РАЗДЕЛ I

ОБЩИ ПОЛОЖЕНИЯ

Чл. 1 Настоящите Вътрешни правила се утвърждават на основание чл. 1, ал. 1, т. 1 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 ДГ № 140"Зорница". 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.

Чл. 2 Потребителите на информационни системи в ДГ № 140 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 минималните изисквания за мрежова и информационна сигурност (ДВ, БР. 59 от 19.07.2019 Г.)

РАЗДЕЛ II

КОНТРОЛ НА ДОСТЪПА И ПРАВИЛА ЗА РАБОТА С НОСИТЕЛИ

Чл..4 Защитата и контролът на информационните и компютърните системи се извършва при спазване на следните основни принципи:

ал. (1) разделяне на потребителски от администраторски функции;

ал. (2) установяване на нива и достъп до информация;

ал. (3) регистриране на достъпа, въвеждането, промяната и заличаването на данни и информация;

ал. (4) осъществяването на контрол от специализирани звена и служители на администрацията.

Чл. 5 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. 6 Контрол на управлението и защитата на достъпа до мрежови връзки и мрежови услуги се извършва чрез средствата на активна директория с конкретно потребителско име.

Чл. 7 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. 8 Лицата, които обработват лични данни, използват уникални пароли с достатъчно сложност, които не се записват или съхраняват онлайн;

Чл. 9 Всички пароли за достъп на системно ниво се променят периодично

Чл. 10 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. 11 На служителите на ДГ № 140, които използват електронни бази данни и техни производни (текстове, разпечатки, карти и скици) се забранява:

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

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

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

Чл. 12 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. 13 При изнасяне на носители извън физическите граници на ДГ № 140, те се поставят в подходяща опаковка и в запечатан плик.

Чл. 14 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. 15 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. 16 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.

Чл.17 Събирането, подготовката и въвеждането на данни на страницата се извършва от служители на ДГ № 140, определени със заповед на Директора. На посочените длъжности лица се създават потребителски имена и пароли за извършване на актуализациите.

Чл.18 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 ДГ № 140.

Чл.19 Работното място се състои от работно помещение, работна маса и стол, компютърна и периферна техника, комуникационни средства.

Чл.20 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.).

Чл.21 Сървъри на локални компютърни мрежи се разполагат в самостоятелни помещения обособени за целта.

Чл.22 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.

Чл.23 Служителят има право да работи на служебен компютър, като достъпът до съхраняваните данни се осъществява от него с въвеждането на потребителско име и парола;

Чл.24 Забранява се на външни лица работата с персоналните компютри на ДГ № 140, 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 изрично определен служител от ДГ № 140.

Чл.25 След края на работния ден всеки служител задължително изключва компютъра, на който работи, или го привежда в режим „log off";

Чл.26 При загуба на данни или информация от служебния компютър, служителят незабавно уведомява Системния администратор/ оторизираното за това лице, който му оказва съответна техническа помощ;

Чл.27 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;

Чл.28 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/ оторизираното за това лице.

Чл.29 Забранява се използването на преносими магнитни, оптични и други носители с възможност за презаписване на данни за прехвърляне на файлове между компютри.

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.

РАЗДЕЛ IV - ПОЛЗВАНЕ НА КОМПЮТЪРНАТА МРЕЖА И ИНТЕРНЕТ

Чл.34 Системния администратор/ оторизираното за това лице извършва необходимите настройки за достъп до интернет, създава потребителски имена и пароли за работа с компютърната мрежа и електронната поща в ДГ № 140.

Чл.35 Ползването на компютърната мрежа и електронната поща от служителите става чрез получените потребителско име и парола.

Чл.36 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.37 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.38 Компютрите, свързани в мрежата на ДГ № 140 използват интернет само от доставчик, с когото ДГ № 140 има сключен договор за доставка.

Чл.39 Забранява се свързването на компютри едновременно в мрежата на ДГ № 140 и в други мрежи, когато това позволява разкриване и достъп до IP адреси от мрежата на ДГ № 140 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.)

. **Чл.40** Забранява се инсталирането и използването на комуникатори (като icq, skype и др. подобни), осигуряващи достъп извън рамките на компютърната мрежа на ДГ № 140 „Зорница"и създаващи предпоставки за идентифициране на IP адрес на потребителя и за достъп на злонамерен софтуер.

Чл.41 Забранява се съхраняването на лични файлове с текст, изображения, видео и аудио.

Чл.42 Забранява се отварянето без контрол от страна на Системния администратор/ оторизираното за това лице:

ал. (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;

ал. (2) получени по електронна поща съобщения, които съдържат неразбираеми знаци

РАЗДЕЛ V ЗАЩИТА ОТ КОМПЮТЪРНИ ВИРУСИ И ДРУГ ЗЛОВРЕДЕН СОФТУЕР

Чл.43 С цел антивирусна защита се прилагат следните мерки

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

Чл.44 Следните мерки се прилагат с цел антивирусна защита:

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

РАЗДЕЛ VIII ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

§ 1. Ръководителите и служителите в ДГ № 140, са длъжни да познават и спазват разпоредбите на тези правила.

§ 2. Контролът по спазване на правилата се осъществява от директора.

§ 3. Настоящите вътрешни правила се разглеждат и оценяват периодично с оглед ефективността им.

§ 4. 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 извеждане на Заповед № 114 / 09.01.2026 г.г.