



ЗАПОВЕД

№ РД-10-3178/14.09.2023г.

На основание чл. 259, ал.1 от ЗПУО и във връзка с чл. 3, ал. 2 и ал. 4 от Закона за киберсигурност, както и чл. 1, ал.1, т.5 и чл. 4 от Наредбата за минималните изисквания за мрежова и информационна сигурност

УТВЪРЖДАВАМ

Вътрешни правила за мрежова и информационна сигурност на Средно училище „Черноризец Храбър“, в сила от 14.09.2023 г.

НАРЕЖДАМ

1.Непосредствено след издаването на настоящата заповед всички служители от педагогическия и непедагогически персонал да се запознаят с Вътрешните правила за мрежова и информационна сигурност.

2.Вътрешните правила за мрежова и информационна сигурност да се публикуват на сайта на СУ „Черноризец Храбър“ град Пловдив

3.Родителите и настойниците да бъдат уведомени, че на сайта на СУ „Черноризец Храбър“ са публикувани Вътрешни правила за мрежова и информационна сигурност.

Контрол по изпълнението на заповедта ще изпълнявам лично.

Таня Атанасова, секретар да уведоми всички служители и работници с настоящата заповед.

Директор:

/Елена Кисьова/





Средно училище „Черноризец Храбър“

гр.Пловдив, ул.„Съединение“№9 тел: 032/ 68 28 49; e-mail: office@cherhrab.com

УТВЪРЖДАВАМ:

Елена Кисьова,

Директор на СУ „Черноризец Храбър“ град Пловдив

**ВЪТРЕШНИ ПРАВИЛА ЗА МРЕЖОВА
И ИНФОРМАЦИОННА СИГУРНОСТ
НА СРЕДНО УЧИЛИЩЕ
„ЧЕРНОРИЗЕЦ ХРАБЪР“
ГРАД ПЛОВДИВ**

I. ОБЩИ ПОЛОЖЕНИЯ

Чл.1. (1) Настоящите вътрешни правила определят политиката на мрежова и информационна сигурност на СУ „Черноризец Храбър“, Пловдив и имат за цел осигуряването на управление и контрол на работата на информационните системи на СУ „Черноризец Храбър“, Пловдив.

(2). В настоящите вътрешни правила 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. (1) Потребителите на информационни системи в СУ „Черноризец Храбър“, Пловдив са задължени с отговорни действия да гарантират ефективното и ефикасно използване на системите.

(2) Системата за сигурност на информацията в СУ „Черноризец Храбър“, Пловдив има за цел да защитава служителите, партньорите и клиентите на СУ „Черноризец Храбър“, Пловдив от незаконни или вредни действия на физически лица, пряко или косвено, съзнателно или несъзнателно при обработката на информация и лични данни, които са на тяхно разположение, а също така и при употребата на определено оборудване за изпълнение на служебните им задължения.

(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.).

II. КЛАСИФИКАЦИЯ НА ИНФОРМАЦИЯТА

Чл.3. (1) Всяка информация, която стане достъпна за служителите при изпълнение на служебните им задължения, ако са свързани със СУ „Черноризец Храбър“, Пловдив и негова дейност, клиенти или партньори за сътрудничество, се счита за собствена и поверителна информация на СУ „Черноризец Храбър“, Пловдив като по този начин се подчинява на защита в съответствие с приложимите закони и правната уредба относно защитата на поверителна информация, търговската тайна и личните данни.

(2) За да се установи подходяща защита на информацията, СУ „Черноризец Храбър“, Пловдив извършва класификация на информацията. Информацията подлежат на защита, независимо от това дали такава информация е на разположение на служителя под формата на печатни материали, устройства за съхранение на данни, аудио/видео материали или по друг начин.

Обща класификация на информацията, приложима в рамките на СУ „Черноризец Храбър“, Пловдив Категория	Описание	Примери (неизчерпателни)
Публична информация	Информация, която може да бъде обработвана и разпространявана в рамките на СУ „Черноризец Храбър“, Пловдив или извън него без никакво отрицателно въздействие върху СУ „Черноризец Храбър“, Пловдив някой от нейните партньори, клиенти и/или свързани лица.	а) Финансови отчети, публикувани до обществени органи; б) Информация, достъпна чрез публични ресурси или публично известна по друг начин, освен ако не е станала обществено достояние вследствие на действия на служители в нарушение на правилата за защита на информация
Вътрешна информация	Всяка употреба на информация по какъвто и да е начин, в случай, че е извършена в нарушение на изискванията на приложимите	а) Документи, разработени и/или изготвени от който и да е служител на СУ „Черноризец Храбър“, Пловдив; б) Всички директории (информация за
	закони или подзаконовни актове, тези Правила или всяка друга регулация, приета от СУ „Черноризец Храбър“, Пловдив може да навреди на интересите на СУ „Черноризец Храбър“, Пловдив и/или неговите служители, партньори и клиенти.	връзка и т.н.), установени и/или използвани за нуждите на СУ „Черноризец Храбър“, Пловдив в) Всякакви вътрешни работни бележки, изявления, становища, разработени за нуждите на СУ „Черноризец Храбър“, Пловдив или с цел ефективност на дейността на СУ „Черноризец Храбър“, Пловдив
Поверителна информация	Всяка информация от такова значение за СУ „Черноризец Храбър“, Пловдив неоторизираното разкриване на която би могло да окаже неблагоприятно въздействие върху дейността, операциите, репутацията, цялостното състояние СУ „Черноризец Храбър“, Пловдив, клиенти и партньори, като последица от такова разкриване, която би причинила сериозни вреди/щети на някое от тези лица.	а) Политики, процедури, вътрешни правила, управленски решения; б) Информация, за която е указано на служителя, че е търговска тайна на СУ „Черноризец Храбър“, Пловдив в) Друга информация от финансово, кадрово, правно, планове и операции; г) Данни за лична идентификация; д) Информация, която подлежи на защита по силата на споразумение за поверителност, което се подписва от дадения служител; е) Информация, която подлежи на защита по силата на споразумения за поверителност или споразумения за сътрудничество, които СУ „Черноризец Храбър“, Пловдив е сключило в хода на дейността си.

III. 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 административно звено, отговарящо за мрежовата и информационната сигурност
- (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.
- (8) Не се допускат външни лица до комуникационните шкафове и техниката за интернет връзка, с изключение на техници от оторизирани фирми, и то само придружени представителите на звеното, отговарящо за мрежовата и информационната сигурност. Не се допуска достъпа на външни лица до компютърната техника в канцелариите в сградата на СУ „Черноризец Храбър“, Пловдив.
- (9) Служителите не могат да отстъпват паролите си за достъп до системата на други служители, външни лица, роднини и приятели.
- (10) Паролите за достъп на всички служители, описани по видове приложения се съхраняват екипа отговарящ за мрежовата и информационната сигурност. 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. 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. 7. Лицата, които обработват лични данни, използват уникални пароли с достатъчна

сложност, които не се записват или съхраняват онлайн;

Чл. 8. Всички пароли за достъп на системно ниво се променят периодично;

Чл. 9. Всички носители на лични данни се съхраняват в безопасна и сигурна среда с ограничен и контролиран достъп.

Чл. 10. На служителите на СУ „Черноризец Храбър“, Пловдив, 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;

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

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

Чл. 11. 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. 12. При изнасяне на носители извън физическите граници на СУ „Черноризец Храбър“, Пловдив, те се поставят в подходяща опаковка и в запечатан плик.

Чл. 13. 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. 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.

IV. 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 СУ „Черноризец Храбър“, 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.

- 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 незабавно уведомява Административно звено, отговарящо за мрежовата и информационната сигурност което му оказва съответна техническа помощ;

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 размятане 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 Административно звено, отговарящо за мрежовата и информационната сигурност;

Чл.24. 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 СУ „Черноризец Храбър“, Пловдив.

Чл.25. 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.26. Архивирана компютърна информация се предоставя само на служители, които имат право на достъп, съгласно заеманата от тях длъжност и изпълнявана задача.

Чл.27. 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.28. Достъпът до помещенията с комуникационните шкафове се ограничава по възможност само до специализиран по поддръжката им персонал.

V . ПОЛЗВАНЕ НА КОМПЮТЪРНАТА МРЕЖА И ИНТЕРНЕТ

Чл.29. Разделяне логически локалната мрежа на три отделни мрежи - локална мрежа за

администрация, локална мрежа за учители и локална мрежа за ученици.

Чл.30. Ползването на компютърната мрежа и електронните платформи /Школо, Уча се, Електронни учебници и др./ от служителите става чрез получените потребителско име и парола.

Чл.31. 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.32. 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.33. Използването на комуникатори, осигуряващи достъп извън рамките на компютърната мрежа на СУ „Черноризец Храбър“, Пловдив и създаващи предпоставки за идентифициране на IP адрес на потребителя и за достъп назлонамерен софтуер и мобилен код до компютрите, свързани в компютърната мрежа на училището, да е ограничено и единствено и само за служебна цел.

Чл.34. Компютрите, свързани в мрежата на СУ „Черноризец Храбър“, Пловдив използват интернет само от доставчик, с когото СУ „Черноризец Храбър“, Пловдив има сключен договор за доставка на интернет.

Чл. 35. Забранява се свързването на компютри едновременно в мрежата на СУ „Черноризец Храбър“, Пловдив и в други мрежи, когато това позволява разкриване и достъп до IP адреси от мрежата на СУ „Черноризец Храбър“, Пловдив“ и/или е в противоречие с изискванията на Наредбата за минималните изисквания за мрежова и информационна сигурност.

Чл.36. Забранява се съхраняването на компютрите на СУ „Черноризец Храбър“, Пловдив на лични файлове е текст, изображения, видео и аудио.

Чл.37. 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 и архивни файлове;

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

VI. ЗАЩИТА ОТ КОМПЮТЪРНИ ВИРУСИ И ДРУГ ЗЛОВРЕДЕН СОФТУЕР

Чл.38. С цел антивирусна защита всички персонални компютри имат инсталиран антивирусен софтуер в реално време, който се обновява ежедневно.

VII. НЕПРЕКЪСНАТОСТ НА РАБОТАТА

Чл.39. 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. служителите включени в звено, отговарящо за мрежовата и информационната сигурност, започват процедура по поетапно спиране на устройствата за съхранение на данни.

(3) При срыв в локалната компютърна мрежа, всеки потребител следва да запише файловете, които е отворил на локалния си компютър, за да се избегне загуба на информация.

VIII. ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

§ 1. Служителите от педагогическия и непедagogическия персонал в СУ „Черноризец Храбър“, Пловдив са длъжни да познават и спазват разпоредбите на тези правила.

§ 2. Контролът по спазване на правилата се осъществява от ръководството на СУ „Черноризец Храбър“, Пловдив § 3. Настоящите вътрешни правила се разглеждат и оценяват периодично с оглед ефективността им, като СУ „Черноризец Храбър“, Пловдив може да приема и прилага допълнителни мерки

и процедури, които са целесъобразни и необходими с оглед защитата на информацията.

§ 3. Тези правила са разработени съгласно Наредбата за минималните изисквания за мрежова сигурност (приета с ПМС № 186 от 26.07.2019 г.) и влизат в сила от датата на извеждане на Заповед № РД-10-3178/14.09.2023г.. на Директора на СУ „Черноризец Храбър“, Пловдив