Утвърждавам:

**Д-Р ОРЛИН ДИМИТРОВ**

*Директор на Регионална здравна инспекция-Враца*

**ВЪТРЕШНИ ПРАВИЛА**

**ЗА МРЕЖОВА И**

**ИНФОРМАЦИОННА СИГУРНОСТ**

**В РЗИ-ВРАЦА**

РАЗДЕЛ I - ОБЩИ ПОЛОЖЕНИЯ

Чл. 1 Настощите вътрешни правила се утвърждават на основание чл. 1, ал. 1, т. от Наредбата за минималните изисквания за мрежова сигурност (приета с ПМС № 186 от 26.07.2019г.,) и имат за цел осигуряването на контрол и управление на работата на информационните системи в РЗИ гр. Враца. В този смисъл понятието информационна система се определя като съвкупност от компютьрна и периферна техника програмни продукти, данни и обслужващ персонал, като компютрите могат да бьдат свързани в локална мрежа или по друг начин, както и да обменят информация чрез сьответните устройства и програми.

Чл. 2 Потребителите на информационни системи са задължени с отговорни действия да гарантират ефективното и ефикасно използване на системите.

Чл.3 Проектирането и изграждането на информационни и комуникацонни системи се извършва така, че те да тредставляват компоненти с възможност за интеграция в единна потребителска среда и при спазване на Наредбата за минималните изисквания за мрежова сигурност (приета с ПМС № 186 от 26.07.2019г.).

# РАЗДЕЛ II – КОНТРОЛ НА ДОСТЬПА И ПРАВИЛА ЗА РАБОТА С НОСИТЕЛИ

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

1. Разделяне на потребителски от администраторски функции.
2. Установяване на нива на достьп до информация.

3. Регистриране на достьпа, въвеждането, промяната и заличаването на данни и информация.

4. Техниката да се използва изключително и само за служебни цели.

5. Не се позволява инсталирането на какъвто и да е нов и реконфигурирането от потребителите на вече инсталиран софтуер и хардуер, както и самостоятелни опити за

поправка или подобрения на горепосочените. При съмнение за възникнал проблем незабавно се уведомява дректора.

6. Не се позволява използването на внесени отвън софтуер и хардуер.

1. Използването на внесени отвън информационни носители (оптични дискове, дискети, флаш памети и др.) става при условие, че първо те се сканират за наличието на вируси. Ако антивирусният софтуер намери такива, носителите не се използват.
2. Не се допускат външни лица до комуникационните шкафове и техниката за интернет - връзка, с изключение на техници от оторизирани фирми, и то само придружени от материално-отгородно лице /домакин/. Не се допуска достьпа на външни лица до компютърната техника в офисите на инспекцията.
3. Служителите не могат да отстъпват паролите си за достьп до системата на други служители, външни лица, роднини и приятели.
4. Паролите за достьп на всичхи служители, описани по видове приложения се съхраняват от материално-отгородно лице. Всички пароли за достьп на системно ниво се променят периодично.

Чл. 5 Всеки служител има точно определени права на достьп и използва уникален потребителски профил за вход в системата и достьп 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, осигурено от материално-отговорното лице, който контролира компютрите, използвани за достъп до мрежи и мрежови услуги.

Чл. 7 Предоставянето на достьп 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 осигурва достьп на неоторизирани лица.

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

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

Чл. 10 Всички носители на лични данни се съхраняват в безопасна и сигурна среда с ограничен и контролиран достъп.

Чл. 11 На служителите в РЗИ-Враца, които използват електронни бази данни и техни производни (текстове, разпечатки, карти и скици и др.)се забранява:

1. да ги изнасят под каквато и да е форма извън служебните помещения без писмено разрешение от директора и преди извеждане от деловодството;
2. да ги използват извън рамките на служебните си задьлжения;
3. да ги предоставят на външни лица без да е заявена услуга.

Чл. 12 За нарушение целостта на данните се считат следните действия:

1. унищожаване на бази данни или части от тях;
2. повреждане на бази данни или частиот тях;
3. вписване на невярна информация в бази данни или части от тях.

Чл. 13 При изнасяне на носители извън физическите граници, те се поставят в подходяща опаковка и в запечатан плик.

Чл. 14 На служителите е строго забранено да използват мобилни компютьрни средства на места, кьдето може да вьзнихне риск за средството и информацията в него. Потребителите на мобилни компютьрни средства и мобилни телефони отоварят за защтата им от кражба и не ги оставят без наблюдение.

Чл.15 Служителите са длъжни да избягват всякакъв риск от достьп до информация от неупълномощени лица. Забранено е съобщаването на тайна и чувствителна информация по мобилни телефони на места, кьдето 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.

# РАЗДЕЛ Ш - РАБОТНО МЯСТО

Чл. 17 Работното място се състои от работно помещение, работна маса и стол, компютърна и периферна техника, комуникационни средства.

Чл. 18 Всеки служител отговаря за целостта на компютьрната и периферна техника, програмните продукти и данни, инсталирани на компютъра на неговото работно място.

Чл. 19 Служителят има право да работи на служебен компютър, като достьпът до съхраняваните данни се осъществява от него с въвеждането на потребителско име и парола;

Чл. 20 Забранява се на външни лица работата с персоналните компютри на РЗИ-Враца , освен за упълномощени фирмени специалисти в случаите на първоначална инсталация на компютьрна и периферна техника, програми, активни и пасивни компоненти на локални компютърни мрежи, комуникационни устройства и сервизна намеса на място, но задължително в присъствие на директор РЗИ, заместник-директор или друго упълномощено от него лице.

Чл. 21 След края на работния ден всеки служител задължително изключва компютъра, на който работи, или го привежда в режим log off;

Чл.22 При загуба на данни или информация от служебния компютър, служителят незабавно уведомява директора на РЗИ-Враца и му се оказва съответна техническа помощ;

Чл.23 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.24 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 съгласуване с директора.

Чл.25 Забранява се използването на преносими магнитни, оптични и други носители с възможност за презаписване на данни за прехвърляне на файлове между компютри, свързани в компютърната мрежа на РЗИ-Враца.

Чл.26 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.27 Архивирана компютърна информация се предоставя само на служители, които имат право на достъп, съгласно заеманата от тях длъжност и изпълнявана задача.

Чл.28 Достьпът до компютьрна 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.29 Достъпът до помещенията с комуникационните шкафове се ограничава по възможност само до специализиран по поддръжката им персонал.

# РАЗДЕЛ IV - ПОЛЗВАНЕ НА КОМПЮТЬРНАТА МРЕЖА И ИНТЕРНЕТ

Чл.30 Фирма ”Римекс” ООД - гр.Враца извършва необходимите настройки за достьп до интернет, разделя логически локалната мрежа на три отделни мрежи — локална мрежа за администрация, локална мрежа за специализирани дирекции и локална мрежа за мобилни екипи. Създава потребителски имена и пароли за работа с компютърната мрежа и електронната поща на РЗИ-Враца

Чл.31 Ползването на компютърната мрежа и електронната поща от служителите става чрез получените потребителско име и парола.

Чл.32 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.33 Служителите на съответните работни места да не споделят своите потребителски имена и пароли с трети лица и носят дисциплинарна отговорност, ако се установи неправомерно ползване на ресурсите на компютьрната мрежа, достъпа до интернет или електронна поща при използване на предоставените им потребителски имена и пароли.

Чл.34 Компютрите, свързани в мрежата на РЗИ-Враца използват интернет само от доставчик, с когото РЗИ -Враца има склочен договор за доставка на интернет.

Чл.35 Забранява се свързването на компютри едовременно в мрежата на РЗИ-Враца и в други мрежи, когато това позволява разкриване и достъп до IP адреси от мрежата на РЗИ-Враца и/или е в противоречие с изискванията на Наредбата за минималните изисквания за мрежова и информационна сигурност.

Чл.36 Забранява се инсталирането и използването на комуникатори (като skype, facebook, messenger, viber и др.подобни), осигуряващи достъп извън рамките на компютърната мрежа на РЗИ-Враца и създаващи предпоставки за идентифициране на адрес на потребителя и за достьп на злонамерен софтуер и мобилен код до компютрите, свърани в компютьрната мрежа на РЗИ-Враца

Чл.З7 Забранява се съхраняването на компютрите на РЗИ-Враца на лични файлове с текст, изображения, видео и аудо.

Чл.38 Забранява се отварянето без контрол от страна на системния администратор:

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 .ехе, .vbs, .reg и архивни файлове;

2. получени по електронна поща съобщения, които съдържат неразбираеми знаци;

РАЗДЕЛ V - ЗАЩИТА ОТ КОМПЮТЪРНИ ВИРУСИ И ДРУГ ЗЛОВРЕДЕН СОФТУЕР

Чл.39 С цел антивирусна защита се прилагат следните мерки:

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

ал. (2) DPO извършва следните дейности:

2.1. активира защитата на съответните ресурси - файлова система, електронна поща и извършва пьрвоначално 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;

ал.(З) При поява на съобщение от антивирусната програма за вирус в локалната мрежа, всеки служител от съответното работно място задължително информира DPO.

# РАЗДЕЛ VI - НЕПРЕКЪСНАТОСТ НА РАБОТАТА

Чл.40 Следните мерки се прилагат с цел антивирусна защита:

. Всички 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. DРО започва процедура по поетапно спиране на устройствата за съхранение на данни.

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.

# РАЗДЕЛ VII - СЪЗДАВАНЕ НА РЕЗЕРВНИ КОПИЯ

Чл. 41 Всеки служител, който работи с класифицирана информация, осигурява автоматично създаване на архивни копия всекидневно.

Чл. 42 Информацията, включително тази, съдържаща лични данни, се резервира по следния начин:

1. Автоматизирано и планово се извършва архивиране на цялата работна информация на запаметяващите устройства и дисковите масиви.
2. Архивирането на данните се извършва по начин, който позволява, при необходимост данните да бъдат инсталирани на друг компютър и да се продължи работният процес без чувствителна загуба на данни;

З. Базите данни се архивират всеки ден в края на работното време.

ал. (4) Споделените документи се резервират 2 пъти седмично.

ал. (5) Резервните копия се съхраняват на носител, различен от този, на който са разположени данните или електронните документи.

ал. (6) Съхраняват се най-малко последните три резервни копия.

ал. (7) Резервните копия се изпитват за консистентност и интегритет чрез пробно възстановяване на данни най-малко веднъж месечно.

## РАЗДЕЛ VIII - ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

 1. Рьководителите и служителите в РЗИ-Враца са длъжни да познават и спазват разпоредбите на тези правила.

2. Контролът по спазване на правилата се осъществява от директора на РЗИ-Враца.

 3. Настоящтте вътрешни правила се разглеждат и оценяват периодично с оглед ефективността им, като РЗИ-Враца може да приема и прилага допълнителни мерки и процедури, които са целесъобразни и необходими с оглед защитата на информацията.

4. Тези правила са разработени съгласно Наредбата за минималните изисквания за мрежова сигурност (прита с ПМС № 186 от 26.07.2019г.) и влизат в сила от датата на извеждане на Заповед № РД-01-175/17.06.2021 г, на Директора на РЗИ-Враца.