Утвърждавам!
Директор: .....
/л.арх. Добрина Андреева/
Заповед РД12-465/10.09.2024 г.

ВЪТРЕШНИ ПРАВИЛА ЗА РАБОТА С ИНФОРМАЦИОННИ СИСТЕМИ В СГСАГ „ХРИСТО БОТЕВ“ за учебна 2024 – 2025 г.

Вътрешните правила са разработени въз основа на НАРЕДБА за минималните изисквания за мрежова и информационна сигурност, приета с ПМС № 186 от 26.07.2019 г., обн., ДВ, бр. 59 от 26.07.2019 г., в сила от 26.07.2019 г.

ГЛАВА ПЪРВА
ОБЩИ ПОЛОЖЕНИЯ

Чл. l. (l) Правилата за използване на информационните системи информират педагогическите специалисти и непедагогическия персонал в образователната институция за правата и задълженията им по отношение на работата с информационните системи/технологии.

(2) Правилата определят изискванията за използване на информацията за вътрешна и външна комуникация, за предоставяне на услуги на родители и учители, за администриране, свързано с образователния процес, а също така са и средство за извършване на проучвания и обмяна на информация.

(3) Достъпът до данните в локалната мрежа и ползването на програмните продукти на
институцията от педагогическите специалисти и непедагогическия персонал е необходимо с оглед ефективното изпълнение на отговорностите и задълженията.

(4) Правата за достъп се делегират на две основни групи - потребителски и администраторски.

Администраторските права на достъп се определят със заповед на директора на институцията.

Чл.2. Информационните технологии включват локалните мрежи, интернет, електронната поща, всички програмни продукти, които образователната институция притежава и използва и всички създадени от педагогическите специалисти електронни уроци.

Чл. 3. Правилата дават указания за начина на употреба от педагогическите специалисти и непедагогическия персонал на информационните технологии, насърчава ползването им с цел увеличаване на продуктивността и ефективността им в работата.

Чл.4. Определеният заместник-директор, Системните администратори в образователната институция са отговорни за цялостната дейност на информационните технологии и за подпомагането работата на персонала с тях.

Чл. 5. Работниците и служителите в образователната институция са задължени да спазват правилата.

Чл. 6. Всички компютърни програмни продукти, уроци и информация, създадена и съхранена от работниците/служителите, са собственост на институцията.

Чл.7.Работниците/служителите в институцията нямат право да копират/ размножават/ разпространяват програмни продукти с цел инсталацията им на други технически устройства, независимо дали са собственост на СГСАГ „Христо Ботев“, с изключение на електронни учебници/познавателни книжки и създадени за онлайн обучение материали.

Чл.8.При прекратяване на трудовите отношения с институцията, работниците/служителите нямат право да копират или унищожават файлове с данни, които са създадени във връзка с тяхната работа.

ГЛАВА ВТОРА
КОНТРОЛ ВЪРХУ РАБОТАТА С ИНФОРМАЦИОННИТЕ ТЕХНОЛОГИИ

Чл. 9. (1) Екипът за управление на институцията има право да контролира ползването на програмните продукти, електронната поща, Интернет и базите данни, създадени от педагогическите специалисти и непедагогическия персонал в образователната институция.
(2) Екипът за управление на образователната институция има право да проверява изцяло служебните компютри, предоставени за целите на обучителния процес на персонала в институцията, както и техниката, която ползват учители и служители във връзка с изпълнение на служебните им задължения.

ГЛАВА ТРЕТА
КОНФИДЕНЦИАЛНОСТ

Чл. 10. (1) Конфиденциалността на информацията е лична отговорност на всеки, чийто профил осигурява достъп до нея, в съответствие с предоставените му права.
(2) Резултатите от извършения контрол върху работата с информационните технологии на образователната институция се считат за конфиденциални и не се разгласяват от екипа за управление.

ГЛАВА ЧЕТВЪРТА
ДОПУСТИМО ПОЛЗВАНЕ НА ИНФОРМАЦИОННИТЕ ТЕХНОЛОГИИ ЗА ЛИЧНИ ЦЕЛИ

Чл. 11. Учебните информационни системи са предназначени за ползване при изпълняване на служебните задължения на работниците/служителите.
Чл. 12. Системите могат да се ползват и за лични цели при следните условия:

1. Инцидентно, рядко и за кратко време.
2. Не по време на работа, а в извънработно време.
3. Ползването не пречи на работата на останалите работници/служители и при хипотезата конфликт на интереси.
4. Ползването не води до допълнителни разходи за институцията.

ГЛАВА ПЕТА
ЗАБРАНА ЗА ПОЛЗВАНЕ НА ИНФОРМАЦИОННИ ТЕХНОЛОГИИ

Чл. 13. Списъкът на забранените дейности във връзка с информационните технологии не е изчерпателен и към него може да се добавят допълнителни забрани със заповед на директора.
Чл. 14. Забранява се ползването на компютърните и информационни системи на образователната институция в следните случаи:
1. Заобикаляне на системите за сигурност, с цел разрушаване или намаляване сигурността на учебната локална мрежа или бази данни.
2. Ползване на компютърните ресурси за извършване на престъпление.
3. Използване на ресурсите за подпомагане дейността на дадена компания, нейните продукти, услуги или бизнес практика.

4. Електронната поща на институцията не може да се ползва за комерсиални лични цели, религиозни цели или да се подпомага бизнес, който не е свързан с дейността на образователната институция.
5. Ползването на компютърните системи за политическа дейност, която пряко или косвено би подпомогнала кампанията за избиране на даден кандидат.
6. Подправяне на електронна поща с цел скриване на самоличността на подателя или фалшифициране на тази самоличност. Всички електронни писма, изпратени от персонала трябва да са лично подписани или подписани с техен електронен подпис.
7. Сваляне от Интернет на аудио и видео файлове.
8. Сваляне и инсталиране на компютърни програми от Интернет без разрешение на системните администратори.
9. Копиране на лицензираните компютърни програми на институцията с цел лична употреба.

ГЛАВА ШЕСТА
РАЗКРИВАНЕ НА ИНФОРМАЦИЯ

Чл. 15. (1) Неоторизираното разкриване на служебна информация може да доведе до негативни последици за образователната институция и накърняване на нейния авторитет и репутация.
(2) Работник/служител, който е копирал и използвал информация от локалната мрежа на институцията за лична изгода или за да причини вреда на институцията, носи съответната дисциплинарна и имуществена отговорност по Кодекса на труда.

ГЛАВА СЕДМА
АНТИВИРУСНА ЗАЩИТА

Чл. 16. (1) Компютърните вируси са голяма заплаха за всички потребители на IT услуги и работниците и служителите трябва да имат необходимите (общи) познания как вирусите се разпространяват, каква вреда могат да нанесат и как да се предпазват от тях. Компютърният вирус е компютърна програма, която се задейства от и на даден компютър, като се разпространява към другите дискове и програми, които са в контакт със заразения компютър. Вирусът може да причини блокиране на компютъра, да промени бази данни, да направи някои данни невъзможни за ползване и даже да форматира диск и така да се загуби цялата записана информация.
Чл. 17. (1) Системните администратори на образователната институция носят пълната отговорност за избирането и инсталирането на антивирусна програма, както и за нейната актуализация на всеки индивидуален компютър. Служителите също трябва да следят дали тяхната антивирусна програма се осъвременява периодично с най-новата версия и антивирусни дефиниции.
(2) Работниците/служителите трябва да приемат всяко съобщение за вирус изключително сериозно и да следват вътрешните процедури за реакция в такъв случай.
(3) Преднамереното разпространяване на данни, за които работникът/служителят знае, че са заразени с вирус е нарушение на служебните задължения, което се санкционира по дисциплинарен ред.
(4) В случай на вирусна атака работникът/служителят трябва незабавно да информира администратора, без да предприема никакви самостоятелни действия.
(5) Входящата електронна поща трябва да се третира с особено внимание поради потенциалната възможност да се зарази с вируси. Отварянето на приложения да се прави само след предварителното им сканиране с антивирусна програма.

(6) Ползването на външни носители (дискове, външна памет и др.) на информация е допустимо само след предварителното им сканиране с антивирусна програма.

ГЛАВА ОСМА
АРХИВИРАНЕ НА ИНФОРМАЦИЯТА И ВЪЗСТАНОВЯВАНЕ

Чл. 18. (1) Сривовете в компютърното оборудване, вирусите и случайното изтриване на файлове могат да причинят загуба на данни, поради което е необходимо информацията във всяка компютърна система да бъде архивирана.
(2) Целта на архивирането е да се възстанови работата възможно най-бързо в случай на прекъсване по технически причини. По този начин се минимизират възможните проблеми и загуби.
(3) Работниците/служителите в институцията, съгласувайки с администратора, трябва да имат адекватна система за архивиране на данните от своята работа на технически носители (дискове, USB и др.).
(4) Задължително архив (архивиране на файлове) се прави веднъж месечно. При необходимост директорът издава заповед за периода/честотата на архивиране на данните.
(5) Направените архивни копия се съхраняват по възможност в специално предназначен за целта заключен шкаф.
(6) Архивните копия се обозначават със следните данни:
1. Име на информацията;
2. Дата на създаване;
3. Срок на съхранение;
4. Име на служителя извършил архивирането.

(7) Архивните копия се проверяват периодично за пълнота на архивираната информация и възможност за възпроизвеждането ѝ.
(8) При срив в информационните системи, специалистът по информационни технологии предприема нужните действия за възстановяване на нормалното функциониране на системите. При загуба или повреждане на информация, я възстановява, като използва последното актуално архивно копие.

ГЛАВА ДЕВЕТА
ДОСТЪП И ПАРОЛИ

Чл. 19. (1) Работниците/служителите получават достъп до локалната мрежа и до всички програми, необходими за изпълнение на служебните им задължения.
(2) Достъпът до дадена програма се дава на конкретен работник/служител и не може да се прехвърля на друг.
(3) Работниците/служителите трябва да пазят своите лични пароли в тайна.
(4) Когато даден продукт или служебен профил изисква парола, следва да се спазват следните правила:
1. Служителят трябва да промени първоначалната парола, обикновено генерирана от програмния продукт като я замени със своя.
2. Паролите следва да съдържат малки и големи букви, цифри и специални символи, дължината им трябва да е не по-малка от 8 символа за потребителските и 12 символа за администраторските профили, но да се помнят лесно , за да не се налага записване на хартиен носител и да се оставят на работното място;
3. Желателно е паролите да се сменят на определени времеви интервали (например 3, 6 месеца), като при периодична промяна, не е желателно да се ползват вече използвани пароли.

ГЛАВА ДЕСЕТА
ИНТЕРНЕТ

Чл. 20. (1) Екипът за управление насърчава ползването на Интернет от работниците/ служителите за обмяна на информация, извършване на проучвания и събиране на данни във връзка с дейността им.
(2) Заместник-директорите и други оторизирани длъжностни лица отговарят за уместната употреба на Интернет от персонала.

ГЛАВА ЕДИНАДЕСЕТА
ЕЛЕКТРОННА ПОЩА

Чл. 21. (1) Електронната поща на институцията не може да се ползва за комерсиални и религиозни цели или да се подпомага бизнес, който не е свързан с дейността на институцията.
(2) Ползването на електронната поща за политическа дейност, която пряко или косвено би подпомогнала кампанията за избиране на даден кандидат също не се позволява.
(3) Подправяне на електронна поща с цел скриване на самоличността на подателя или фалшифициране на тази самоличност се забранява. Всички електронни писма, изпращани от работниците/служителите трябва да са лично подписани.
(4) Всички електронни писма и важни съобщения, които имат отношение към дейността на образователната институция, трябва да се принтират и представят за завеждане с входящ номер в Регистъра за входяща кореспонденция от определеното длъжностно лице, като екземпляр се съхранява в съответните класьор и в електронната поща.

ГЛАВА ДВАНАДЕСЕТА
ЛИЦЕ ЗА КОНТАКТ

Чл. 22. Всички технически въпроси във връзка с работата на компютърните системи се насочват към администраторите на образователната институция или към друго лице, определено от директора.

ГЛАВА ТРИНАДЕСЕТА
РАБОТА СЪС СПОДЕЛЕНИ ПАПКИ, СЪРВЪР И ОБЛАЧНО ПРОСТРАНСТВО

Чл. 23. Работниците и служителите, които имат достъп и право да работят с данните от сървъра на СГСАГ „Христо Ботев“ са администратори, екип за управление, главен счетоводител, касиер-счетоводител, финансов контрольор, архивист, служител-човешки ресурси, технически сътрудник ЕПП, секретар, завеждащ административна служба, домакин.
Чл. 24. Работниците/служителите в институцията, работещи със сървъра и споделените папки в него нямат право да копират/размножават/разпространяват информацията оттам на други устройства, които не са собственост на СГСАГ „Христо Ботев“.
Чл. 25. При работа със споделени папки в облачното пространство, педагогическите специалисти се задължават да НЕ разпространяват линк към споделената папка на трети лица. Линк за споделяне има право да изпрати само създателят на папката към заинтересованите лица.
Чл.26. При прекратяване на трудовите отношения с институцията, работниците/служителите нямат право да копират или унищожават файлове с данни, които

са създадени във връзка с тяхната работа от сървъра и споделените папки там. При прекратяване на трудовите правоотношения, достъпът на служителя до информационните системи на СГСАГ „Христо Ботев“ се заличава в същия ден.
(2) Работата с данните от сървъра и споделените папки в него се считат за конфиденциални и не се разгласяват от екипа за управление и служителите на СГСАГ „Христо Ботев“.

ДОПЪЛНИТЕЛНИ РАЗПОРЕДБИ

1. При извършване на самооценката на вътрешните контроли следва да се направи анализ и оценка на риска на критичните информационни системи в образователната институция.
2. Целта е да се идентифицират най-важните компоненти (оборудване, програми, бази данни и др.), заплахата за тяхната повреда или загуба, последиците от това за дейността на институцията, за да се предотвратят потенциалните проблеми, както и да се въведат допълнителни контроли, които са необходими за подобряване на системата.
3. Оценката на риска обхваща извършеното, както и моментното състояние, мерките за подобряване на слабите места във вътрешните контроли, необходимите ресурси и остатъчния риск за институцията, които контролите няма как да елиминират.
4. При създаването на програмен продукт специално за нуждите на институцията е необходимо още при задаването на неговите параметри на доставчика да се заложат основните контролни функции, които този продукт трябва да има.

ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

1. Настоящите правила са обект на изменения и допълнения, когато те служат за подобряване на ефективността на изпълнението им и/или третират проблеми, останали незасегнати в тях.
2. Настоящите правила са приети с Решение с Протокол № 15/10.09. 2024 от заседание на Педагогическия съвет и са утвърдени със Заповед № РД12-465/10.09.2024 г. на директора.
3. Правилата за работа с информационните системи/технологии влизат в сила от датата на утвърждаването им със Заповед №. РД-465/10.09.2024 г. на директора.