гр. Бургас, ул. “Христо Ботев” 42
тел./факс 817690 - директор
0885782294- зам. директор
0886108863- зам. директор web: http://ivazov-burgas.com
056 817693- канцелария e-mail: info-200227@edu.mon.bg

УТВЪРЖДАВАМ:

Виктор Григоров

Директор

ВЪТРЕШНИ ПРАВИЛА ЗА МРЕЖОВА И ИНФОРМАЦИОННА СИГУРНОСТ В СУ“ИВАН ВАЗОВ“, ГРАД БУРГАС

Заповед № РД-70/15.09.2025 г.

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 сигурност (приета с ПМС № 186 от 26.07.2019 г.,) и имат за цел осигуряването на контрол и управление на работата на информационните системи в СУ „ Иван Вазов“, град Бургас. 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 СУ „ Иван Вазов“, град Бургас, 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 сигурност (приета с ПМС № 186 от 26.07.2019г.).

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 на достъп до информация.
3. Регистриране на достъпа, 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 отговорния служител-госпожа Дарина Русенова.
6. Не се позволява използването на внесени отвън софтуер и хардуер.
7. 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.

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 отговорния служител. Не се допуска достъпа на външни лица до компютърната техника в канцеларииите в сградата на СУ „ Иван Вазов“, град Бургас

8. Служителите не могат да отстъпват паролите си за достъп до системата на други служители, външни лица, роднини и приятели.
9. Паролите за достъп на всички служители, описани по видове приложения се съхраняват от отговорния служител. Всички пароли за достъп на системно ниво се променят периодично.

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, осигурено от отговорния служител, 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 с ограничен и контролиран достъп.

Чл. 11 На служителите на СУ „Иван Вазов“, град Бургас 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; З. 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 СУ „ Иван Вазов“, град Бургас, 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. 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.

РАЗДЕЛ III
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 компютърната 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 достъпът 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, 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 директор, заместник директор или госпожа Дарина Русенова.

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 отговорния служител, който му 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 ръководителя на направление „ИКТ".

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.

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

ПОЛЗВАНЕ НА КОМПЮТЪРНАТА МРЕЖА И ИНТЕРНЕТ

Чл.30 Достъпът до компютърната мрежа и интернет се извършва първично от фирма „ВИВАКОМ-България" при изграждане на компютърната мрежа и се поддържа от отговорния служител-Дарина Русенова, която отговаря за необходимите настройки за достъп до интернет, разделя логически локалната мрежа на четири отделни мрежи — локална мрежа за администрация, локална мрежа за учители, локална мрежа за ученици и локална мрежа за гости. Създава потребителски имена и пароли за работа с компютърната мрежа и електронната поща на СУ „Иван Вазов", град Бургас.

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 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.34 Компютрите, свързани в мрежата на СУ „Иван Вазов“, град Бургас използват интернет само от доставчик, с когото институцията има сключен договор за доставка на интернет.
Чл.35 Забранява се свързването на компютри едновременно в мрежата на СУ „Иван Вазов“ и в други мрежи, когато това позволява разкриване и достъп до адреси от мрежата на СУ „Иван Вазов“, град Бургас 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 facebook, messenger, и др. подобни), осигуряващи достъп извън рамките на компютърната мрежа на СУ „Иван Вазов“, град Бургас 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 СУ „Иван Вазов“, град Бургас.
Чл. 37 Забранява се съхраняването на компютрите на СУ „Иван Вазов“, град Бургас на лични файлове с текст, изображения, видео и аудио.
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 .exe, .vbs, .reg и архивни файлове;
2. получени по електронна поща съобщения, които съдържат неразбираеми знаци.

РАЗДЕЛ IV
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) Госпожа Дарина Русенова: 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;
ал.(3) При поява на съобщение от антивирусната програма за вирус в локалната мрежа, всеки служител от съответното работно място задължително информира госпожа Дарина Русенова.

РАЗДЕЛ V
НЕПРЕКЪСНАТОСТ НА РАБОТАТА

Чл. 40 Следните мерки се прилагат с цел антивирусна защита:
1. 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., отговорният служител задейства процедура по поетапно спиране на устройствата за съхранение на данни.
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.

РАЗДЕЛ VI
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;
3. Базите данни на следните програми се архивират всеки ден в края на работното време:
3.1 база данни на програмата НЕИСПУО;
3.2 база данни от програма WTERES;
3.3 база данни от модул „Граждански договори“
3.4 3.4 база данни от програма FSD;
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 VII

ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

1. Ръководителите и служителите в СУ „Иван Вазов“, град Бургас са длъжни да познават и спазват разпоредбите на тези правила.

2. Контролът по спазване на правилата се осъществява от ръководството на СУ „Иван Вазов“, град Бургас

3. Настоящите вътрешни правила се разглеждат и оценяват периодично с оглед ефективността й, като СУ „Иван Вазов“, град Бургас 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 , приета с ПМС № 186 от 26.07.2019 г. и са утвърдени със заповед на директора № РД-70/15.09.2025 г.