



РЕПУБЛИКА БЪЛГАРИЯ
Министерство на земеделието, храните и горите
Областна дирекция "Земеделие"-Пловдив

З А П О В Е Д

№ РД-11-71

28.02.2019 г.

**На основание чл. 25, ал.4 от Закона за администрацията и чл.27 от
Устройствен правилник на Областните дирекции „Земеделие“**

/обн., ДВ. Бр.7 от 26.10.2010г., изм.и доп. ДВ. бр.12 от 12.02.2016г./

Н А Р Е Ж Д А М:

Утвърждавам Вътрешни правила за мрежова и информационна сигурност в
ОД „Земеделие“-Пловдив, съгласно приложението.

Настоящата заповед да се сведе до знанието на съответните длъжностни лица
за сведение и изпълнение.

С уважение

Татяна Богчева (Директор)
27.02.2019г. 17:30ч.
ОДЗ-Пловдив



Електронният подпись се намира в отделен файл с название signature.txt.p7s

БД/АПФСДЧР

гр. Пловдив 4000, бул. "Марица" № 122
тел: (+359) 32/ 634 022, факс: (+359) 32/ 628 730,
e-mail: odzg_plovdiv@abv.bg



РЕПУБЛИКА БЪЛГАРИЯ

Министерство на земеделието, храните и горите

Областна дирекция "Земеделие"-Пловдив

**УТВЪРДИЛ: ТАТЯНА БОГОЕВА
ДИРЕКТОР ОД "ЗЕМЕДЕЛИЕ"-ГР. ПЛОВДИВ**
Заповед № РД-11-71/28.02.2019 г.



ВЪТРЕШНИ ПРАВИЛА

ЗА ПОВИШАВАНЕ НИВОТО НА МРЕЖОВА И ИНФОРМАЦИОННА СИГУРНОСТ В ОБЛАСТНА ДИРЕКЦИЯ „ЗЕМЕДЕЛИЕ“ – ПЛОВДИВ

**гр. ПЛОВДИВ,
2019 година**



РЕПУБЛИКА БЪЛГАРИЯ

Министерство на земеделието, храните и горите

Областна дирекция "Земеделие"-Пловдив



УТВЪРДИЛ: ТАТЯНА БОГОЕВА
ДИРЕКТОР ОД "ЗЕМЕДЕЛИЕ" - ГР. ПЛОВДИВ

Заповед № РД -11-71 /28.02.2019 г=

ВЪТРЕШНИ ПРАВИЛА

**ЗА ПОВИШАВАНЕ НИВОТО НА МРЕЖОВА И
ИНФОРМАЦИОННА СИГУРНОСТ В ОБЛАСТНА ДИРЕКЦИЯ
„ЗЕМЕДЕЛИЕ“ – ПЛОВДИВ**

гр. ПЛОВДИВ,
2018 година

ОБЛАСТНА ДИРЕКЦИЯ “ЗЕМЕДЕЛИЕ” – ПЛОВДИВ

ВЪТРЕШНИ ПРАВИЛА ЗА ПОВИШАВАНЕ НИВОТО НА МРЕЖОВА И ИНФОРМАЦИОННА СИГУРНОСТ В ОД

“ЗЕМЕДЕЛИЕ”-ПЛОВДИВ

РАЗДЕЛ I ОБЩИ ПОЛОЖЕНИЯ

Чл.1 Настоящите правила имат за цел осигуряването на контрол и управление на работата на информационните системи в ОД “Земеделие”-Пловдив. 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 са специфични за всяко звено от дирекцията и с общо предназначение.

Чл.2 Потребителите на информационни системи в ОД “Земеделие”-Пловдив 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 Наредбата за общите изисквания за оперативна съвместимост и информационна сигурност (ЗАГЛ. ИЗМ. - ДВ. БР. 5 от 2017 Г., В СИЛА ОТ 01.03.2017 Г.)

ЦЕЛ

Чл.4 Целта на тези правила е да се осигури необходимото ниво на защита на базите с данни от съответните заплахи към тях, без оглед на тяхната природа, дали са породени от вътрешни или външни за ОД “Земеделие”-Пловдив източници, умышленi или случайни.

Чл.5 Чрез прилагането на описаните правила се цели да се постигне:

1. Предпазване от нерегламентиран вътрешен или външен достъп до базите данни с цел повреждане, модифициране или унищожаването на данни;
2. Недопускане на кражбата или изтичане на информация от базите данни, както и използването ѝ за лични облаги;
3. Предпазване от случайна, преднамерена и/или по непредпазливост промяна или загуба на данни;
4. Предпазване от повреждане или унищожаване на информация при експлоатационните процеси в организацията;
5. Предотвратяване от загуба на информация при съхранението и преноса на базите данни на външни устройства;
6. Постигане и поддържане на оторизирания достъп до наличност на информацията в базите данни за упълномощени потребители, процеси и/или приложения, без прекъсвания на работните процеси;
7. Спазване на националните законови и подзаконови изисквания за защита на различни типове информация;
8. Непрекъснатост на дейностите по оценка и анализ на заплахите, уязвимостта и на свързаните с тях рискове към сигурността на базите данни;
9. Предотвратяване на загуба на данни, в следствие на други въздействия като пожар, наводнения, стихийни бедствия, аварии и др.

РАЗДЕЛ II КОНТРОЛ НА ДОСТЪПА И ПРАВИЛА ЗА РАБОТА С НОСИТЕЛИ

Чл.6 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 служители на ОД “Земеделие”-Пловдив.

Чл.7 Всеки служител има точно определени права на достъп и използва уникарен потребителски профил за вход в системата и достъп до данните, за които е

ОБЛАСТНА ДИРЕКЦИЯ "ЗЕМЕДЕЛИЕ" – ПЛОВДИВ

ВЪТРЕШНИ ПРАВИЛА ЗА ПОВИШАВАНЕ НИВОТО НА МРЕЖОВА И ИНФОРМАЦИОННА СИГУРНОСТ В ОД
"ЗЕМЕДЕЛИЕ"-ПЛОВДИВ

оторизиран, така че да може да бъде идентифициран. Не е разрешено използването на групови профили;

Чл. 8 Контрол на управлението и защитата на достъпа до мрежови връзки и мрежови услуги се извършва чрез средствата на активна дирекция с конкретно потребителско име, осигурено от Системния администратор, който контролира компютрите, използвани за достъп до мрежи и мрежови услуги.

Чл. 9 Представянето 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. 10 Лицата, които обработват лични данни, използват уникални пароли с достатъчно сложност, които не се записват или съхраняват онлайн;

Чл. 11 Всички пароли за достъп на системно ниво се променят периодично;

Чл. 12 Всички носители на лични данни се съхраняват в безопасна и сигурна среда – въвствие със спецификациите на производителите, в заключени шкафове, с ограничен и контролиран достъп.

Чл. 13 На служителите на ОД "Земеделие"-Пловдив, 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 заявлена услуга.

Чл. 14 За нарушение целостта на данните се считат следните действия:

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

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

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

Чл. 14 При изнасяне на носители извън физическите граници на ОД "Земеделие"-Пловдив, 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 бе спасно за намаляване на риска от изтичане на чувствителна информация към не пълномощени 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 интернет страницата на ОД "Земеделие"-Пловдив се извършва от служители, определени със заповед на директора. На посочените длъжности лица се създават потребителски имена и пароли за извършване на актуализациите.

Чл. 19 Събирането и подготовката на данните се извършва от служители в техния реестър, след което данните се изпращат в електронен вид (на файлове) на служителите отговорни за качването им на интернет страницата на ОД "Земеделие"-Пловдив.

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

ОБЛАСТНА ДИРЕКЦИЯ "ЗЕМЕДЕЛИЕ" – ПЛОВДИВ

ВЪТРЕШНИ ПРАВИЛА ЗА ПОВИШАВАНЕ НИВОТО НА МРЕЖОВА И ИНФОРМАЦИОННА СИГУРНОСТ В ОД
"ЗЕМЕДЕЛИЕ"-Пловдив

труда и социалната политика и министъра на здравеопазването, обн., дв. бр. 70 от 26.08.2005 г.).

Чл.22 Сървъри на локални компютърни мрежи се разполагат в самостоятелни помещения съобразно изискванията на Приложение № 11 към чл. 45 ал. 2 от Наредба за общите изисквания за оперативна съвместимост и информационна сигурност (Приета с ПМС № 279 от 17.11.2008 г.).

Чл.23 Всеки служител отговаря за целостта на компютърната и периферна техника, програмните продукти и данни, инсталиирани на компютъра на неговото работно място или ползвани от него на сървъра на локалната компютърна мрежа съобразно дадените му права.

Чл.24 Служителят има право да работи на служебен компютър, като достъпът до съхраняваните данни в програмен продукт ФЕРМА се осъществява с въвеждането на потребителско име и парола;

Чл.25 Забранява се на външни лица работата с персоналните компютри на ОД "Земеделие"-Пловдив, 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 системния администратор или служител от дирекция "АПФСДЧР".

Чл.26 След края на работния ден всеки служител задължително изключва компютъра, на който работи, или го привежда в режим log off;

Чл.27 При загуба на данни или информация от служебния компютър, служителят незабавно уведомява Системния администратор, който му оказва съответна техническа помощ;

Чл.28 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 каквото и да е действия, които улесняват трети лица за несанкциониран достъп;

Чл.29 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 от системния администратор.

Чл.30 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.31 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.32 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.33 Достъпът до помещенията, където са разположени сървърите и комуникационните шкафове се ограничава по възможност само до специализиран по поддръжката им персонал.

РАЗДЕЛ IV ОТГОВОРНОСТИ НА СЛУЖИТЕЛИТЕ ПО ПОДДРЪЖКА НА БАЗА ДАННИ

Чл.34 Отговорности на служителите по поддръжка на бази данни са:

1. да прилагат правилата за информационна сигурност на базите данни и свързаните с тях специфични изисквания;
2. да изготвят специфичните изисквания за сигурност на базите данни, вкл. процедури, инструкции др.;
3. да инсталират, конфигурират и управляват системите за управление на базите данни /СУБД/; да следят за актуалността и допълнения на СУБД като създават организация за прилагането им;

ОБЛАСТНА ДИРЕКЦИЯ “ЗЕМЕДЕЛИЕ” – ПЛОВДИВ

БЪЛГАРСКИ ПРАВИЛА ЗА ПОВИШАВАНЕ НИВОТО НА МРЕЖОВА И ИНФОРМАЦИОННА СИГУРНОСТ В ОД
“ЗЕМЕДЕЛИЕ”-ПЛОВДИВ

4. да създават, администрират и поддържат бази данни според конкретните нужди на информационната система и при спазване на правилата за сигурност на базите данни;
5. да резервираят и архивират базите данни;
6. да извършват ежедневен сутрешен и вечерен обход и оглед на центровете за съхранение на данни;
7. да упражняват ежедневен контрол на базите данни относно нарастване, консистентност, повреди и др.;
8. да съществяват и контролират трансфера на данни (входящ и изходящ), както вътрешноведомствен, така и с други институции, като стриктно се спазват условията, договорени с институциите за приемане и предаване на данни;
9. да предприемат необходимите действия при възникване на инциденти или при установяване на уязвимост, свързани със сигурността на базите;
10. да участват в разрешаването на извънредни ситуации във връзка с нормалното функциониране на базите данни;
11. да контролират и извършват периодичен преглед на правата на достъп до базите данни;
12. да осъществяват контрол по спазването на изискванията за сигурност на базите данни);

Чл.35 При реализацията на проекти по разработване и внедряване на програмни продукти и модули, съдържащи бази данни, екипът по проекта:

1. определя изискванията към сигурността на базите данни в съответствие с правилата за сигурност на базите данни;
2. подпомага избора и прилагането на подходящи решения за сигурност на базите данни;
3. дефинира при какви условия ще бъде осигуряван достъпа на потребителите до базите данни, спазвайки съответните правила.

Чл.36 Инсталацирането, конфигурирането и актуализирането на СУБД се извършва при следните условия:

1. инсталацирането и конфигурирането на СУБД се извършва от оторизирани служители при спазване на лицензионната политика.
2. не се допускат промени по СУБД от други служителите, освен ако изрично не са утълненоощени за това;
3. актуализирането на СУБД се извършва само след предварително проведени тестове и подготвен подробен план за актуализация;

Чл.37 Създаване и разполагане на базите данни

1. Базите данни се съхраняват само в специализирани дискови системи от висок клас, като не се допуска съхранение в незашитени дискови системи, без резервиране на дисковете в масива;
2. Устройствата, съхраняващи базите данни, трябва да бъдат физически недостъпни за външни лица;
3. Не се допуска присъединяване на каквото и да е било външни устройства към дисковите масиви;
4. Не се допуска нерегламентираното създаване на БД върху дисковите масиви без изрично писмено съгласие за това;
5. Не се допускат физически операции извън тези, гарантиращи поддръжката на БД.

Чл.38 Използване на базите данни

1. Базите данни се контролират ежедневно относно нарастване, консистентност, повреди, интегритет и др.;
2. Ежедневно се следят репликации и трансфери на данни, както и различни обработки управлявани от СУБД;
3. Следят се логове и производителността на базите данни и се извършва мониторинг на състоянието на базите данни;
4. При инцидент по сигурността се уведомява прекия ръководител и се предприемат незабавни мерки за отстраняването му, следвайки стратегията за възстановяване на работоспособността на базите данни.

Чл.39 Резервиране и архивиране на бази данни.

ОБЛАСТНА ДИРЕКЦИЯ “ЗЕМЕДЕЛИЕ” – ПЛОВДИВ

ВЪТРЕШНИ ПРАВИЛА ЗА ПОВИШАВАНЕ НИВОТО НА МРЕЖОВА И ИНФОРМАЦИОННА СИГУРНОСТ В ОД

“Земеделие”-Пловдив

1. Изготвя се график за създаване на резервни и архивни копия на базите данни; Архивирането на базите данни се извършва по график;
2. На архивиране и възстановяване подлежат всички налични и функциониращи бази данни;
3. Достъпът до системите за архивиране на базите данни и контролът на процеса се извършва само от определени за целта служители, които следят и за успешното архивиране на данните;
4. Периодично се провеждат тестове за възстановяване на базата данни последното направено архивно копие.

РАЗДЕЛ V ПОЛЗВАНЕ НА КОМПЮТЪРНАТА МРЕЖА И ИНТЕРНЕТ

Чл.40 Упълномощени служители от дирекцията извършват необходимите настройки за достъп до интернет, създават потребителски имена и пароли за работа със система за управление на документооборота и работния поток-Eventis в електронната поща на ОД “Земеделие”-Пловдив.

Чл.41 Ползването на компютърната мрежа и електронната поща от служителите става чрез получените потребителско име и парола или електронен подпис (Doc Sign Doc Pro).

Чл.42 Служителите на ОД “Земеделие”-Пловдив 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, достъп до интернет или електронна поща при използване на представените им потребителски имена и пароли.

Чл.43 Компютрите, свързани в мрежата на ОД “Земеделие”-Пловдив използват интернет само от доставчик, с когото дирекцията има сключен договор за доставка на интернет.

Чл.44 Забранява се свързването на компютри едновременно в мрежата на ОД “Земеделие”-Пловдив и в други мрежи, когато това позволява разкриване и достъп до IP адреси от мрежата на дирекцията и/или е в противоречие с изискванията на Закона за електронното управление (ЗЕУ) и Наредба за общите изисквания за оперативна съвместимост и информационна сигурност (ЗАГЛ. ИЗМ. - ДВ, БР, бр. 5 от 2017 Г., В СИЛА ОТ 01.03.2017 Г.).

Чл.45 Забранява се инсталирането и използването на комуникатори (като Icq, skype и др. подобни), осигуряващи достъп извън рамките на компютърната мрежа на ОД “Земеделие”-Пловдив и създаващи предпоставки за идентифициране на IP адреса на потребителя и за достъп на злонамерен софтуер и мобилен код до компютрите, свързани в компютърната мрежа на дирекцията.

Чл.46 Забранява се съхраняването на сървърите на ОД “Земеделие”-Пловдив на лични файлове с текст, изображения, видео и аудио.

Чл.47 Забранява се отварянето без контрол от страна на системния администратор на:

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 VI ЗАЩИТА ОТ КОМПЮТЪРНИ ВИРУСИ И ДРУГ ЗЛОВРЕДЕН СОФТУЕР

Чл.48 С цел антивирусна защита в ОД “Земеделие”-Пловдив се прилагат следните мерки:

1. Всички персонални компютри имат инсталиран антивирусен софтуер в реално време, който се обновява ежедневно.
2. Системният администратор извършва следните дейности:

ОБЛАСТНА ДИРЕКЦИЯ “ЗЕМЕДЕЛИЕ” – ПЛОВДИВ

ВЪТРЕШНИ ПРАВИЛА ЗА ПОВИШАВАНЕ НИВОТО НА МРЕЖОВА И ИНФОРМАЦИОННА СИГУРНОСТ В ОД
“Земеделие”-Пловдив

- 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, но поне веднъж седмично.
- 2.3. активира защитата на различните програмни продукти за предупреждение при наличие на макроси и настройва защитната стена на система;
- 2.4. проверява за правилно настроен софтуер за автоматично обновяване на операционната система и инсталирания софтуер;
3. При появя на съобщение от антивирусната програма за вирус в локалната мрежа, всеки служител от общинска служба или в дирекцията задължително информира Системния администратор.

Чл.49 Организационни мерки за защита:

1. Превенция за възникнали уязвимости и осъществени атаки:

Със заповед на директора на ОД “Земеделие”-Пловдив се определя служител, отговарящ за провеждане на дейности свързани с прилагане на политиките за мрежата и информационна сигурност.

2. Етапментиране на правата и задълженията на потребителите на комуникационно и информационната среда.

Чл.50 Мерки за защита на хостове (компютър, сървър):

1. Оценка на степента на постигнатата мрежова и информационна сигурност, свързани с ежедневни дейности от страна на служители от компетентната дирекция, по отношение администриране и мониторинг на информационните системи и техническа инфраструктура. Извършване на ежедневен мониторинг на журналните файлове за събития индициращи отклонения от нормалното състояние.

2. Подобряване сигурността на хостове (security hardening):

2.1. Прилагане на Политики, които ограничават портове, услуги и забраняват употреба на протоколи;

2.2. Прилагане на политики: политика за пароли в (комбинация от букви, цифри, специални символи), управление на акаунти и достъпи в различните системи, изпълнение на политики за използване на минимални привилегии (least privilege). С ограничаване на софтуера който може да бъде инсталиран и изпълняван върху различни платформи.

2.3. Управление на оборудването – сигурно изтриване на информацията преди да е извадено от устройство да бъде извадено от употреба.

2.4. Настройка на бекъп на домейн контролери и сървъри с критични услуги.

Чл.51 Мерки за мрежова сигурност

Във възъка с повишения риск от кибер- атаки и инциденти, както и увеличаване на неподчинените действия и щетите, които нанасят с цел запазване на целостта, единствеността, наличността и достъпността на информацията, и системите и ресурсите в които тя се събира, обработва, използва и съхранява се предприемат допълнителни мерки:

1. Съпоринг на комуникационните канали осигуряващи свързаността на ОД “Земеделие”-Пловдив;

2. Аплидиране на параметри за нормалното функциониране на ИКТ инфраструктурата на ОД “Земеделие”-Пловдив;

3. Аплидиране на работоспособността на външните услуги предлагани от ОД “Земеделие”-Пловдив – интернет портали, страници, регистри и др.;

4. Аплидиране на работоспособността на вътрешните услуги – Активна директория, Електронна поща, бази данни, приложения и др.;

5. Съвременно уведомяване на администраторите при настъпили отклонения в параметрите, за да бъдат предприети адекватни мерки за гашаването на проблема;

Чл.52 Мерки за защита на приложения и данни:

1. Използване на приложения и данни от вътрешната мрежова инфраструктура, които за защита се отнасят за решения свързани със съвместната работа на

ОБЛАСТНА ДИРЕКЦИЯ "ЗЕМЕДЕЛИЕ" – ПЛОВДИВ

ВЪТРЕШНИ ПРАВИЛА ЗА ПОВИШАВАНЕ НИВОТО НА МРЕЖОВА И ИНФОРМАЦИОННА СИГУРНОСТ В ОД

"ЗЕМЕДЕЛИЕ"-Пловдив

различни приложения и услуги- електронна поща, вътрешни портали, файлови услуги, комуникация в реално време и др.

2. При приложения с достъп от интернет, мерките за сигурност касаещи публичния уеб сайт, както и системи свързани с електронните услуги и обмен на файлове, изпълняваните дейности са в обхвата на защита на онлайн транзакциите, контрол на достъпа на външни клиенти, осигуряване на отказ устойчивост на системите и интегритет на публичната информация.

3. За защита на услугата електронна поща да се извърши сканиране на входящ и изходящ трафик.

4. За преносимите носители на информация се прилагат добри практики за ограничаване автоматично стартиране на изпълним код при включването им и дейности свързани с защита на преносимите медии, заличаване на информация при изваждане от употреба, обозначаване, съхранение и транспортиране.

5. Достъпът на служителите до работните им станции и общите информационни системи се осъществява със служебни потребителско име и парола.

Чл.53 Мерки за непрекъснатост на работата:

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., Системният администратор започва процедура по поетапно спиране на сървърите.

4. 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 VI ПРАВА НА ДОСТЪП ДО ИНФОРМАЦИОННИ РЕСУРСИ

Чл.54 При назначаване на нов служител или служител по заместване, Директорът на Дирекция „АПФСДЧР“ уведомява за това системния администратор не по-късно от 3 работни дни преди датата на назначаване. След постъпване на работа новоназначеният служител представя попълнена заявка по образец или копие от заповед, издадена на основание чл. 44, ал.1, т.14 от ЗМСМА или чл. 24, ал.4 от Закона за защита на личните данни, на основание на която му се разрешават права на достъп до определени ресурси. Заявката може да се предостави и в електронен вид (по електронна поща) на системния администратор от директор на дирекция или началника на общинска служба, в която работи служителят, за когото се отнася заявката.

Чл.55. За промяна в правата на достъп служителят представя на системния администратор заявка по образец. Заявката може да се предостави и в електронен вид (по електронна поща) от директор на дирекция или началника на общинска служба, в която работи служителят, за когото се отнася заявката.

Чл.56 При прекратяване на служебното (трудовото) правоотношение между администрацията на Од "Земеделие"-Пловдив и определен служител, Директорът на дирекция „АПФСДЧР“ уведомява за това Системния администратор не по-късно от 3 работни дни преди датата на прекратяване. С изтичане на работния ден, предхождащ прекратяването на правоотношенията на служителя с Од "Земеделие"-Пловдив, отговорен служител прекратява правата на достъп до мрежови ресурси, електронна поща и компютър на служителя, чието служебно(трудово) правоотношение с Од "Земеделие"-Пловдив се прекратява и при необходимост извърши преинсталация на компютъра.

РАЗДЕЛ VII КОНТРОЛ

ОБЛАСТНА ДИРЕКЦИЯ “ЗЕМЕДЕЛИЕ” – ПЛОВДИВ

**ВЪТРЕШНИ ПРАВИЛА ЗА ПОВИШАВАНЕ НИВОТО НА МРЕЖОВА И ИНФОРМАЦИОННА СИГУРНОСТ В ОД
“ЗЕМЕДЕЛИЕ”-ПЛОВДИВ**

Чл.57 Ръководителите на звена от администрацията/Директорите на дирекции и началниците на общинските служби по земеделие/ контролират използването на компютърната и периферна техника, като при необходимост изясняват причините за не използването на техниката и програмите или използването им не по предназначение като уведомяват Главния секретар на ОД “Земеделие”-Пловдив с цел прилагане на съответните административни действия.

Чл.58 Системният администратор контролира изпълнението на дейности, които засягат работата с електронни бази данни, ползване на сървърно дисково пространство, достъп до отдалечени ресурси и които не се контролират от други инстанции, като при установяване на неизпълнение или лошо изпълнение по някоя от точките, касаещи работата с електронни данни приема действия за възстановяване на изправността и уведомява Главния секретар с цел прилагане на съответните административни действия.

Чл.59 На периодична проверка от системния администратор подлежат веднъж годишно:

1. компютрите относно: промени в хардуерната конфигурация, инсталирания софтуер, допълнително инсталиран софтуер, неразрешени промени в операционната система на компютъра;
2. сървърите относно: лични файлове с текст, изображения, видео и аудио.

РАЗДЕЛ VIII ЗАЩИТА СРЕЩУ НЕЖЕЛАН СОФТЕУР

Чл.60 Защитата срещу нежелан софтуер в информационните системи на ОД “Земеделие”-Пловдив се организира от служителите, отговарящи за мрежовата и информационната сигурност в дирекцията.

Чл.61 Съгласно чл.45, ал.1 от Наредбата за и общите изисквания за мрежова и информационна сигурност Директорът на ОД “Земеделие”-Пловдив осигурява мерки за физическата защита на информационните системи в дирекцията и общинските служби по земеделие/ Приложение 1/.

Чл.62 Съгласно чл.41 от Наредбата за и общите изисквания за мрежова и информационна сигурност директорът на ОД “Земеделие”-Пловдив осигурява мерките за защита срещу нежелан софтуер /Приложение 2/

Чл.63 Националният център за действие при инциденти по отношение на мрежовата и информационната сигурност поддържа актуална информация за всички опити за проникване на нежелан софтуер в информационните системи на административните органи, както и за предприетите действия за защита от тях.

Чл.64 Директорът на ОД “Земеделие”-Пловдив приема превантивни действия за защита на информационните системи от природни бедствия като застрахова риска от щети от природни бедствия на информационните системи в рамките на задължителните годишни застраховки.

Чл.65 Директорът на ОД “Земеделие”-Пловдив осигурява условия, при които неовластени лица не могат да получат физически достъп до работните станции и сървърите, използвани от администрацията.

Чл.66 Директорът на ОД “Земеделие”-Пловдив утвърждава план за действие при инциденти, свързани с мрежовата и информационната сигурност на използваните от тях информационни системи, с цел осигуряване непрекъсваемост на дейността на съответната администрация /Приложение 3/.

Чл.67 Служителят по мрежова и информационна сигурност в ОД “Земеделие”-Пловдив е длъжен да уведомява незабавно Националния център за действие при инциденти по отношение на мрежовата и информационната сигурност за всеки инцидент в информационните системи на дирекцията.

ОБЛАСТНА ДИРЕКЦИЯ "ЗЕМЕДЕЛИЕ" - ПЛОВДИВ

ВЪТРЕШНИ ПРАВИЛА ЗА ПОВИШАВАНЕ НИВОТО НА МРЕЖОВА И ИНФОРМАЦИОННА СИГУРНОСТ

"Земеделие"-Пловдив

РАЗДЕЛ IX ДИСЦИПЛИНАРНА ОТГОВОРНОСТ

Чл.68 Служители, които не поддържат актуални данните, с които работят и изглеждат умишлено неверни данни и създават условия за разпространяване на фалшиви електронна информация, се наказват с дисциплинарно наказание за нарушение на трудовата дисциплина в съответствие с чл. 187, т. 3, 4, 7, 8 и 10 от КТ или чл.89, ал.2 от ЗДСЛ и се задължават да възстановят данните в актуално състояние.

Чл.69 Служители на ОД "Земеделие"-Пловдив, които заразят програми и бази данни с компютърни вируси се наказват с дисциплинарно наказание за нарушение на трудовата дисциплина в съответствие с чл. 187, т. 9 от КТ или чл.89, ал.2 от ЗДСЛ и със заплащане на стойността на повредените програми и на разходите за възстановяване на данните.

Чл.70 Служители на ОД "Земеделие"-Пловдив, които деинсталират, инсталират или разместват компютърни конфигурации, части от тях, периферна техника, като пасивни компоненти на локални компютърни мрежи както и комуникационни устройства се наказват с дисциплинарно наказание за нарушения на дисциплина в съответствие с т. 187, ал. 3 и 9 от КТ или чл.89, ал.2 от ЗДСЛ, при повреда на техниката - и със заплащане на стойността на повредената техника.

Чл.71 При установяване, че външни лица използват компютърна и периферна техника в ОД "Земеделие"-Пловдив извън регламентираните в настоящите правила случаи, служителите ОД "Земеделие"-Пловдив допуснали това се наказват с дисциплинарно наказание за нарушения на трудовата дисциплина в съответствие с чл. 187, т. 3, 8 и 9 от КТ или чл.89, ал.2 от ЗДСЛ, а при установяване на повреда на техника, данни и програми и със заплащане на стойността на повредените техника и програми, както и на разходите за възстановяване на данните.

Чл.72 При установяване на действия на служителите на ОД "Земеделие"-Пловдив, които са довели до унищожаване на служебна информация, разположена на ползваните от тях компютри, служителите се наказват с дисциплинарно наказание за нарушения на трудовата дисциплина в съответствие с чл. 187, т. 3,8 и 9 от КТ или чл.89, ал.2 от ЗДСЛ.

Чл.73 Служители на ОД "Земеделие"-Пловдив, които в установленото рабоче време не изпълняват служебните им задължения и поставените им задачи, а използват компютрите за компютърни игри или за друг вид дейност, която не е свързана с изпълнението на служебните им задължения, се наказват с дисциплинарно наказание за нарушения на трудовата дисциплина в съответствие с чл. 187, т. 3 и 9 от КТ или чл.89, ал.2 от ЗДСЛ.

Чл.74 При следващи нарушения на провинилия се служител се налагат следните по степен дисциплинарни наказания съгласно чл. 188 от КТ или чл.90 от ЗДСЛ.

ПРЕХОДНИ И ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

§ 1. Настоящите правила са неразделна част към Системите за функциониране и управление и контрол в ОД „Земеделие“-Пловдив и подлежи на периодично актуализиране при възникната необходимост.

§ 2. Правилата и процедурите могат да се допълват и изменят със запоръка на Директор ОД“Земеделие“-Пловдив.

§ 3. Указания по прилагането на настоящите правила дава директория АПФСДЧР“.

§ 4. Контрола по прилагане на настоящите правила се осъществява от секретар на ОД“Земеделие“-Пловдив.

ОБЛАСТНА ДИРЕКЦИЯ “ЗЕМЕДЕЛИЕ” – ПЛОВДИВ

ВЪТРЕШНИ ПРАВИЛА ЗА ПОВИШАВАНЕ НИВОТО НА МРЕЖОВА И ИНФОРМАЦИОННА СИГУРНОСТ В ОД
“ЗЕМЕДЕЛИЕ”-ПЛОВДИВ

Приложение 1

Параметри на физическата сигурност

1. За осигуряване физическата защита на информационни системи директорът на ОД “Земеделие”-Пловдив приема следните мерки:
 - а) мерки по управление на физическия достъп;
 - б) противопожарни мерки;
 - в) защита на поддържащата инфраструктура;
 - г) защита на мобилните системи.
2. Препоръчва се мерките за физическа защита да включват следните инфраструктурни компоненти:
 - 2.1. Сградите и помещенията, в които се разполагат техническото оборудване, софтуерът и архивите, необходими за информационните системи на административните органи, да отговарят на следните архитектурно-строителни изисквания:
 - а) помещенията да имат бетонни или тухлени стени;
 - б) плочите да бъдат стоманобетонни с дебелина 0,15 [m];
 - в) помещенията да имат специални подвижни отвори, които предпазват от свръхнаглягане;
 - г) двойният под да има височина не по-малка от 0,30 [m];
 - д) покаченият таван да има височина не по-малка от 0,50 [m];
 - е) климатичните системи за помещенията да позволяват управление от алармни сигнал, на пожарогасителна система;
 - ж) до помещенията да се осигури отделна стая, в която да се разположат действащата и резервната батерии бутилки с пожарогасителния агент.
 - 2.2. Помещенията, в които се разполагат техническото оборудване, софтуерът и архивите, необходими за информационните системи на администрации, се оборудват със следните технически системи за защита, безопасност и охрана:
 - а) пожарогасителна система, която трябва да отговаря на изискванията на EN 14520;
 - б) климатизация;
 - в) резервно електрозахранване;
 - г) системи за телевизионно видеонаблюдение;
 - д) системи за контрол на достъпа.
 3. Срещите между посетителите и служителите в администрации трябва да се извършват в специализирани помещения.
 4. В случаите по т. 3 да се води списък на посетителите кога и с кого са се срещали по какъв въпрос. Списъкът да се съхранява не по-малко от една година от датата на посещението. Списъкът може да се води и само в електронна форма.
 5. Служителите, използващи преносими компютри, трябва задължително да използват пароли за достъп до ресурсите на мобилните устройства (дискови устройства, системни платки, софтуер и др.)

Приложение 2

Заштита срещу нежелан софтуер

1. 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:
 - а) компютърни вируси;
 - б) мрежови червеи;
 - в) троянски коне, и
 - г) логически бомби.
2. Защитата срещу нежелан софтуер в информационните системи на ОД “Земеделие”-Пловдив трябва да бъде ориентирана в две основни направления:
 - а) чрез забрана за използване на нерегламентиран софтуер;

ОБЛАСТНА ДИРЕКЦИЯ "ЗЕМЕДЕЛИЕ" – ПЛОВДИВ

ВЪТРЕШНИ ПРАВИЛА ЗА ПОВИШАВАНЕ НИВОТО НА МРЕЖОВА И ИНФОРМАЦИОННА СИГУРНОСТ В ОД

"ЗЕМЕДЕЛИЕ"-Пловдив

б) чрез задължително използване на утвърден за цялата администрация антивирусен софтуер и софтуер за откриване на нерегламентирани промени на информационните активи.

3. Администраторът на единната национална мрежа (ЕНМ) тряба да прилага средства за откриване на опити за проникване на различни нива и периметри на мрежата.

4. Програмните продукти, предназначени за откриване на опити за проникване, трябва да разпознават следните подозрителни действия в мрежата:

а) опити да се използват услуги, блокирани от защитни стени;

б) неочаквани заявки, особено от непознати адреси;

в) неочаквани шифровани съобщения;

г) извънредно активен трафик от непознати сървъри и устройства;

д) значителни изменения на предишни действия на мрежата;

е) опити за използване на известни системни грешки или уязвимости;

ж) опити за вход от непознати потребители от неочаквани адреси;

з) несанкционирано или подозрително използване на администраторски функции;

и) значителни изменения в обичайните действия на потребител и пр.

5. При установяване на открити опити за проникване трябва незабавно:

а) да се уведомява системният администратор за предприемане на адекватни мерки;

б) да се изключват или ограничават мрежовите услуги, свързани с информационния актив - обект на проникването.

6. Всяко устройство, което се включва в мрежата на съответната администрация, автоматично да се проверява за вируси и нежелан софтуер, преди да получи достъп до ресурсите на мрежата.

Приложение З

Управление на инциденти, свързани с мрежовата и информационната сигурност

1. Планирането на дейността по управление на инциденти, свързани с мрежовата и информационната сигурност, включва следните етапи:

а) определяне на критично важните функции на системата и установяване на приоритетите за възстановителни работи;

б) идентификация на ресурсите, необходими за изпълнение на критично важните функции;

в) определяне списък на възможните инциденти с вероятности за появяването им, изходящи от оценките на риска;

г) разработка на стратегии за възстановителни работи;

д) подготовка на мероприятия за реализация на стратегиите.

2. Цикълът на управлението на инциденти включва следните основни етапи:

а) подготовка;

б) откриване и анализ;

в) ограничаване на влиянието, премахване на причината, възстановяване;

г) дейности след инцидента.

3. Критичен елемент от управлението на инциденти е незабавното възстановяване на дейността на системата.

4. Политиката за защита от инциденти и възстановителни работи на ОД "Земеделие"-Пловдив която произтича от оценката на риска по глава трета, раздел III от Наредбата за общите изисквания за мрежова и информационна сигурност, идентифицира средствата за резервиране и възстановяване с оглед покриване ниво на резервиране над пето по класацията на Асоциация Share.

5. Средствата по т. 4 могат да бъдат:

а) паралелно записване или огледална репликация на съхраняваните данни (технологии "Disk Mirroring" или "RAID" ("Redundant Array of Independent Drives"));

б) създаване на сървър за възстановяване след инциденти (т. нар. "Disaster Recovery Center"), в който се извършва постоянно архивно съхранение ("back-up") на

ОБЛАСТНА ДИРЕКЦИЯ "ЗЕМЕДЕЛИЕ" – ПЛОВДИВ

ВЪТРЕШНИ ПРАВИЛА ЗА ПОВИШАВАНЕ НИВОТО НА МРЕЖОВА И ИНФОРМАЦИОННА СИГУРНОСТ В ОД
"ЗЕМЕДЕЛИЕ"-Пловдив

информацията от системата, така че да може да се възстанови нейната дейност след инцидента;

в) създаване на резервен сървър, в който се поддържа репликирано състояние на критичните оперативно действащи системи, така че дейността им да бъде незабавно посвета от него.

6. Планът за действия при инциденти на ОД "Земеделие"-Пловдив, включва мерки, които да се проведат след възстановяването и които да целят избягване на инциденти са:

- а) повишаване нивото на контрол на достъпа;
- б) промяна на конфигурациите на зоните за сигурност;
- в) изменение на режима на физически достъп;
- г) инсталiranе на допълнителни модули за защита към софтуера на системата;
- д) саниране и де класификация на носителите;

С уважение

Татяна Богдева (Директор)
27.02.2019г. 17:30ч.
ОДЗ-Пловдив



Електронният подпись се намира в отделен файл с название signature.txt.p7s