проблеми и инциденти в информационната система; - всеки служител отговаря за целостта на предоставената му компютърна и периферна техника и инсталирания софтуер;
- служителите, извършващи въвеждане и актуализация на данните са длъжни да ги поддържат в актуално състояние и носят отговорност за съответствието им с използваните оригинали или за тяхната достоверност, в случай че те са първоизточник на данните.

Системни администратори (служителите по информационна сигурност):

- подготвят работните станции за работа. Инсталират антивирусна защита и софтуер, необходим за изпълнение на служебните задължения;
- архивират информацията и съхраняват копията в помещения, различни от тези, в които са разположени сървърите.

6. Оценка и управление на риска за мрежовата и информационна сигурност

(1) Рискът за сигурността е фактическо състояние, което създава заплахи за уязвяване на един или няколко информационни актива, което да предизвика тяхното повреждане или унищожаване. Оценката на риска се прилага към цялата информационна система и включва приложения, сървъри, мрежа, всеки процес или процедура, чрез които системата се администрира и/или поддържа.

(2) Действия по оценка и управление на риска:

Заплахите за мрежовата и информационната сигурност се класифицират по следните критерии:

- достъпност, цялостност, конфиденциалност;
- апаратура, софтуер, данни, поддържаща инфраструктура;
- случайни/преднамерени действия;
- от природен/технологичен характер и др.

При идентифициране на риск се предприема едно от следните действия:

- ликвидиране на риска, чрез отстраняване на причиняващите го обстоятелства;
- намаляване на риска и смекчаване на последствията, чрез използване на допълнителни защитни средства.

Заплахите срещу мрежовата и информационната сигурност, могат да бъдат:

- достъп до служебна информация, чрез прихващане на електронни съобщения;
- нежелан код, който може да доведе до загуба на конфиденциалност. Той може да се използва, за да се заобиколи проверка за достоверност, както и всички защитни функции, свързани с нея. В резултат кода може да доведе до загуба на достъпността, ако данните или файловете са разрушени;
- осъществяване на нерегламентиран достъп, чрез компрометиране (записване и разкриване) на пароли и до нарушаване на интегритета при интервенции от трети лица;
- софтуерни грешки могат да застрашат конфиденциалността, ако грешка в софтуера осигури възможност за нежелан достъп до информационна система;
- нерегламентиран достъп до компютри, информационни ресурси, услуги и приложения може да доведе до разкриване на данни и до нарушаване интегритета на тези данни, ако нерегламентираната им промяна е възможна. Нерегламентираният достъп до компютри, данни, услуги и приложения може да наруши достъпността до данните, ако тяхното изтриване или заличаване е възможно;
- нерегламентиран достъп до носител на данни може да застраши съхраняваните върху него данни;

- повреждане на носител на информация може да наруши интегритета и достъпността до данните, които се съхраняват на този носител;

- аварии в електрозахранване и климатични инсталации могат да доведат до нарушаване на интегритета и достъпността до данни, ако вследствие на настъпването на авариите са увредени информационни системи или носители на данни;

- технически аварии (например аварии в мрежите) могат да нарушат интегритета и достъпността до информация, която се съхранява или разпространява чрез тази мрежа; - грешки при предаването на информацията могат да доведат до нарушаване на нейната цялост и достъпност;

- употреба на нерегламентирани програми и информация могат да нарушат интегритета и достъпността до данните, съхранявани и разпространявани чрез информационната система, в която е настъпило такова събитие. Програмите и информацията може да съдържат нежелан код и да се използват, за да се изменят съществуващи програми и данни по неразрешен начин;

- потребителски грешки могат да нарушат интегритета и достъпността до данни чрез неумишлено или умишлено действие;

- аварии в комуникационното оборудване и услуги могат да увредят достъпността на данните, предавана чрез тези услуги;

- външни въздействия с огън, вода, химикали и др. могат да доведат до увреждане или унищожаване на информационното и комуникационно оборудване;

- природни бедствия могат да доведат до унищожаване на данни и информационни системи.

- претоварване на комуникационния канал може да доведе до нарушаване бързодействието и достъпността до обменяните данни.

7. Управление на достъпа и защита срещу неправомерен достъп

(1) Защитата на системните ресурси и на информационни системи на РИОСВ – Стара Загора се регулира като до тях се осигурява достъп само на упълномощени лица. С това се цели предотвратяването на нерегламентирания достъп до ресурсите от външни лица.

(2) Чрез логическо управление на достъпа се определят допустими операции и идентификация за всеки ползвател. Достъпът на служителите до локалната мрежа се осъществява чрез потребителско име и парола;

(3) При назначаване на нов служител - директора на съответната дирекция предоставя информация за необходимите информационни и комуникационни ресурси и

достъпи, които трябва да бъдат предоставени на служителя. На основание на заявката се извършват необходимите настройки на работната станция. Създават се потребителски имена и пароли за работа в компютърната мрежа, информационните системи и приложения, които са необходими на служителя, за изпълнение служебните си задължения.

(4) Служителите са длъжни да не споделят своите пароли да достъпи с трети лица. При съмнение за компрометиране на паролата са длъжни своевременно да променят паролата си и да уведомят лицето по мрежова и информационна сигурност.

(5) При промяна на служебните задължения на служител - директорът на съответната дирекция предоставя информация за необходимите информационни и комуникационни ресурси и достъпи, които трябва да бъдат предоставени, ограничени или напълно прекратени. На това основание се извършват промени по достъпа на потребителския профил за работа в компютърната мрежа, информационните системи и приложения, които са необходими на служителя за изпълнение служебните му задължения.

(6) При прекратяване на служебно/трудово правоотношение, директорът на дирекция АФПД в РИОСВ – Стара Загора уведомява за това отговорните лица и с изтичане на последния работен ден с протокол се прекратява правото на достъп на лицето до мрежови ресурси, информационни системи, приложения и работна станция.

(7) На служителите, които използват електронни бази данни и техни производни (текстове, разпечатки, карти, скици и други) се забранява:

- да ги използват извън рамките на служебните си задължения;
- да ги предоставят на външни лица, извън предвидения в ЗДОИ процедура и ред;
- да нарушават целостта на данните, чрез вписване на невярна информация в бази данни или унищожаване и повреждане на файлове.

(8) Като лице, носещо пряка отговорност за мрежовата и информационна сигурност (МИС) в администрацията, директорът на РИОСВ – Стара Загора може да разпорежда предоставяне, ограничаване или прекратяване на достъп до мрежови ресурси, информационни системи и приложения по собствена преценка и във връзка с „принципа на най-малката привилегия“ (PoLP), извън хипотезата на чл. 7, т.3, т.5 и т.6 от настоящите вътрешни правила.

8. Защита срещу нежелан софтуер

(1) Нежеланият софтуер, който може да уязви един или няколко информационни актива и да предизвика смущаване на нормалната им работа, увреждане или унищожаване, включва следните видове:

- компютърни вируси;

- мрежови червеи;
- троянски коне;
- логически бомби.

(2) Защитата срещу нежелан софтуер в РИОСВ – Стара Загора е организирана в следните направления:

- на всички работни станции се инсталира утвърдения корпоративен антивирусен софтуер;
- всяко устройство, което се включва в мрежата, е необходимо да се проверява за вируси преди да получи достъп до ресурсите на мрежата;
- преди работа с външни носители (дискети, флаш-памет, оптичен диск и други) служителите на съответното работно място задължително ги сканират за наличие на компютърни вируси и злонамерен код;
- забранява се инсталиране и използване на нерегламентиран софтуер;
- забранява се отварянето на получени по електронна поща съобщения, които съдържат изпълними файлове или такива, които могат да предизвикат промени в системната конфигурация, напр. файлове с разширения *.exe, *.vbs, *.reg;
- при проверка на електронната поща служителите трябва да бъдат внимателни с прикачените файлове и линкове. Необходимо да се следва процедура за идентифициране автентичността на посланието и неговия източник:
  - Източникът известен ли е и регистриран ли е като такъв?
  - Съдържа ли „странна“ информация, която изглежда погрешна?
  - Адресът на източника познат ли е и включен ли е в списъка с контакти?
  - Да се провери пълната заглавна част на посланието.
  - Подателят автентичен ли е, логично ли е да изпраща подобен прикачен файл?
  - При съмнение да се провери подателят, като поиска помощ от отговорно лице.
  - При съмнение да не се отварят линкове и да не се сваля никакъв софтуер.
  - Ако е изпратен линк, първо се копира и проверява на сайт за сканиране за вируси (например: https://virusdesk.kaspersky.com/, https://www.urlvoid.com/ https://transparencyreport.google.com/safe-browsing/search?hl=en и други).

(3) При установяване на открити опити за проникване трябва незабавно:

- да се уведомяват отговорните лица за предприемане на мерки;
- да се изключват или ограничават мрежовите услуги, свързани с обекта на проникването.

9. Мониторинг

(1) При настъпване на събития и инциденти, свързани с информационните системи в РИОСВ – Стара Загора, се създават следните записи:

- дата и час на настъпване на събитието;
- име на ползвателя - инициатор на действието;
- тип на събитието;
- резултат от събитието;
- източник на събитието;
- списък на засегнатите обекти;
- описание на измененията в системата, произтекли от събитието.

10. Физическа сигурност и защита от околната среда

В РИОСВ – Стара Загора се прилагат следните мерки за физическата защита на информационните системи и ресурси:

(1) Управление на физическия достъп:

- физическият достъп до помещенията, в които е разположено техническото и комуникационното оборудване се извършва от или в присъствие на служители на РИОСВ – Стара Загора или на служители на РЛ – Стара Загора;
- изнасянето на информационните активи извън сградата се извършва с разрешение
- от Директора на инспекцията и/или директора на дирекция АФПД;
- служебна информация не се оставя без надзор или контрол, което означава и видима на екран;
- всяко устройство се маркира с инвентарен номер.

(2) защита на поддържащата инфраструктура:

- сървърите и работните станции са разположени в помещение с климатизация;
- сървърите и работните станции са разположени в заключващи се помещения;
- при възможност сървърите са свързани с непрекъсваемо токозахранване, подсигуряващо работата им, в случай на неизправност в електрическата мрежа или внезапно отпадане на напрежението поради авария.

11. Сигурност, свързана със служителите

(1) Мерки за постигане сигурност по отношение на персонала:

За постигане на мрежова и информационна сигурност по отношение на персонала се предприемат следните мерки за идентификацията на служителите и оправомощаването им да извършват действия по отношение експлоатацията на информационните системи:

- достъпът на служителите до локалната мрежа и работните станции се осъществява чрез служебно потребителско име и парола;
- достъпът на служителите до специализираните информационни системи се осъществява чрез служебно потребителско име и парола;
- работният плот на всяка работна станция е персонализиран според работата на конкретния потребител;
- създадена е връзка към директории на файловия сървър, в които са разположени всички необходими файлове при ежедневната работа на експертите. Всеки служител е с принадлежност към профил, съответстващ на служебните му задължения;
- служителите са с права за достъп до ресурсите и информационните системи с минимални привилегии;
- достъпът до системите на други администрации е само доколкото е необходим за изпълнение на служебните им задължения;
- при необходимост от временно спиране на сървърното оборудване се спазва концепцията "Позиция на безопасно спиране". Системите преустановяват работата си безопасно и се предотвратява неочакваното спиране на работа.

12. Вътрешна организация на информационната сигурност

(1) В РИОСВ – Стара Загора се провежда политика за координиране на цялата дейност в организацията по внедряването и поддържането на мерките за защита, което включва:

- защита на активите;
- поддръжка на ключови ресурси – мрежа и сървъри;
- закупуване, изменения и поддръжка на софтуерните ресурси и хардуерни компоненти;

(2) С цел защита на информационната сигурност на потребителите се забраняват:

- действия, които могат да доведат до проблеми със сигурността или работоспособността на външни мрежи, като например: действия, свързани със сканиране на портове на сървъри и/или мрежи, изпращане на множество заявки към сървър, с цел претоварването му, опити за преодоляване на защитни механизми на сървъри и/или мрежи и др.;
- възпрепятстване изпълнението на ъпдейтите на операционната система и приложния софтуер;
- злоупотреба с ресурси и претоварването на комуникационния канал (в това число гледане на онлайн клипове, филми и телевизия и онлайн развлекателни игри), което може да доведе до недостъпност на данни и услуги и да попречи на останалите потребители на локалната мрежа за изпълнението на служебните им задължения;
- теглене или изпращане по интернет на обемна информация, която не е свързана със служебните задължения – филми, музика, снимки и др.

- изтеглянето и инсталирането на нелегален, нелицензиран и/или несвързан с изпълнението на служебните задължения софтуер;

- съхраняване на информация с неслужебен характер (файлове с текст, изображения, видео и аудио) в директория на файловия сървър на РИОСВ – Стара Загора (в т.ч. в папка „Документи");

- да се предприемат действия от служителите с намерение да се разрушат, да се направят негодни или по друг начин да се отнеме възможността на други потребители да използват компютърните ресурси, както и действия, увреждащи целостта и сигурността на съхраняваните програми, служебна информация и данни.

(3) Профили с администраторски права се създават само на служители, които извършват административни операции (инсталиране, конфигуриране, управление, поддръжка и др.) съгласно чл. 17, ал. 1, т.4 на НМИМИС.

(4) Паролите за оторизация на профилите създадени по т. 3 се сменят задължително периодично – май-малко веднъж в годината, съгласно чл. 17, ал.2, т. 1.

13. Управление на активите

(1) Управлението на активите се отнася до служителите и до цялото информационно оборудване, собственост на РИОСВ – Стара Загора. Системите, свързани с интернет, локална мрежа, включително компютърното оборудване, приложния софтуер, операционните системи, средствата за съхранение на информация, електронните пощи и други са собственост на РИОСВ – Стара Загора. Тези системи са предназначени да се използват за целите на дейността и в интерес на инспекцията.

(2) Данните, които потребителите обработват и съхраняват при изпълнение на служебните си задължения са собственост на РИОСВ – Стара Загора.

(3) За целите на сигурността и поддръжката на мрежата, отговорното лице може да наблюдава оборудването, системите и мрежовия трафик по всяко време.

(4) Деинсталират 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, платени и безплатни програми, и др.

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

14.Разработване, внедряване и поддържане на информационните системи

Разработването и внедряването на информационни системи се предхожда от анализ за необходимостта от тях, както и от ясно и конкретно дефиниране на процесите, които съответните системи предстои да обслужват.

15. Управление на инциденти и подобряване на сигурността на информацията

В РИОСВ – Стара Загора следва да се събират данни и да се извършва анализ на вида и броя на инцидентите. Целта е да се идентифицират повтарящите се инциденти или инцидентите с голямо влияние, да се ограничат честотата, щетите и загубите от появата им в бъдеще.

16. Придобиване и ползване на лицензи

(1) Лицензите за ползване на операционни системи и приложен софтуер се поддържат от Интегрирана система за лицензите в държавната администрация (ИСЛА), достъп до която се осъществява посредством потребителско име и парола.

(2) Компютрите на РИОСВ – Стара Загора, използват лицензиран софтуер и са защитени от вируси с корпоративна антивирусна защита. Забранява се на потребителите да внасят софтуер отвън и да го инсталират на своите компютри.

17. Заключителни разпоредби

Служителите на РИОСВ – Стара Загора се задължават да спазват всички вътрешни актове, издадени във връзка с информационната сигурност.

Всеки служител, който прецени, че има злоупотреба с настоящите правила, уведомява незабавно прекия си ръководител или длъжностното лице отговарящо за мрежова и информационна сигурност в РИОСВ – Стара Загора.

$ 1. Вътрешните правила за мрежова и информационна сигурност, кибер сигурност в РИОСВ – Стара Загора са разработени в съответствие с Наредбата за минималните изисквания за мрежова и информационна сигурност.

$ 2. Вътрешните правила за мрежова и информационна сигурност РИОСВ – Стара Загора могат да бъдат изменяни при настъпили промени в нормативната база.

$ 3. Правилата важат за всички служители на РИОСВ – Стара Загора, като те задължително се запознават с тях.

$ 4. Настоящите вътрешни правила са утвърдени съгласно Заповед № РД – 08 – 29 от 14.02.2023 г.