Утвърдени :

със Заповед № РД-11-634/20.12.19г.

на Директора на Областна дирекция „Земеделие“ Бургас

Лидия Станкова

ВЪТРЕШНИ ПРАВИЛА

ЗА
МРЕЖОВА И ИНФОРМАЦИОННА СИГУРНОСТ В
ОБЛАСТНА ДИРЕКЦИЯ „ЗЕМЕДЕЛИЕ“ БУРГАС

гр. Бургас 8000, ул. "Цар Иван Шишман" № 8
Тел: (+35956) 84 43 03, Факс: (+35956) 84 43 03

РАЗДЕЛ I
ОБЩИ ПОЛОЖЕНИЯ

Чл.1.(1) С настоящите Вътрешни правила за мрежова и информационна сигурност, наричани по-долу „Правилата“, се определят необходимите технически и организационни мерки за защитата на информационните мрежи и системи, както и информационния обмен между тях в Областна дирекция „Земеделие“ Бургас, наричана по-долу „Дирекцията“ и в териториалните и звена Общински служби по земеделие, наричани по-долу „Общинските служби“.

(2) Правилата са разработени в съответствие със Закона за киберсигурност, Наредбата за общите изисквания за мрежова и информационна сигурност, наричана по-долу НОИМИС, както и със Закона за електронното управление, Закона за електронната идентификация, Закона за електронните съобщения, Наредбата за електронните административни услуги и други.

Чл.2. (1) Правилата са част от политиката за мрежова и информационна сигурност на Дирекцията и целят защитата на информационните мрежи и системи срещу неправомерен или случаен достъп, използване, правене достояние на трети лица, промяна или унищожаване, доколкото такива събития или действия могат да нарушат достъпността, автентичността, целостта, интегритета и конфиденциалността на съхраняваните или предаваните данни, а също така на предоставяните електронни услуги, свързани с тези мрежи и системи.

(2) Дирекцията предприема необходимите технически и административни мерки за защита на информационните мрежи и системи, съобразно спецификата на административните процеси. Решенията за мрежова и информационна сигурност се изграждат за осигуряване на всяко от следните нива:

1. мрежи;
2. системи;
3. приложения;
4. информация.

(3) За всяко от нивата по ал.2 се осигурява съответният контрол с цел да се обезпечи адекватно ниво на сигурност, като се прилагат разписаните принципи в НОИМИС.

РАЗДЕЛ II
ОРГАНИЗАЦИЯ НА МРЕЖОВАТА И ИНФОРМАЦИОННА СИГУРНОСТ

Чл.3.(1) Директорът отговаря за мрежовата и информационна сигурност в Дирекцията и Общинските служби, като взема необходимите документирани решения, чрез утвърждаването на политики, правила, процедури и други, както и чрез осигуряване на необходимата инфраструктура за гарантиране на мрежовата и информационна сигурност на използваните информационни мрежи и системи.

(2) Отговорностите на служителите за гарантиране на мрежовата и информационна сигурност на използваните информационни мрежи и системи се определят в длъжностните им характеристики или работни планове, както и на друго документирано основание.

(3) Директорът определя звено, отговарящо за мрежовата и информационна сигурност в Дирекцията и Общинските служби, на пряко негово подчинение. Функциите на звеното, отговарящо за мрежовата и информационната сигурност са разписаните в НОИМИС.

(4) Директорът възлага на Главния секретар контрола по изпълнението на взетите документирани решения за гарантиране на мрежовата и информационна сигурност на използваните информационни мрежи и системи.

(5) Директорът организира комплексни проверки за оценяване степента на постигнатата мрежова и информационна сигурност в използваните в Дирекцията и Общинските служби информационни мрежи и системи.

РАЗДЕЛ III
ОЦЕНКА И УПРАВЛЕНИЕ НА РИСКА

Чл.4.(1) С настоящите Правила се определят основните действия по оценка и управление на риска за мрежовата и информационна сигурност в Дирекцията и Общинските служби, както и идентифициране на потенциалните рискови фактори във връзка с нея.

(2) Рискът за сигурността се определя като фактическо състояние, създаващо заплахи за уязвяване на един или няколко информационни актива, което предизвика тяхното повреждане или унищожаване.

(3) Оценката на риска се определя чрез изчисление на вероятността за уязвяване въз основа на ефективността на съществуващите или планираните мерки за сигурност.

(4) Действията по управление на риска обхващат оценка на неговия размер, изработване на ефективни и икономични мерки за неговото снижаване и оценка дали резултативният риск е в приемливи граници. Управлението на риска се извършва чрез последователно прилагане на два типа периодично повтарящи се действия:

1. оценка (преоценка) на риска;
2. избор на ефективни и икономични средства за неговата неутрализация.

Чл.5. При идентифициране на риска се предприема едно от следните действия:

1. ликвидиране на риска, чрез отстраняване на причиняващите го обстоятелства;
2. намаляване на риска, чрез използване на допълнителни защитни средства;
3. приемане на риска и разработване на план за действия в обстановка на риск;

Чл.6.(1) Процесът на управление на риска включва следните етапи:

1. избор на анализируемите обекти и ниво на детайлизация на анализа;
2. избор на методология за оценка на риска;
3. идентификация на информационите активи;
4. анализ на заплахите и последствията от тях, откриване на уязвимите места в защитата;
5. оценка на рисковете;
6. избор на защитни мерки;
7. реализация и проверка на избраните мерки;
8. оценка на резултативния риск.

(2) Процесът на управление на риска следва периодичност, като последният етап е

нов цикъл на оценка, който се провежда:

1. ако резултативния риск е определен като неудовлетворителен;
2. с определената ежегодна периодичност.

Чл.7.(1) Заплахите за мрежовата и информационната сигурност се класифицират по следните критерии:

1. по елементите на мрежовата и информационната сигурност - достъпност, автентичност, целостта, интегритет и конфиденциалност, към които са насочени;
2. по компонентите на информационната система - апаратура, софтуер, данни, поддържаща инфраструктура, към които са насочени;
3. по начина на осъществяване - случайни или преднамерени действия, от природен или технологичен характер и други;
4. по разположението на източника - вътре или извън информационната система.

(2) Потенциалните рискови фактори за мрежовата и информационната сигурност, които могат да застрашат достъпността, автентичността, целостта, интегритета и конфиденциалността, са както следва:

1. подслушване и електромагнитно излъчване;
2. нежелан код и маскиране на потребителската идентичност;
3. погрешно насочване или пренасочване на съобщенията, както и липса на потвърждаване;
4. софтуерни грешки;
5. нерегламентиран достъп до информационните активи, повреждане, кражба и злоупотреба с тях;
6. грешки при поддръжката;
7. грешки при предаването на информация;
8. употреба на нерегламентирани програми и информация;
9. потребителски грешки;
10. претоварване на комуникационния трафик;
11. технически аварии и аварии в комуникационното оборудване, аварии в електрозахранването и климатичните инсталации, природни бедствия и външни въздействия с огън, вода, химикали и други.

Чл.8.(1) Идентифицирането, оценката и действията по управление на риска за мрежовата и информационна сигурност се осъществяват от звеното, отговорящо за мрежовата и информационна сигурност.

(2) Чрез оценката на риска за мрежовата и информационна сигурност се цели идентифицирането на неприемливите опасности, за които се налага да бъдат предприети съответните действия, както и върху опасностите, които са на приемливо ниво, за да се упражни контрол същите да останат в тези граници.

(3) Съобразно резултатите от извършената оценка звеното, отговарящо за мрежовата и информационна сигурност избира реакция по отношение на всеки от рисковете като определя контролните цели и действия, които се вписват в План за действие. Броят и обхвата на контролните цели и действия следва да е достатъчен, за да даде увереност, че неприемливите рискове за мрежовата и информационна сигурност са ограничени до приемливи нива.

РАЗДЕЛ IV
ИНВЕНТАРИЗАЦИЯ НА ИНФОРМАЦИОННИТЕ АКТИВИ

Чл.9.(1) Предприемат се необходимите действия за създаване и поддържане на инвентарни списъци на наличните информационни активи в Дирекцията и Общинските служби.

(2) За инвентарен списък се считат вписаните данни в регистъра на информационните ресурси, воден от Държавна агенция „Електронно управление".

(3) Информационни активи са:

1. хардуерните устройства;
2. софтуерните продукти;
3. информационните системи;
4. комуникационната инфраструктура.

Чл.10. В картите на наличните информационни ресурси в Дирекцията и Общинските служби се определят еднозначно:

1. конкретен служител отговаря за конкретни информационни ресурси - работни станции, устройства, софтуерни продукти, информационни системи, бази данни и други;
2. конкретен софтуерен продукт, информационна система и база данни се използват на конкретни работни станции и устройства.

Чл.11. Инвентарните списъци за наличните информационни ресурси в Дирекцията и Общинските служби включват минималния набор от данни разписан в НОИМИС.

Чл.12. Според мястото и начина на поддръжка информационните системи в Дирекцията и Общинските служби са:

1. разположени на локални работни станции;
2. разположени на сървъри в локалната мрежа;
3. разположени на външни сървъри;
4. външни системи, в които се поддържа информация от служителите на Дирекцията и Общинските служби;
5. външни системи, ползвани от служителите със специални права.

Чл.13.(1) По отношение на информационните активи в Дирекцията и Общинските служби се спазват следните правила:

1. върху работните станции и сървърите се инсталират само софтуерни продукти, за които Дирекцията разполага с лиценз за ползване;
2. исталирането и настройката на нови софтуерни и хардуерни продукти се планира и всички лица, използващи засегнатите ресурси се уведомяват не по-малко от 3 дни преди извършване на инсталацията или настройката;
3. преди извършване на инсталация се правят резервни копия на софтуера, файловете и базите данни, като се разработи и „roll back" план;
4. инсталирането, настройката и поддръжката на нови софтуерни и хардуерни продукти се извършват в периоди с минимално натоварване на съответните ресурси;
5. преди инсталиране в оперативно действащите системи на нови софтуерни и хардуерни продукти те се тестват в тестова среда максимално близка до реалните работни условия.

(2) Информационните ресурси се получават от служителите, които ги използват,

срещу подпис върху документ, съдържащ пълното описание на устройствата и инсталирания софтуер.

РАЗДЕЛ V
УПРАВЛЕНИЕ НА ДОСТЪПА

Чл.14.(1) Средствата за управление на достъпа в Дирекцията и Общинските служби позволяват да се определят и контролират действията, които различни ползватели могат да извършват по отношение на информационните ресурси.

(2) Средствата за управление на достъпа на участниците в електронния обмен включват три категории функции:

1. административни - създаване и съпровождане на атрибути за управление на достъпа;
2. спомагателни - обслужване на процесите на достъп на ползвателите;
3. информационни - събиране на информация за процесите на достъп с оглед подобряване на взаимодействието.

Чл.15.(1) Системният администратор и администраторите на информационни системи управляват идентификаторите на ползвателите на информационните системи и процеси чрез:

1. уникална идентификация на всеки ползвател;
2. верификация на идентификатора на всеки ползвател;
3. прилагане на процедурите за разпространение, заместване на загубени, компрометирани или повредени идентификатори, както и прекратяване на действието им;
4. архивиране на идентификаторите.

(3) Информационните системи скриват ехо изображението на идентифициращата информация в процеса на проверка на идентичността с цел да я защитят от възможно използване от страна на неоправомощени лица.

Чл. 16.(1) Достъпа до информационните активи на Дирекцията и Общинските служби се предоставя само на лица, придобили потребителски права. Потребители на информационните активи са всички ръководители, служители по служебно или трудово правоотношение, както и лицата, ползващи информационни ресурси на друго документирано основание.

(2) В зависимост от изпълняваните функции и права по отношение на информационните ресурси, се дефинират следните типове потребители:

1. системен администратор - служител на главна дирекция „АР“ или дирекция „АПФСДЧР“, на когото са възложени такива функции по длъжностна характеристика, в работен план или на друго документирано основание, следящ за нормалното функциониране на работните процеси на сървърите и комуникационните устройства. Отговаря и за своевременното създаване, изменение или прекратяване на различните типове потребителски акаунти и права на потребителите за работа в локалната мрежа на Дирекцията и Общинските служби;
2. администратори на информационни системи - служители на главна дирекция „АР“ и дирекция „АПФСДЧР“, отговорящи за своевременното създаване, изменение

или прекратяване на различните типове потребителски акаунти и права на потребителите за работа в информационните системи;

3. потребители с достъп до информационни ресурси с общо предназначение - ръководители, служители на главна дирекция „АР“ и Общинските служби, дирекция „АПФСДЧР“ и други лица, ползващи информационни ресурси на Дирекцията на друго документирано основание, с осигурен достъп от системния администратор;

4. потребители с достъп до информационни ресурси със специализирано предназначение - ръководители, служители на главна дирекция „АР“ и Общинските служби, дирекция „АПФСДЧР“, ползващи информационни ресурси на Дирекцията и външни такива, с осигурен достъп от администраторите на информационни системи.

Чл. 17.(1) Информацията за възникването, изменението и прекратяването на потребителските акаунти и права на потребителите се предоставя посредством одобрена от Г лавния секретар докладна на:

1. Главния директор на главна дирекция „АР“ за служителите в специализираната администрация и Общинските служби;

2. Директора на дирекция „АПФСДЧР“ за служителите на общата администрация.

(2) Докладната съдържа имената на служителя на кирилица и латиница, длъжността и мястото в йерархията на Дирекцията, както и специализираните информационни системи, до които следва да бъде предоставен, изменен или прекратен достъпа.

(3) В зависимост от типа потребител системният администратор или администраторите на информационни системи:

1. създават потребителски акаунт в инфраструктурата на Дирекцията и Общинските служби в срок до 1 работен ден от получаване на одобрената заявка за предоставяне на достъп;

2. правят промени в съществуващия достъп в срока по т.1;

3. блокират незабавно потребителския акаунт след одобрена заявка за прекратяване на достъпа за срок от 1 месец, след което същият се архивира, както и свързаната с него home папка.

Чл. 18.(1) Системата на потребителски акаунти в Дирекцията и Общинските служби включва:

1. акаунти за достъп до локалната мрежа и информационните системи с общо предназначение - персонална и споделени папки върху файлови сървъри, Internet, правно-нормативни системи и други.

а) потребителския акаунт се състои от потребителско име и парола за достъп;

б) потребителското име се състои от собственото име и фамилия на потребителя на латиница, като се допускат букви преди фамилията при съвпадение на имената;

в) паролата се генерира като 8-знаков буквено-цифров символен код, изискващ автоматична промяна на всеки 6 месеца;

2. акаунти за достъп до служебна електронна поща - официална и оперативна.

а) Дирекцията ползва официален e-mail адрес в домейна на Министерство на земеделието, храните и горите - odzg_burgas@mzh.government.bg и оперативен email адрес - zemedelie@odzburgas.com

б) Общинските служби ползват e-mail адреси в @abv.bg с формирана първа част по аналогия с този на Дирекцията;

в) паролата се генерира като 8-знаков буквено-цифров символен код, изискващ автоматична промяна на всеки 6 месеца или при отпадане на основанията на ползване на потребителски права;

3. акаунти за достъп до специализирани информационни системи.

а) за тези разположени на работни станции и в локалната мрежа, и администрирани от Дирекцията се прилагат правилата по т.1;

б) за останалите разположени на външни сървъри или изобщо външни системи, администрирани от други институции - съобразно вътрешните им правила;

в) и в двата случая - на буква а) и б), паролата се сменя задължително от потребителя след нейното предоставяне.

(2) По отношение на системата на потребителските акаунти и правата на потребителите в Дирекцията и Общинските служби се прилагат следните общи правила:

1. идентификаторите са персонални и служителите не могат да ги предоставят нерегламентирано;

2. загубени, компрометирани или повредени идентификатори подлежат на промяна след уведомяване на системният администратор или администраторите на информационни системи съобразно типа потребител;

3. действието на идентификатор се прекратява при липса на активност на потребител повече от 1 месец;

4. акаунтът се заключва при 3 последователни несполучливи опита на потребител за вход в информационната система;

5. архивната информация се записва и съхранява за срок от 1 година за потребителите с осигурен достъп до информационните системи, както и за всички лица, участвали в електронния информационен обмен.

Чл. 19.(1) Новите потребители с достъп до информационни ресурси преминават първоначален инструктаж относно ползването им, проведен от системния администратор или администраторите на информационни системи, съобразно типа потребител.

(2) Новите потребители се инструктират относно спазването на политиката за мрежова и информационна сигурност на Дирекцията, както и относно настоящите Правила от звеното, отговарящо за мрежовата и информационна сигурност.

(3) Новите потребители получават персоналните си идентификатори - потребителските имена и пароли лично.

Чл.20.(1) На главна дирекция „АР“ и дирекция „АПФСДЧР“ се предоставя общо дисково пространство на файловите сървъри на Дирекцията с определен лимит, което може да се ползва от служителите на съответната дирекция за споделяне на файлове.

(2) На всеки служител се предоставя лична папка на файловия сървър в локалната мрежа с определен лимит, върху който може да се съхранява служебна информация.

Чл.21.(1) Информацията, съхранявана от потребителите на файловите сървъри се архивира ежедневно.

(2) Системният администратор се грижи за изготвяне на резервни копия на важната информация, съхранявана върху работните станции на потребителите с периодичност,

позволяваща възстановяване на основните данни при хардуерен, софтуерен или потребителски срив.

Чл.22. Най-малко веднъж годишно се преглеждат и анализират правата на системния администратор и администраторите на информационни системи, както и правата за достъп на потребителите на информационни системи.

РАЗДЕЛ VI
ЗАЩИТА СРЕЩУ НЕПРАВОМЕРЕН ДОСТЪП

Чл.23.(1) Защитата на информационните ресурси на Дирекцията и Общинските служби е процес, при който използването им се регулира в съответствие с политиката за мрежова и информационна сигурност и настоящите Правила, позволено е само на документирано основание и включва предотвратяването на нерегламентиран достъп до ресурсите, включително предотвратяване на достъп до ресурсите по нерегламентиран начин.

(2) Управлението на защитата от нерегламентиран достъп в Дирекцията и Общинските служби се категоризира в няколко степени в зависимост от оценките на потенциалните последствия при нарушаване на достъпността, автентичността, целостта, интегритета и конфиденциалността, както следва:

1. ограничено - на информационните активи са причинени незначителни вреди, финансовите загуби са незначителни, а административните функции са с понижена ефективност;

2. умерено - на информационните активи са причинени значителни вреди и финансовите загуби са значителни, а ефективността на административните функции е съществено понижена;

3. високо - когато на информационните активи са причинени тежки вреди и финансовите загуби са много големи, а загубата на достъпността, автентичността, целостта, интегритета и конфиденциалността оказва тежко или непоправимо въздействие на административните функции.

Чл.24.(1) Системният администратор предприема необходимите мерки за предотвратяване на неправомерен достъп от трети лица до ресурсите на информационните системи на Дирекцията и Общинските служби.

(2) Определят се следните нива на защита от неправомерен достъп до всеки информационен актив и се прилагат следните общи правила:

1. Ниво „0“ - ниво на свободен достъп, обхващащо открита и общодостъпна информация.

а) не изисква прилагането на средства за конфиденциалност, поради анонимното ползване на информацията.

2. Ниво „1“ - ниво на произволно управление на достъпа.

а) достъпът до точно определени обекти се разрешава на точно определени ползватели;

б) ползвателите се идентифицират, преди да изпълняват каквито и да са действия, контролирани от системата за достъп чрез механизъм от типа идентификатор/ парола, като няма изисквания за доказателство за идентичността при регистрация;

в) идентифициращата информация е защитена от нерегламентиран достъп;

г) доверителната изчислителна система поддържа област за собственото изпълнение, защитена от външни въздействия и от опити да се следи хода на работата;

д) информационната система разполага с технически и/ или програмни средства, позволяващи периодично да се проверява коректността на компонентите на доверителната изчислителна система;

е) защитните механизми са проверени и се гарантира, че неоторизиран ползвател няма очевидна възможност да получи достъп до доверителната изчислителна система.

3. Ниво „2“ - ниво на принудително управление на достъпа, изискващо в допълнение към изискванията към ниво „1“:

а) за проверка на идентичността се използва удостоверение за електронен подпис, независимо дали е издадено в рамките на вътрешна инфраструктура на публичния ключ, или от външен доставчик на удостоверителни услуги;

б) при издаване на удостоверението издаващият орган проверява съществените данни за личността на ползвателя, без да е необходимо личното му присъствие;

в) доверителната изчислителна система осигурява реализация на принудително управление на достъпа до всички обекти и взаимна изолация на процесите чрез разделяне на адресните им пространства.

4. Ниво „3“ - ниво на проверена сигурност, изискващо в допълнение към изискванията към ниво „2“:

а) като механизъм за идентификация се използва единствено удостоверение за универсален електронен подпис;

б) при издаване на удостоверението се гарантира физическата идентичност на лицето;

в) доверителната изчислителна система е с проверена устойчивост към опити за проникване и притежава механизъм за регистрация на опити за нарушаване политиката за сигурност.

РАЗДЕЛ VII
УПРАВЛЕНИЕ НА ЕКСПЛОАТАЦИОННИТЕ ПРОЦЕСИ

Чл.25.(1) Осигуряват се мерки за сигурност при управление на експлоатационните процеси в информационните системи, включително сигурността на електронните съобщения в Дирекцията и Общинските служби.

(2) Прилагат се необходимите технически и организационни средства за извършване на контрол по ал.1, включително при териториална отдалеченост в случаите, отнасящи се до Общинските служби.

(3) Системният администратор следи за неправомерно инсталиран софтуер на работните станции или файлови сървъри и вземат мерки за неговото отстраняване.

Чл.26.(1) Като основно средство за управление на експлоатационните процеси в Дирекцията и Общинските служби за осигуряване на мрежова и информационна сигурност са създадени зони на сигурност в информационните системи.

(2) Като области от софтуерната архитектура на информационните системи, зоните за сигурност осигуряват определено ниво на сигурност чрез специфичен

комплекс от мерки. Зоните са адекватно разделени една от друга, като преносите на данни от една зона в друга са строго регламентирани и се осъществяват през контролни обекти, като защитни стени, прокси-сървъри и други.

(3) Мерките за сигурност при управление на експлоатационните процеси в информационни системи включват:

1. препоръчителна многослойна архитектура на информационните системи, при която потребителя, приложението и данните са логически и физически разделени;
2. спазване на правилата за резервиране и архивиране на данни и файлове, както следва:

а) резервиране и архивиране на данни и файлове само от служители, притежаващи документирано основание за това;

б) създаване на резервни копия и архив на текущите данни и файлове поне веднъж месечно посредством твърдо копиране на налична информация на нарочно определени за целта запаметяващи устройства;

в) съхраняване на резервни копия и архиви на данни и файлове за срок не по - малко от 6 месеца, но не повече от година, освен в случай на документирано основание.

3. редовно изготвяне на резервни копия на базите данни и файловете във файловите сървъри, като графиците за резервиране се определят в зависимост от характера на дейността на главна дирекция „АР“, дирекция „АПФСДЧР“ и Общинските служби и препоръчително е ежедневното резервиране;
4. съхраняване на резервните копия в специално отделно помещение или огнеупорна каса от системния администратор и администраторите на информационни системи;
5. достъп до резервни и архивни копия под контрола на звеното, отговарящо за мрежовата и информационна сигурност.

Чл.27.(1) Управлението на електронните съобщения в Дирекцията и Общинските служби се осъществява чрез мониторинг, контрол и координация на работата на компонентите на системата.

(2) За реализация на функциите на мрежовата сигурност се използват следните механизми или комбинации от тях:

1. криптиране;
2. цифрови сертификати;
3. механизми за управление на достъпа;
4. механизми за идентификация;
5. механизми за управление на маршрутизацията;
6. механизми за отбелязвания и записи на комуникационните характеристики.

(3) Защитата на електронните съобщения в Internet включва:

1. защитна стена;
2. защита от вируси, нежелан код и спам, както и проверка на прикачените файлове за вируси и нежелан код;
3. защита от DoS (denial of service) и HA (harvesting attacks) атаки;
4. защита на e-mail адресите от търсещи роботи;
5. защита от изтичане на информация и шпионски софтуер (spyware);
6. защита на IM (instant messaging) и гласовите комуникации (Skype, ICQ,

други);

7. проверка за съответствие с нормативните документи и приетите вътрешни политики, правила и процедури;

8. контрол върху обмена (изпращане, получаване) на големи файлове.

Чл.28. Копие от цялата служебна електронна поща се съхранява от системния администратор на сървъра на Дирекцията не по-малко от две години.

Чл.29.(1) Служителите в Дирекцията и Общинските служби използват за получаване и изпращане на служебна кореспонденция единствено служебната електронна поща.

(2) Електронни съобщения, изпратени от служители в Дирекцията и Общинските служби, съдържат задължително идентифициращa информация:

1. име, длъжност и учреждение;

2. телефон и електронна поща;

(3) В края на всяко изходящо електронно съобщение автоматично се прикачва изявление за ограничаване на отговорността (disclaimer) и указания към адресата за действия при погрешно получаване.

РАЗДЕЛ VIII
ЗАЩИТА СРЕЩУ НЕЖЕЛАН СОФТУЕР

Чл.30.(1) Защитата срещу нежелан софтуер в информационните мрежи и системи на Дирекцията и Общинските служби се организира от звеното, отговарящо за мрежовата и информационната сигурност.

(2) Нежеланият софтуер, който може да експлоатира уязвимостта на един или няколко информационни актива и да предизвика смущаване на нормалната им работа, увреждане или унищожаване, включва следните основни програми:

1. компютърни вируси;

2. мрежови червеи;

3. троянски коне;

4. логически бомби.

Чл. 31. Защитата срещу нежелан софтуер в информационните системи на Дирекцията и Общинските служби е ориентирана в две основни направления:

(1) използване на регламентиран софтуер:

1. включващ предварително определен набор за инсталиране на работните станции;

2. инсталиран от системния администратор на работните станции или файлови сървъри след одобрена докладна от:

а) Главния директор на главна дирекция „АР“ за служителите в специализираната администрация и Общинските служби;

б) Директора на дирекция „АПФСДЧР“ за служителите на общата администрация;

3. инсталиран от външни фирми, доставчици на информационно- комуникационни услуги в присъствието на системния администратор.

(2) задължително използване на утвърден антивирусен софтуер и софтуер за откриване на нерегламентирани промени на информационните активи.

Чл.32.(1) Системният администратор прилага средства за откриване на опити за проникване на различни нива и периметри на мрежата.

(2) Програмните продукти, предназначени за откриване на опити за проникване, следва да разпознават следните подозрителни действия в мрежата:

1. опити да се използват услуги, блокирани от защитни стени;
2. неочаквани заявки, особено от непознати адреси;
3. неочаквани шифровани съобщения;
4. извънредно активен трафик от непознати сървъри и устройства;
5. значителни изменения на предишни действия на мрежата;
6. опити за използване на известни системни грешки или уязвимости;
7. опити за вход от непознати потребители от неочаквани адреси;
8. несанкционирано или подозрително използване на администраторски функции;
9. значителни изменения в обичайните действия на потребител и други.

Чл.33.(1) При установяване на открити опити за проникване следва незабавно:

1. да се уведомява системният администратор за предприемане на адекватни мерки;
2. да се изключват или ограничават мрежовите услуги, свързани с информационния актив, обект на проникването.

(2) Всяко устройство, което се включва в мрежата на Дирекцията и Общинските служби, автоматично да се проверява за вируси и нежелан софтуер, преди да получи достъп до ресурсите на мрежата.

РАЗДЕЛ IX
МОНИТОРИНГ НА СЪБИТИЯТА И ИНЦИДЕНТИТЕ В ИНФОРМАЦИОННИТЕ СИСТЕМИ

Чл.34.(1) Информация за събития и инциденти, свързани с информационните системи на Дирекцията и Общинските служби се поддържа от звеното, отговарящо за мрежовата и информационна сигурност и съдържа следните записи:

1. дата и време на настъпване на събитието;
2. уникален идентификатор на ползвателя - инициатор на действието;
3. тип на събитието;
4. резултат от събитието;
5. източник на събитието;
6. списък на засегнатите обекти;
7. описание на измененията в системата за защита, произтекли от събитието.

Чл.35. Звеното, отговарящо за мрежовата и информационна сигурност разработва точни процедури за мониторинг на използването на системите, с които да осигурят изпълнението само на регламентирани процеси от страна на ползвателите, както следва:

1. реалистична оценка и мерки за управление на риска;
2. проследяване на изключения или ненормално поведение на ползватели за определен период;
3. осигуряване на записи както на успешните, така и на отказаните опити за достъп в системата.

Чл.36. За осигуряване на точност и пълнота на записите на логовете, които могат да

се използват за разследване на неправомерни действия или за нуждите на ангажиране на съдебни доказателства се осигурива поддържането на единно време в информационните системи съгласно Наредбата за електронните административни услуги.

Чл.37.(1) Звеното, отговарящо за мрежовата и информационна сигурност изготвя план за действие при инциденти, свързани с мрежовата и информационната сигурност на използваните информационни мрежи и системи, с цел осигуряване непрекъсваемост на дейността на Дирекцията и Общинските служби.

(2) Планирането на дейността по управление на инциденти, свързани с мрежовата и информационната сигурност включва следните етапи:

1. определяне на критично важните функции на системата и установяване на приоритетите за възстановителни работи;
2. идентификация на ресурсите, необходими за изпълнение на критично важните функции;
3. определяне списък на възможните инциденти с вероятности за появяването им, изхождайки от оценките на риска;
4. разработка на стратегии за възстановителни работи;
5. подготовка на мероприятия за реализация на стратегиите.

(3) Цикълът на управлението на инциденти включва следните основни етапи:

1. подготовка;
2. откриване и анализ;
3. ограничаване на влиянието, премахване на причината и възстановяване;
4. дейности след инцидента.

(4) Критичен елемент от управлението на инциденти е незабавното възстановяване на дейността на информационните системи.

(5) Меропиятията, които се провеждат след възстановяването и които целят избягване на подобни инциденти включват мерки по:

1. повишаване нивото на контрол на достъпа;
2. промяна на конфигурациите на зоните за сигурност;
3. изменение на режима на физически достъп;
4. инсталиране на допълнителни модули за защита към софтуера на системата;
5. саниране и декласификация на носителите и други.

Чл.38. Звеното, отговарящо за мрежова и информационна сигурност е длъжно да уведоми Националния център за действие при инциденти по отношение на мрежовата и информационната сигурност за всеки инцидент в информационните системи, както следва:

1. до 2 часа при първоначално уведомяване след констатирането на инцидента;
2. до 5 работни дни при предоставянето на пълната информация за инцидента, определена съгласно НОИМИС.
3.

РАЗДЕЛ X
ФИЗИЧЕСКА СИГУРНОСТ

Чл.39. Осигуряването на мерки за физическата защита на информационните системи в Дирекцията и Общинските служби включва:

1. мерки по управление на физическия достъп;
2. противопожарни мерки;
3. защита на поддържащата инфраструктура;
4. защита на мобилните системи.

Чл.40.(1) Мерките за физическа защита включват следните инфраструктурни компоненти:

1. сградите и помещенията, в които се разполагат техническото оборудване, софтуерът и архивите, необходими за информационните системи отговарят на следните архитектурно-строителни изисквания:

а) помещения с бетонни или тухлени стени;

б) стоманобетонни плочи с дебелина 0,15 [m];

в) климатизация;

г) разполагане на действаща и резервна батерии бутилки с пожарогасителен агент.

2. помещенията, в които се разполагат техническото оборудване, софтуерът и архивите, необходими за информационните системи на администрациите, се оборудват със следните технически системи за защита, безопасност и охрана:

а) разполагане действаща и резервна батерии бутилки с пожарогасителен агент;

б) климатизация;

в) системи за телевизионно видеонаблюдение.

Чл.41. Срещите между посетителите и служителите на Дирекцията и Общинските служби се извършват в специализирани помещения.

Чл.42. Служителите, използващи преносими компютри задължително използват пароли за достъп до ресурсите на мобилните устройства (дискови устройства, системни платки, софтуер и други).

Чл.43.(1) Предприемат се превантивни действия за защита на информационните системи от природни бедствия.

(4) Осигуряват се условия, при които неовластени лица не могат да получат физически достъп до работните станции и сървърите, използвани от служителите на Дирекцията и Общинските служби.

(5)

РАЗДЕЛ XI
СИГУРНОСТ ПО ОТНОШЕНИЕ НА СЛУЖИТЕЛИТЕ

Чл. За постигане на мрежовата и информационна сигурност по отношение на служителите в Дирекцията и Общинските служби при експлоатацията на информационните мрежи и системи се прилагат:

1. организационни мерки свързани с управление на достъпа и инструктаж на служителите, както следва:

а) достъпа на служителите до работните им станции и общите информационни системи се осъществява със служебни потребителско име и парола;

б) достъпа на служителите до специализираните информационни системи се осъществява със служебни потребителско име, парола или удостоверение за публичен ключ;

в) осигуряването на права за достъп на ръководителите и различните групи служители до ресурсите на информационните системи се извършва на основание утвърдените с настоящите Правила профили;

г) на всеки служител е определена принадлежност към профил, съответстващ на служебните му задължения, вписани в длъжностната му характеристика, работния му план или друго документирано основание;

д) служителите имат право на достъп само до тези ресурси на информационните системи, в която работят, или до системите на други администрации само доколкото са им необходими за изпълнение на служебните задължения съгласно длъжностната им характеристика, работния им план или друго документирано основание;

е) ежегодно се провежда инструктаж по мрежова и информационна сигурност, през които преминават всички служители;

ж) всички служители преминат инструктаж за действия при инциденти с мрежовата и информационна сигурност.

2. мерки по ангажиране отговорността на служителите при извършването на нарушения, свързани с политиката на мрежова и информационна сигурност на Дирекцията, както следва:

а) дисциплинарна отговорност за действия и бездействия;

б) имуществена отговорност за поверените им информационни активи;

в) административно-наказателна отговорност за неизпълнение на задължения.

РАЗДЕЛ XII
ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

1. Настоящите Правила се утвърждават със заповед на Директора на Областна дирекция „Земеделие“ Бургас.

2. Правилата се развиват и усъвършенстват в посока на тяхното надграждане чрез процедури по модела „Системи за управление на мрежовата и информационна сигурност“.

3. Правилата се преглеждат поне веднъж годишно и при необходимост се актуализират под ръководството на звеното, отговарящо за мрежовата и информационна сигурност.

4. Контрола по изпълнението на настоящите Правила се осъществява от Главния секретар на Областна дирекция „Земеделие“ Бургас.

СЪДЪРЖАНИЕ