**УТВЪРЖДАВАМ: ……………/п/……………….**

**/инж. Слави Димитров/**

**ДИРЕКТОР ОД „ЗЕМЕДЕЛИЕ” - ВРАЦА**

ВЪТРЕШНИ ПРАВИЛА

**ЗА УСЪЩЕСТВЯВАНЕ НА КОНТРОЛ И УПРАВЛЕНИЕ НА ИЗГРАДЕНИТЕ СИСТМИ ЗА МРЕЖОВА И ИНФОРМАЦИОННАТА СИГУРНОСТ В ОБЛАСТНА ДИРЕКЦИЯ "ЗЕМЕДЕЛИЕ” - ВРАЦА.**

**гр. ВРАЦА**

**2023 г.**

**РАЗДЕЛ I**

**ОБЩИ ПОЛОЖЕНИЯ**

Чл. 1. Настоящите правила имат за цел осигуряването на контрол и управление на работата на информационните системи в ОД „Земеделие” – Враца. 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, като и да обменят информация чрез съответните устройства и програми. Програмните продукти и бази данни могат да бъдат специфични за всяко звено към ОД „Земеделие” или с общо предназначение.

Чл. 2. Потребителите на информационни системи в ОД „Земеделие”– Враца са задължени с отговорни действия да гарантират ефективното и ефикасно използване на системите.

Чл. 3. Със заповед на директора на ОД „Земеделие” – Враца се определя служител, който отговаря за мрежовата и информационна сигурност на използваните информационни системи.

Чл. 4. Създаването, разместването, преконфигурирането на звена и работни места в ОД „Земеделие”– Враца, на чието разположение са или се предвижда да бъдат предоставени компютри се съгласува със определения служител по чл. 3.

**ЦЕЛ**

**Чл. 5.** 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“ - Враца източници, умишлени или случайни.

**Чл. 6.**  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 й 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 ІІ**

**КОНТРОЛ НА ДОСТЪПА И ПРАВИЛА ЗА РАБОТА С НОСИТЕЛИ**

**Чл. 7.** 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 служител на ОД “Земеделие“ - Враца.

**Чл. 8.** Всеки служител има точно определени права на достъп и използва уникален потребителски профил за вход в системата и достъп до данните, за които е оторизиран, така че да може да бъде идентифициран. Не е разрешено използването на групови профили;

**Чл. 9.** Контрол на управлението и защитата на достъпа до мрежови връзки и мрежови услуги се извършва чрез средствата на активна директория с конкретно потребителско име, осигурено от Системния администратор, който контролира компютрите, използвани за достъп до мрежи и мрежови услуги.

**Чл. 10.** Предоставянето на достъп става по дефиниран вътрешен ред, като се задават определени права на достъп до конкретни информационни ресурси, според заемната длъжност и функция. Не се задава и не се осигурява достъп на неоторизирани лица.

**Чл. 11.** Лицата, които обработват лични данни, използват уникални пароли с достатъчна сложност, които не се записват или съхраняват онлайн;

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

**Чл. 13** На служителите на ОД “Земеделие“ - Враца, които използват електронни бази данни и техни производни (текстове, разпечатки, карти и скици) се забранява:

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

2.да ги използват извън рамките на служебните си задължения;

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

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

1.унищожаване на бази данни или части от тях;

2.повреждане на бази данни или части от тях;

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

**Чл. 15.** При изнасяне на носители извън физическите граници на ОД “Земеделие“ - Враца, те се поставят в подходяща опаковка и в запечатан плик.

**Чл. 16.** 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. 17.** 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. 18.** След като повече не са необходими, носителите се унищожават сигурно и безопасно за намаляване на риска от изтичане на чувствителна информация към неупълномощени лица. Физическото унищожаване на информационните носители става със счупване. Предварително се проверят, за да е сигурно, че необходимата информация е копирана и след това цялата информация е изтрита от тях преди унищожаване.

**РАЗДЕЛ IIІ**

**ПОЛЗВАНЕ НА КОМПЮТЪРНАТА МРЕЖА И ИНТЕРНЕТ**

**Чл. 19.** Определения служител по чл.3 извършва необходимите настройки за достъп до интернет, създават потребителски имена и пароли за работа със Система за управление на документооборота и работния поток- „Eventis“ и електронната поща на ОД “Земеделие“ - Враца.

**Чл. 20.** Ползването на компютърната мрежа и електронната поща от служителите става чрез получените потребителско име и парола или електронен подпис /Doc или Doc Pro/.

**Чл. 21.** Служителите на ОД “Земеделие“ - Враца са длъжни да не споделят своите потребителски имена и пароли с трети лица и носят дисциплинарна отговорност, ако се установи неправомерно ползване на ресурсите на компютърната мрежа, достъпа до интернет или електронна поща при използване на предоставените им потребителски имена и пароли.

**Чл. 22.** Компютрите, свързани в мрежата на ОД “Земеделие“ - Враца и използват интернет само от доставчик, с когото дирекцията има сключен договор за доставка на интернет.

**Чл. 23.** Забранява се свързването на компютри едновременно в мрежата на ОД “Земеделие“- Враца 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.

**МЕРКИ ЗАЩИТА ОТ КОМПЮТЪРНИ ВИРУСИ И ДРУГ ЗЛОВРЕДЕН СОФТУЕР**

**Чл. 24.** Защитата срещу нежелан софтуер в информационните системи на ОД “Земеделие“ - Враца се организира от служителя, отговарящ за мрежовата и информационната сигурност в дирекцията.

**Чл. 25.** Съгласно чл.45, ал.1 от Наредбата за общите изисквания за мрежова и информационна сигурност Директорът на ОД “Земеделие“ - Враца, осигурява мерки за физическата защита на информационните системи в дирекцията и общинските служби по земеделие/ Приложение1/.

**Чл. 26** Съгласно чл.41 от Наредбата за и общите изисквания за мрежова и информационна сигурност,мерките за защита срещу нежелан софтуер се организират от служителя отговарящ за мрежовата и информационната сигурност в администрацията. /Приложение 2/

**Чл. 27.** 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. 28.** Директорът на ОД “Земеделие“ - Враца осигурява условия, при които неовластени лица не могат да получат физически достъп до работните станции и сървърите, използвани от администрацията.

**Чл. 29.** Директорът на ОД “Земеделие“ - Враца, утвърждава план за действие при инциденти, свързани с мрежовата и информационната сигурност на използваните от тях информационни системи, с цел осигуряване непрекъсване на дейността на съответната администрация.

**Чл. 30.** При установяване на открити опити за проникване трябва 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.

**Чл. 31.** 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.

**Чл. 32.** С цел антивирусна защита в ОД “Земеделие“ - Враца 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:

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 поява на съобщение от антивирусната програма за вирус в локалната мрежа, всеки служител от общинска служба или в дирекцията задължително информира Системния администратор.

**Чл. 33.** **Организационни мерки за защита:**

1. Превенция за възникнали уязвимости и осъществени атаки:

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

**Чл. 34.** **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 нае 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 уязвими 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). Ограничаване на софтуера който може да бъде инсталиран и изпълняван върху работните станции.

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

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

**Чл. 35.** **Мерки за мрежова сигурност**

Във връзка с повишения риск от кибер - атаки и инциденти, както и увеличаване на злонамерените действия и щетите, които нанасят с цел запазване на целостта, автентичността, наличността и достъпността на информацията, и системите и регистрите в които тя се събира, обработва, използва и съхранява се предприемат следните мерки:

1.Мониторинг на комуникационните канали осигуряващи свързаността на ОД “Земеделие“- Враца;

2.Наблюдение на параметри за нормалното функциониране на ИКТ инфраструктурата в ОД “Земеделие“ - Враца;

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

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

5.Своевременно уведомяване на администраторите при настъпили отклонения в наблюдаваните параметри, за да бъдат предприети адекватни мерки за отстраняването на проблема;

**Чл. 36. Мерки за защита на приложения и данни:**

1.При ползване на приложения и данни от вътрешната мрежова инфраструктура, мерките за защита се отнасят за решения свързани със съвместната работа на различни приложения и услуги- електронна поща, вътрешни портали, файлови услуги, комуникация в реално време и др.

1.1. 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.

1.2. За защита на услугата електронна поща да се извършва сканиране на входящ и изходящ трафик .

1.3.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.

* 1. Достъпът на служителите до работните им станции и общите информационни

системи се осъществява със служебни потребителско име и парола.

**Чл. 37. 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.

3.При срив в локалната компютърна мрежа, всеки потребител следва да запише файловете, които е отворил на локалния си компютър, за да се избегне загуба на информация. При възстановяване на мрежата, всички локално запазени файлове следва да се преместят отново на сървъра и да се изтрият локалните копия.

**БАЗИ ДАННИ**

Чл. 38. Обменът на електронни бази данни става само след одобряване от директора на ОД „Земеделие” – Враца.

Чл. 39. Служителите на съответните работни места, които въвеждат и актуализират бази данни са длъжни да ги поддържат в актуално състояние.

Чл. 40. При наличие на изисквания към съдържанието и структурата на бази данни, поставени с нормативни документи, създаваните и използвани бази данни задължително се съобразяват с тези изисквания.

Чл. 41. Определеният служител по чл. 3 създава сървър места за съхраняване на данни за всяко едно от звената, където служителите правят копия на файловете, с които работят. Архивирането на външни носители се извършва от отговорния служител веднъж месечно, като архивните носители се надписват и съхраняват в огнеупорен шкаф в помещение, различно от това, където са разположени сървърите.

Чл. 42. Всички действия по подготовката на данни за въвеждане в информационна система, а именно: събиране, актуализиране, сортиране и подреждане се извършват съобразно организация, създадена в съответните звена.

Чл.43. Въвеждането и актуализацията на така подготвените данни с цел създаване на електронни бази данни се извършва от съответните специалисти по звена, съобразно длъжностните им характеристики и при спазване на определените права на достъп.

Чл. 44. Форматите на електронните бази данни се определят съобразно нормативните актове и стандарти в тази област. Ако такива не съществуват, форматите се определят от определения служител по чл. 3, съобразно съвместимостта с използваните в ОД „Земеделие” – Враца бази данни, възможностите за обмен на съвместими данни с МЗХ, други Областни дирекции Земеделие, държавни учреждения и институции, предимствата на определена система за управление на бази данни (СУБД), международни стандарти.

Чл. 45. Служителите, извършващи въвеждане и актуализация на данните носят отговорност за тяхната достоверност.

Чл. 46. Издаването на документи при използване на съответната електронна база данни се извършва от съответните служители по звена, съобразно длъжностните им характеристики.

Чл. 47. За общо ползване от всички специалисти са предвидени бази данни, съдържащи действащите и отменени нормативни документи, практиките на съдилищата, образци от документи и др. съобразно съдържанието на ползваните програмни продукти.

Чл. 48. Правата на достъп до общи бази данни за определено звено са „разглеждане на данните” – в зависимост от предмета на дейност на съответното звено и необходимата за дейността му информация, които се определят съобразно потока на информацията в ОД „Земеделие” – Враца, мястото на съответното звено във функционалната структура на дирекцията и длъжностните характеристики на съответните служители.

Чл. 49. На служителите на ОД „Земеделие” – Враца 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;

2. да ги използват извън рамките на служебните си задължения;

3. да ги предоставят на външни лица;

Чл. 50. За нарушение на целостта на данните се считат следните действия:

1. унищожаване на бази данни или части от тях;

2. повреждане на бази данни или части от тях;

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

Чл. 51. Определеният служител по чл. 3 предлага и реализира концепции за защита и опазване на електронни бази данни.

Чл. **52.** Събирането, подготовката и въвеждането на данни директно в специфични раздели на страницата на ОД „Земеделие” – Враца, се извършва от определения служител по чл. 3, посредством предоставени от МЗХ потребителски имена и пароли за извършване на актуализациите.

Чл. **53.** За всички останали раздели на интернет страницата на администрацията директорите на дирекции, разпореждат събирането и подготовката на данните от служителите в техния ресор, след което данните се предоставят в електронен вид (на файлове) на определения служител по чл. 3, от където данните се поставят директно на интернет страницата.

Чл. **54.** Копия от всички данни, изпращани за публикуване на интернет страницата на ОД „Земеделие” – Враца се записват и съхраняват на компютър или магнитооптичен носител при определения служител по чл. 3.

**РАЗДЕЛ IV**

**ТЕХНИЧЕСКО ОСИГУРЯВАНЕ – КОМПЮТЪРНА И ПЕРИФЕРНА ТЕХНИКА**

**Чл. 55.** Техническото осигуряване се избира с оглед на изискванията на програмните продукти, които ще се използват на съответното работно място, както и със състоянието и тенденциите за развитие на компютърните технологии. Компютърната конфигурация се определя от служителя по чл. 3.

**Чл. 56.** Подмяна на части, добавяне на компоненти, принадлежности и други за подобряване на компютърните конфигурации се извършват по преценка на определения служител по чл. 3.

**Чл. 57.** Инсталирането на компютърните конфигурации, системните и приложните програми, както и следващи промени в тях се прави само от определения служител по чл. 3. Или упълномощените за това фирми – доставчици на компютърна, периферна техника и програмни продукти, но задължително в присъствие на определения служител по чл. 3.

**Чл. 58.** Гаранционното обслужване на техника се извършва само от упълномощените за това фирмени сервизи.

**Чл. 60.** Техническото обслужване (поддръжка), доколкото не се изисква намеса на упълномощен сервиз и дейности по ремонт, се извършва от определения служител по чл. 3. При необходимост от извънгаранционен ремонт и в случай, че не сключен договор за абонаментна поддръжка, определения служител по чл. 3 е длъжен да се погрижи за техниката като се свърже с този фирмен сервиз, който може да осигури най-бързото, качествено и безпроблемно възстановяване.

**Чл. 61.** Компютърна и периферна техника, която не се използва, се предава на определения служител по чл. 3, като по негова преценка техниката се пренасочва към работни места, които имат нужда от такава.

**Чл. 62.** Внасянето и изнасянето на компютърна и периферна техника от сградата на ОД „Земеделие” – Враца става само в присъствието на определения служител по чл. 3 или при наличие на съответния приемо-предавателен протокол

**РАЗДЕЛ V**

**ПОЛЗВАНЕ НА КОМПЮТЪРНА МРЕЖА И ИНТЕРНЕТ**

**Чл. 63.** Определеният служител по чл. 3 извършва необходимите настройки за достъп до интернет, създава потребителски имена и пароли за работа с компютърната мрежа и електронната поща на ОД „Земеделие” – Враца.

**Чл. 64.** Ползването на интернет и служебна електронна поща се ограничават съобразно скоростта на ползвания достъп до интернет, броя на откритите работни места и необходимостта от ползване на тези услуги съобразно служебните задължения на служителите.

**Чл. 65.** Служителите на съответните работни места са длъжни да не споделят своите потребителски имена и пароли с трети лица и носят дисциплинарна отговорност, ако се установи неправомерно ползване на ресурсите на компютърната мрежа, достъпа до интернет или електронна поща при използване на предоставените им потребителски имена и пароли.

**Чл. 66.** Компютрите, свързани в мрежата на ОД „Земеделие” – Враца използват интернет само от доставчик, с когото дирекцията има сключен договор за доставка на интернет.

**Чл. 67.** Забранява се отварянето на получени по електронна поща съобщения, които съдържат неразчитаеми знаци без контрол от страна на определения служител по чл. 3

**РАЗДЕЛ VI**

**ПРАВА НА ДОСТЪП ДО ИНФОРМАЦИОННИ РЕСУРСИ**

**Чл. 68.** При назначаване на нов служител или служител по заместване, служителят по човешки ресурси уведомява за това определения служител по чл. 3, не по-късно от 3 работни дни преди датата на назначаване с оглед задаване на права на достъп до определени информационни ресурси.

**Чл. 69.** При прекратяване на служебното (трудовото) правоотношение между ОД „Земеделие” – Враца и определен служител, служителят по човешки ресурси уведомява за това определения служител по чл. 3 не по-късно от 3 работни дни преди датата на прекратяване. С изтичане на работния ден, предхождащ прекратяването на правоотношенията със служителя, определения служител по чл. 3 прекратява правата на достъп до мрежови ресурси, електронна поща и компютър на служителя, след което се извършва преинсталация на компютъра.

**РАЗДЕЛ VII**

**ОЦЕНКА И УПРАВЛЕНИЕ НА РИСКА ЗА МРЕЖОВА И ИНФОРМАЦИОННА СИГУРНОСТ**

**Чл. 70.** Видовете заплахи, които могат да застрашат конфиденциалността, интегритета и достъпността, са следните:

1. Подслушване, изразяващо се в достъп до служебна информация чрез прихващане на електронни съобщения независимо от използваната технология.

2. Електромагнитно излъчване, изразяващо се в действия на трето лице, целящо да получи знание за обменяни данни посредством информационна система.

3. Нежелан код, който може да доведе до загуба на конфиденциалността чрез записването и разкриването на пароли и до нарушаване на интегритета при интервенции от трети лица, осъществили нерегламентиран достъп с помощта на такъв код. Нежелан код може да се използва, за да се заобиколи проверка за достоверност, както и всички защитни функции, свързани с нея. В резултат кодът може да доведе до загуба на достъпността, когато данните или файловете са разрушени от лицето, получило нерегламентиран достъп с помощта на нежелан код.

4. Маскиране на потребителската идентичност може да доведе до заобикаляне на проверката за достоверност и всички услуги и защитни функции, свързани с нея.

5. Погрешно насочване или пренасочване на съобщенията може да доведе до загуба на конфиденциалност, ако се осъществи нерегламентиран достъп от трети лица. Погрешното насочване или пренасочване на съобщенията може да доведе и до нарушаване на интегритета, ако погрешно насочените съобщения са променени и след това насочени към първоначалния адресат. Погрешното насочване на съобщения води до загуба на достъпността до тези съобщения.

6. Софтуерни грешки могат да застрашат конфиденциалността, ако софтуерът е създаден с контрол на достъпа или за криптиране или ако грешка в софтуера осигури възможност за нежелан достъп в информационна система.

7. Кражбата на информационни активи може да доведе до разкриване на информация, която представлява служебна или друга защитена от закона тайна. Кражбата може да застраши достъпността до данните или информационното оборудване.

8. Нерегламентиран достъп до компютри, информационни ресурси, услуги и приложения може да доведе до разкриване на поверителни 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.

9. Нерегламентиран достъп до носител на данни може да застраши съхраняваните върху него данни.

10. Повреждане на носител на информация може да наруши интегритета и достъпността до данните, които се съхраняват на този носител.

11.Грешка при поддръжката. Неизвършването на редовна поддръжка на информационните системи или допускане на грешки по време на процеса по поддръжка може да доведе до нарушаване на достъпността до данни.

12. 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.

13. Технически аварии (например аварии в мрежите) могат да нарушат интегритета и достъпността до информация, която се съхранява или разпространява чрез тази мрежа.

14. Грешки при предаването на информацията могат да доведат до нарушаване на нейната цялост и достъпност.

15. 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, и програмите и информацията се използват, за да се изменят съществуващи програми и данни по неразрешен начин или ако те съдържат нежелан код.

16. Потребителски грешки могат да нарушат интегритета и достъпността до данни чрез неумишлено или умишлено действие.

17. Липса на потвърждаване може да застраши интегритета на данните. Предпазните мерки за предотвратяване на непотвърждаването трябва да се прилагат в случаите, когато е важно да се получи доказателство за това, че дадено съобщение е изпратено и е/не е получено, както и за това, че мрежата е пренесла съобщението.

18. Интервенции срещу интегритета на данните могат да доведат до тяхното сериозно увреждане и до невъзможност от по-нататъшното им използване.

19. Аварии в комуникационното оборудване и услуги могат да увредят достъпността на данните, предавана чрез тези услуги.

20. Външни въздействия с огън, вода, химикали и др. могат да доведат до увреждане или унищожаване на информационното оборудване.

21. Злоупотреба с ресурси може да доведе до недостъпност до данни или услуги.

22. Природни бедствия могат да доведат до унищожаване на данни и информационни системи.

23. Претоварване на комуникационния трафик може да доведе до нарушаване на достъпността до обменяни данни.

**Чл. 71.** Управлението на защитата от нерегламентиран достъп се категоризира на няколко степени в зависимост от оценките на потенциалните последствия при нарушаване на конфиденциалността, интегритета и/или достъпността, както следва:

1. ограничено- организацията продължава да изпълнява функциите си, но с понижена ефективност, на информационните активи са причинени незначителни вреди и финансовите загуби са незначителни;

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

3. високо - загубата на конфиденциалност, интегритет и/или достъпност оказва тежко или непоправимо въздействие на администрацията, при която тя загубва способност да изпълнява основните си функции, на информационните активи са причинени тежки вреди и финансовите загуби са много големи.

**Чл. 72.** Средствата за управление на достъпа позволяват да се определят и контролират действията, които различни ползватели на информационните системи и процеси в тях могат да извършват по отношение на информационни ресурси. Логическото управление на достъпа трябва да позволява да се определят множество допустими операции за всеки ползвател или процес и да се контролира изпълнението на установените правила.

**Чл. 73**. Всяко самостоятелно звено на администрацията управлява идентификаторите на ползвателите на информационните системи чрез:

1. уникална идентификация на всеки ползвател;

2. верификация на идентификатора на всеки ползвател;

3. регламентиране на административните процедури за разпространение, заместване на загубени, компрометирани или повредени идентификатори;

4. прекратяване действието на идентификатора след определен период на липса на активност;

5. архивиране на идентификаторите.

**РАЗДЕЛ VIII**

**ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ**

**Чл. 74.** Ръководителите и служителите в ОДЗ и ОСЗ са длъжни да познават и спазват разпоредбите на тези правила.

**Чл. 75.** Контролът по спазване на правилата се осъществява от директорите на дирекции.

**Чл. 76.** Настоящите вътрешни правила се разглеждат и оценяват периодично с оглед ефективността й, като ОД „Земеделие“ - Враца може да приема и прилага допълнителни мерки и процедури, които са целесъобразни и необходими с оглед защитата на информацията.

**Чл. 77.** Тези правила са разработени съгласно последните измениения на Закона за киберсигурността и Наредбата за минималните изисквания за мрежова и информационна сигурност.

**Чл. 78.** Настоящите Вътрешни правила отменят предходните такива, утвърдени с Заповед № 28/18.02.2019 г. на директора на ОД „Земеделие“ – Враца.