УТВЪРЖДАВАМ:

Изпълнителен Директор на Втора МБАЛ

Доц. Д-р……../ Стефан Узунов/

ВЪТРЕШНИ ПРАВИЛА ЗА МРЕЖОВА И ИНФОРМАЦИОННА СИГУРНОСТ ВТОРА МБАЛ -СОФИЯ

2022 г.

2022 г.

РАЗДЕЛ I
ОБЩИ ПОЛОЖЕНИЯ

Чл. 1 Настоящите правила имат за цел осигуряването на контрол и управление на работата на информационните системи във Втора МБАЛ – София ЕАД. 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 болничната администрация или с общо предназначение.

Чл. 2 Потребителите на информационни системи във Втора МБАЛ 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 2019 Г., В СИЛА ОТ 01.03.2019 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:

(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 специализирани звена и служители на болницата.

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 от Системния администратор, който контролира компютрите, използвани за достъп до мрежи и мрежови услуги.

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 Втора МБАЛ, 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. 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 части от тях;

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

Чл. 13 При изнасяне на носители извън физическите граници на Втора МБАЛ, 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 Втора МБАЛ, определени със заповед на изпълнителния директор на болницата. 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 болницата.

РАЗДЕЛ III

РАБОТНО МЯСТО

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 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.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 Забранява се на външни лица работата с персоналните компютри на Втора МБАЛ, 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 Системният администратор.

Чл.24 След края на работния ден всеки служител задължително изключва компютъра, на който работи, или го привежда в режим log off;

Чл.25 При загуба на данни или информация от служебния компютър, служителят незабавно уведомява Системния администратор, който му оказва съответна техническа помощ;

Чл.26 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.27 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 със Системният администратор

Чл.28 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 Втора МБАЛ.

Чл.29 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.30 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.31 Достъпът до помещенията, където са разположени сървърите и комуникационните шкафове се ограничава по възможност само до Системният администратор.

РАЗДЕЛ IV

ПОЛЗВАНЕ НА КОМПЮТЪРНАТА МРЕЖА И ИНТЕРНЕТ

Чл.32 Системният администратор извършва необходимите настройки за достъп до интернет, създава потребителски имена и пароли за работа с компютърната мрежа и електронната поща на Втора МБАЛ.

Чл.33 Ползването на компютърната мрежа и електронната поща от служителите става чрез получените потребителско име и парола.

Чл.34 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.35 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.36 Компютрите, свързани в мрежата на Втора МБАЛ използват интернет само от доставчик, с когото Втора МБАЛ има сключен договор за доставка на интернет след провеждане на процедура по реда на ЗОП.

Чл.37 Забранява се свързването на компютри едновременно в мрежата на Втора МБАЛ и в други мрежи, когато това позволява разкриване и достъп до IP адреси от мрежата на Втора МБАЛ 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. 5 ОТ 2019 Г., В СИЛА ОТ 01.03.2019 г.).

Чл.38 Забранява се инсталирането и използването на комуникатори (като icq, skype, viber и др. подобни), осигуряващи достъп извън рамките на компютърната мрежа на Втора МБАЛ и създаващи предпоставки за идентифициране на IP адрес на потребителя и за достъп на злонамерен софтуер и мобилен код до компютрите, свързани в компютърната мрежа на Втора МБАЛ.

Чл.39 Забранява се съхраняването на сървърите на Втора МБАЛ на лични файлове с текст, изображения, видео и аудио.

Чл.40 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 .exe, .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.41 С цел антивирусна защита 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 съответното работно място задължително информира Системния администратор.

РАЗДЕЛ VI

НЕПРЕКЪСНАТОСТ НА РАБОТАТА

Чл.42 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.

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.

РАЗДЕЛ VII

СЪЗДАВАНЕ НА РЕЗЕРВНИ КОПИЯ

Чл. 43. Длъжностно лице / системния администратор/, определено със Заповед на директора на 2МБАЛ осигурява автоматизираното създаване на резервни копия на всички база данни и електронни документи всеки ден.
Чл. 44. Информацията, включително тази, съдържаща лични данни, се резервира по следния начин:

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

(2) Архивирането на данните се извършва по начин, който позволява, при необходимост данните да бъдат инсталирани на друг сървър/ компютър и да се продължи работният процес без чувствителна загуба на данни;

(3) Базите данни на следните програми се архивират всяка вечер:

3.1. база данни на програмите Global HIS; - медицински дейности

3.2. база данни от програма „AIS“ - документооборот

3.3 база данни от програма ЛБД „Global Lab“– лабораторни медицински дейности

3.4 база данни от програма „Поликонт “ – личен състав и ТРЗ

3.5 база данни от програма “Архив” - документален архив

3.6 база данни от програма „AGFA“ – рентгенография

3.7 база данни от програма „ТБ“ – отчет на туберколозни заболявания

(4) Споделените документи се резервират 2 пъти седмично.

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

(6) Съхраняват се най-малко последните три резервни копия.
(7) Резервните копия се изпитват за консистентност и интегритет чрез пробно възстановяване на данни най-малко веднъж месечно.

РАЗДЕЛ VIII

ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

§ 1. Ръководителите и служителите в общинска администрация са длъжни да познават и спазват разпоредбите на тези правила.

§ 2. Контролът по спазване на правилата се осъществява от изпълнителния директор и определеното със заповед отговорно лице за гарантиране на мрежовата и информационната сигурност на използваните информационни системи във Втора МБАЛ.

§ 3. Настоящите вътрешни правила се разглеждат и оценяват периодично с оглед ефективността й, като Втора МБАЛ 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 общите изисквания за мрежова и информационна сигурност загл. изм. - дв, бр. 5 от 2017 г., и са утвърдени с решение на СД на Втора МБАЛ – София с протокол № 8 /15.03.2022г.