МИНИСТЕРСТВО НА ЗЕМЕДЕЛИЕТО
СЕВЕРОИЗТОЧНО ДЪРЖАВНО ПРЕДПРИЯТИЕ
Адрес: гр. Шумен, ПК 9700, ул. "Петра" № 1, тел.:054/ 833-123, факс: 054/ 833-123, e-mail: office@sidp.bg, www.sidp.bg

УТВЪРДИЛ:……(П)…….
инж. Ради Иванов
Директор на СИДП ДП - Шумен

ВЪТРЕШНИ ПРАВИЛА ЗА МРЕЖОВА И ИНФОРМАЦИОННА СИГУРНОСТ ЗА ТП ДГС/ДЛС КЪМ СИДП ДП- гр. ШУМЕН

/в сила от 01.04.2023 година/

„Североизточно държавно предприятие“ ДП, гр. Шумен
2023

Съдържание

I. ОБЩИ ПОЛОЖЕНИЯ

1. Настоящите Вътрешни правила се утвърждават на основание чл. 1, ал.1, т.5 от Наредбата за минималните изисквания за мрежова и информационна сигурност и имат за цел осигуряването на контрол и управление на работата на информационните системи в териториалните поделения (ТП) ДГС/ДЛС на ТП ДГС/ДЛС ДП. В този смисъл понятието информационна система се определя като съвкупност от компютърна и периферна техника, програмни продукти, данни и обслужващ персонал, като компютрите могат да бъдат свързани в локална мрежа или по друг начин, както и да обменят информация чрез съответните устройства и програми. Програмните продукти и бази данни могат да бъдат специфични за всяко звено от администрацията или с общо предназначение.

2. Потребителите на информационни системи в ТП ДГС/ДЛС са задължени с отговорни действия да гарантират ефективното и ефикасно използване на системите.

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 минималните изисквания за мрежова и информационна сигурност *(ДВ, бр. 59 от 19.07.2019 г.).*

II. КОНТРОЛ НА ДОСТЪПА И ПРАВИЛА ЗА РАБОТА С НОСИТЕЛИ

1. 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.
2. Контрол на управлението и защитата на достъпа до мрежови връзки и мрежови услуги се извършва от поддържащата компютърна техника (КТ) фирма, които контролират компютрите, използвани за достъп до мрежи и мрежови услуги.
3. Предоставянето на достъп става според заемната длъжност и функция, като се задават определени права на достъп до конкретни информационни ресурси. Не се задава и не се осигурява достъп на неоторизирани лица.
4. Лицата, които обработват лични данни, използват уникални пароли с достатъчно сложност, които не се записват или съхраняват онлайн.
5. Всички пароли за достъп на системно ниво се променят периодично.

6. Всички носители на лични данни се съхраняват в безопасна и сигурна среда, в заключени шкафове, с ограничен и контролиран достъп.

7. На служителите на ТП ДГС/ДЛС, които използват електронни бази данни и техни производни /текстове, разпечатки, дела, преписки и други/ се забранява:

(1) да ги изнасят под каквато и да е форма извън служебните помещения, освен с разрешение на Директора на стопанството;

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

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

8. 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.

9. При изнасяне на носители извън физическите граници на ТП ДГС/ДЛС, те се поставят в подходяща опаковка и могат да бъдат изнесени след разрешение на прекият ръководител на съответното звено.

11. 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.

12. 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.

13. 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.

14. Събирането, подготовката и въвеждането на данни на страницата на стопанството се извършва от определен служител/служители. На посочените длъжности лица администратор от ЦУ на СИДП създава потребителски имена и пароли за извършване на актуализациите.

15. Събирането и подготовката на данните се извършва от служители в техния ресор, след което данните се изпращат в електронен вид /на файлове/ на служителите отговорни за качването им на интернет страницата на® ТП ДГС/ДЛС.

III. РАБОТНО МЯСТО

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

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

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

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

5. Забранява се на външни лица работата с персоналните компютри на ТП ДГС/ДЛС, освен за упълномощени фирмени специалисти в случаите на сервизна намеса на място, но задължително в присъствие на изрично определен служител от ТП ДГС/ДЛС.

6. След края на работния ден всеки служител задължително изключва компютъра, на който работи, или го привежда в режим „log off“.

7. При загуба на данни или информация от служебния компютър, служителят незабавно уведомява поддържащата КТ фирма, които му оказва съответна техническа помощ.

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

9. Инсталиране и разместване на компютърни конфигурации и части от тях, на периферна техника, на активни и пасивни компоненти на локални компютърни мрежи, на комуникационни устройства се извършва само след разрешение от директора на стопанството.

10. Забранява се използването на непроверени преносими магнитни, оптични и други носители с възможност за презаписване на данни за прехвърляне на файлове между компютри, свързани в компютърната мрежа на ТП ДГС/ДЛС.

11. 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.

12. Достъпът до компютърна информация, бази данни и софтуер се ограничава посредством технически методи - идентификация на потребител, пароли, КЕП, проследяване на несанкциониран достъп.

IV. ПОЛЗВАНЕ НА КОМПЮТЪРНАТА МРЕЖА И ИНТЕРНЕТ

1. Поддържащата КТ фирма извършва необходимите настройки за достъп до интернет, създава потребителски имена и пароли за работа с компютърната мрежа и електронната поща в ТП ДГС/ДЛС.

2. Ползването на електронната поща от служителите става чрез получените от администратор от ЦУ на СИДП потребителско име и парола.

3. 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.

4. 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.

5. Компютрите, свързани в мрежата на ТП ДГС/ДЛС, използват интернет само от доставчик, с когото ТП ДГС/ДЛС има сключен договор за доставка на интернет.

6. Забранява се свързването на компютри едновременно в мрежата на ТП ДГС/ДЛС и в други мрежи, когато това позволява разкриване и достъп до IP адреси от мрежата на ТП ДГС/ДЛС и/или е в противоречие с изискванията на Закона за електронното управление (ЗЕУ) и Наредбата за минималните изисквания за мрежова и информационна сигурност (в сила от 26.07.2019 г.).

7. Забранява се съхраняването на сървърите на ТП ДГС/ДЛС на лични файлове с текст, изображения, видео и аудио.

8. Забранява се отварянето непроверени 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, архивни файлове и получени по електронна поща съобщения, които съдържат неразбираеми знаци.

V. ЗАЩИТА ОТ КОМПЮТЪРНИ ВИРУСИ И ДРУГ ЗЛОВРЕДЕН СОФТУЕР

1. С цел антивирусна защита се прилагат следните мерки:

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

(2) Поддържащата КТ фирма извършва следните дейности:

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

б) настройва антивирусния софтуер за периодични сканирания на файловите системи на компютрите за вируси;

в) активира защитата на различните програмни продукти за предупреждение при наличие на макроси и настройва защитната стена на система, освен в случаите когато работата с определени продукти или услуги на други институции не изискват различни настройки;

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

(3) При поява на съобщение от антивирусната програма за вирус в локалната мрежа, всеки служител от съответното работно място задължително информира поддържащата КТ фирма или системен администратор от ЦУ на СИДП.

VI. НЕПРЕКЪСНАТОСТ НА РАБОТАТА

1. Следните мерки се прилагат с цел антивирусна защита:

Всички сървъри и устройства за съхранение на данни да са свързани към устройство за непрекъсваемост на ел. снабдяването;

2. 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.

VII. СЪЗДАВАНЕ НА РЕЗЕРВНИ КОПИЯ

1. Поддържащата КТ фирма осигурява автоматизираното създаване на резервни копия на всички база данни.

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

(1) Автоматизирано и планово се извършва архивиране на цялата работна информация на сървърите и дисковите масиви;

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

(3) Съхраняват се най-малко последните три резервни копия;

VIII. ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

§ 1. Служителите в ТП ДГС/ДЛС са длъжни да познават и спазват разпоредбите на тези правила.

§ 2. Настоящите вътрешни правила се разглеждат и оценяват периодично с оглед ефективността им, като Североизточно държавно предприятие може да приема и прилага допълнителни мерки и процедури, които са целесъобразни и необходими с оглед защитата на информацията.

§ 3.Тези правила са разработени съгласно Наредбата за минималните изисквания за мрежова и информационна сигурност *(в сила от 26.07.2019 г.)* и влизат в сила от датата на утвърждаване на настоящите правила.