ОСНОВНО УЧИЛИЩЕ "СТОЯН МИХАЙЛОВСКИ"
гр. Пловдив, ул. „Константин Геров“ № 45
ou_st.mihaylovski@oustmihaylovski.com
ou-stmihaylovski.com
тел.0877 807 230 – директор; 032/69-92-86 – канцелария

ВЪТРЕШНИ ПРАВИЛА ЗА МРЕЖОВА И ИНФОРМАЦИОННА СИГУРНОСТ В

ОУ „Стоян Михайловски“

град Пловдив

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 ОУ „Стоян Михайловски“ - Пловдив. 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 ОУ „Стоян Михайловски“ - ПЛОВДИВ 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.

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 се уведомява отговорното лице.
6. Не се позволява използването на внесени отвън софтуер и хардуер.
7. Използването на внесени отвън информационни носители (оптични дискове, 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.
8. Не се допускат външни лица до комуникационните шкафове и техниката за интернет- връзка, с изключение на техници от оторизирани фирми.
9. Не се допуска достъпа на външни лица до компютърната техника в канцеларите в сградата на ОУ „Стоян Михайловски“ - Пловдив.
10. Служителите не могат да отстъпват паролите си за достъп до системата на други служители, външни лица, роднини и приятели.

11. При създаване на нов профил в системата, служителят е длъжен да смени дадената му парола с нова. Паролата се помни и съхранява на сигурно място.

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 администратора на системата, който контролира компютрите, използвани за достъп до мрежи и мрежови услуги.

Чл. 7. Предоставянето на достъп става като се задават определени права 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 ОУ „Стоян Михайловски" - Пловдив, които използват електронни бази данни и техни производни се забранява:

- да ги изнасят под каквато и да е форма извън служебните помещения;
- да ги използват извън рамките на служебните си задължения;
- да ги предоставят на външни лица без да е заявена услуга.

Чл. 12. При изнасяне на носители извън физическите граници на ОУ „Стоян Михайловски" - Пловдив, те се поставят в подходяща опаковка и сигурна среда.

Чл. 13. На служителите е строго забранено да използват служебни мобилни компютърни средства на места, където може да възникне риск за средството и информацията в него.

Чл. 14. 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. 15. 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. 16. Работното място се състои от работно помещение, работна маса и стол, компютърна и периферна техника, комуникационни средства.

Чл. 17. Всеки служител отговаря за целостта на компютърната и периферна техника,

програмните продукти и данни, инсталирани на компютъра на неговото работно място.

Чл. 18. 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. 19. Забранява се на външни лица работата с персоналните компютри на ОУ „Стоян Михайловски" - Пловдив, 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 домакин;
- провеждане на обучения на външни педагогически специалисти по програми и проекти на МОН или РУО, но само след разрешението на Директора на училището.

Чл. 20. След края на работния ден всеки служител задължително изключва компютъра, на който работи.

Чл. 21. При загуба на данни или информация от служебния компютър, служителят сам носи отговорност.

Чл. 22. 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. 23. 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 на училището.

Чл. 24. 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. 25. 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. 26. Достъпът до помещенията с комуникационните шкафове се ограничава по възможност само до специализиран по поддръжката им персонал.

РАЗДЕЛ IV. ПОЛЗВАНЕ НА КОМПЮТЪРНАТА МРЕЖА И ИНТЕРНЕТ

Чл. 27. Компютрите, свързани в мрежата на ОУ „Стоян Михайловски" – Пловдив, използват интернет само от доставчик, с когото училището има сключен договор за доставка на интернет.

Чл. 28. Фирмата, доставчик на интернет услугата, изгражда вътрешна мрежа с необходимите мрежови комутатори, VLAN, рутери, защитни стени, VPN; избира техническите устройства, извършва 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 и създава потребителски имена и пароли за работа с компютърната мрежа.

Чл. 29. Ползването на компютърната мрежа и електронните платформи /Школо, Уча се, Електронни учебници и др./ от служителите става чрез получените потребителско име и парола.

Чл. 30. 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. 31. Служителите на съответните работни места са длъжни да не споделят своите потребителски имена и пароли с трети лица и носят отговорност, ако се установи неправомерно ползване на ресурсите на компютърната мрежа, достъпа до интернет или електронните платформи при използване на предоставените им потребителски имена и пароли.

Чл. 32. Използването на комуникатори (skype, facebook, messenger, viber, zoom и др. подобни), осигуряващи достъп извън рамките на компютърната мрежа на ОУ „Стоян Михайловски" - Пловдив 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 училището, да е ограничено и единствено и само за служебна цел.

Чл. 33. Забранява се отварянето без контрол от страна на системния администратор на:

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

Чл. 34. Не се толерира влизането в Интернет - сайтове с неизвестно съдържание.

РАЗДЕЛ V. ЗАЩИТА ОТ КОМПЮТЪРНИ ВИРУСИ И ДРУГ ЗЛОВРЕДЕН СОФТУЕР

Чл. 35. С цел антивирусна защита се прилагат следните мерки:

- Всички персонални компютри имат инсталиран антивирусен софтуер, който се обновява.
- При наличие на появило се съобщение със съмнително съдържание се уведомява отговорното лице. Забранява се на служителите да изпращат отговор на съмнителни съобщения.

Чл.36. При установяване на открити опити за пробив в ситемите следва незабавно:

1. да се уведоми Директора на училището и администратора за предприемане на адекватни мерки;
2. да се изключват или ограничават мрежовите услуги, свързани с информационния актив, обект на проникването.

РАЗДЕЛ VI. НЕПРЕКЪСНАТОСТ НА РАБОТАТА

Чл. 37. 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 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. 38. Всеки служител, който работи с класифицирана информация, осигурява автоматично създаване на архивни копия всекидневно.

Чл. 39. Информацията, включително тази, съдържаща лични данни, се резервира по следните начини:

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:

- база данни на програмата НЕИСПУО,

РАЗДЕЛ VIII. КИБЕРЗАЩИТА, ИНСТИТУЦИОНАЛНА НЕУТРАЛНОСТ И ПРЕВЕНЦИЯ В УЧИЛИЩНАТА ОБЩНОСТ

1. Институционална неутралност и комуникационен протокол: - Всички педагогически и непедагогически специалисти стриктно спазват принципа на институционална неутралност Забранява се воденето на субективни дискусии, изказването на неофициални мнения и разпространяването на слухове/спекулации относно възникнали

инциденти с ученици
- Всички служители и ученици спазват Етичния кодекс на училищната общност.
- При запитвания от медии или външни лица служителите не дават самостоятелни изявления, а пренасочват въпросите директно към Директора на училището.
2. Обучения за киберсигурност и превенция на насилието сред учениците: - Педагогическият съветник съвместно с класните ръководители провеждат беседи и обучения за безопасно поведение във виртуалната среда, киберсигурност и защита на личната информация онлайн,
- Реализират се дейности за превенция на кибертормоза, недопускане на език на омразата, провокации и споделяне на непотвърдена информация в интернет и в училище.
- Развиват се социално-емоционалните компетентности за критично възприемане на съдържание в социалните мрежи.
3. Взаимодействие с родителите: - Класните ръководители провеждат тематични родителски срещи / консултации за киберсигурността, безопасността на децата в дигиталното пространство, поставянето на граници, родителския контрол и зачитането на индивидуалността на юношите
. - Чрез електронния дневник и официалните канали се отправят регулярни апели към родителите за съдействие и повишен контрол върху коментарите и изявите на учениците в социалните mrevi. 4. Психологическа подкрепа и реакция при кризи: - Педагогическият съветник своевременно идентифицира и оценява нуждата от психологическа подкрепа сред ученици и служители
- При нужда от специализирана подкрепа от Националната мобилна група за психологическа подкрепа (НМГПП), педагогическият съветник незабавно уведомява Директора за задействане на процедура пред РУО – Пловдив,
- Училището оказва пълно съдействие на МВР, РУО, АСП/ДСП по въпросите на превенцията на тормоза и насилието.

РАЗДЕЛ XI. ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

§ 1. Ръководителите и служителите в ОУ „Стоян Михайловски“ - Пловдив са длъжни да познават и спазват разпоредбите на тези правила.

§ 2. Контролът по спазване на правилата се осъществява от ръководството на ОУ „Стоян Михайловски“ – Пловдив.

§ 3. Настоящите вътрешни правила се разглеждат и оценяват периодично с оглед ефективността им, като ОУ „Стоян Михайловски“ - Пловдив 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 26.07.2019г.) и влизат в сила от датата на извеждане на Заповед № РД-10- /15.09.2026 г. на Директора на ОУ „Стоян Михайловски“ – Пловдив. Разгледани са на Педагогически съвет на 09.09.2026 г. с протокол № 7 и предстои запознаване с Правилата на Общо събрание.