СОФИЙСКА ГИМНАЗИЯ ПО СТРОИТЕЛСТВО, АРХИТЕКТУРА И ГЕОДЕЗИЯ "ХРИСТО БОТЕВ"
1164, гр. София, бул. „Евлоги и Христо Георгиеви“ №34, тел. 0879 908 715, *e-mail: sgcag@sgcag.info; web: www.sgcag.info*

Утвърждавам!
Директор: .....
/ландш. арх. Добрина Андреева/
Заповед № РД12-465/10.09.2024 г.

ВЪТРЕШНИ ПРАВИЛА ЗА МРЕЖОВА И ИНФОРМАЦИОННА СИГУРНОСТ

в СГСАГ „Христо Ботев“ гр. София

Постановление № 186 от 26 юли 2019 г. обн., ДВ, бр. 59 от 26.07.2019 г., в сила от 26.07.2019 г. за приемане на Наредба за минималните изисквания за мрежова и информационна сигурност:

Септември, 2024 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 и информационна сигурност (приета с ПМС № 186 от 26.07.2019г.,) и имат за цел осигуряването на контрол и управление на работата на информационните системи в СГСАГ „Христо Ботев“, гр. София. 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 СГСАГ „Христо Ботев“, гр. София 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 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.).

РАЗДЕЛ II
КОНТРОЛ НА ДОСТЪПА И ПРАВИЛА ЗА РАБОТА С НОСИТЕЛИ

Чл. 4 Защитата и контролът на информационните и компютърните системи на СГСАГ „Христо Ботев“ се извършва при спазване на следните основни принципи и дейности:

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 софтуер и преконфигурирането от потребителите на вече инсталиран такъв, както и хардуер и/или самостоятелни опити за поправка или подобрения на горепосочените. При съмнение за възникнал проблем, незабавно се уведомява Системен администратор.
6. 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.
7. 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 представителите на звеното, отговарящо за мрежовата и информационната сигурност.
8. Не се допуска достъпа на външни лица до компютърната техника в канцеларииите в сградата на СГСАГ „Христо Ботев“, с изключение на техници и софтуерни специалисти от оторизирани фирми, и то само придружени от представителите на звеното, отговарящо за мрежовата и информационната сигурност.

9. **При никакви обстоятелства,** служителите не могат да предоставят паролите си за достъп до системата на други служители, външни лица, роднини и приятели !!!
10. Всички пароли за достъп на системно ниво се променят периодично!
11. Документите на електронен носител и базите данни се съхраняват на специализирани сървъри, компютърни системи и/или външни носители на информация. Архивирането се извършва периодично на технически носител, от обработващия администратор на съответните данни (лични данни, бази данни, файлове и документи на използваните в училището софтуерни продукти), с оглед запазване на информацията в актуален вид и/или възможност за възстановяване.
12. Архивните копия се съхраняват на различно местоположение от мястото на компютърното оборудване, обработващо данните. Достъп до архивите имат само обработващият администратор на лични данни и оторизираните длъжностни лица.
13. Достъп до архивираните данни, имат единствено оторизираните лица съобразно възложените им от закона правомощия.
14. Сървърните системи се архивират периодично от системните и мрежови администратори чрез основни ИТ процедури, които се изпълняват**:**

    14.1 Създаване на системен имидж – сектор по сектор на сървърните операционни системи.
    14.2 Архивиране на базите данни, инсталирани или съхранявани на сървърите.
    14.3 Периодичността по създаване на архивите се определя от директора на училището.
15. Служителите в счетоводството и касата правят ежедневни (в края на работния ден) архивни копия на данните, с които работят.

Чл. 5 Всеки служител има точно определени права на достъп и използва уникален потребителски профил за вход в съответна система–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. Нивата на достъп са зададени в **Приложение 1**.

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 СГСАГ „Христо Ботев“, 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 (поставяне на изходящ номер и дата);
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 СГСАГ „Христо Ботев“, те се поставят в подходяща опаковка и в запечатан плик.

Чл. 13 На служителите е строго забранено да използват мобилни компютърни устройства на места, където може да възникне риск устройството и информацията в него. Потребителите на мобилни компютърни устройства 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 по сигурен и безопасен начин 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 такава 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 СГСАГ „Христо Ботев “, 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 присъствието 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, освен тези, които са в непрекъснат режим на работа.

Чл.21 При загуба на данни или информация от служебния компютър, служителят незабавно уведомява Административното звено (Системен/Мрежови администратор), отговарящо за мрежовата и информационната сигурност, като при нужда му оказва съответна техническа помощ.

Чл.22 Забраняват се опити за достъп до компютърна информация и бази данни, на служители, чиято заемана длъжност не предполага предоставяне на права за достъп, както и извършването на каквито и да е действия, които улесняват трети лица за **нерегламентиран** 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 Административното звено, отговарящо за мрежовата и информационната сигурност.

Чл. 24 Забранява се използването на преносими носители с възможност за презаписване на данни за прехвърляне на файлове между компютри, свързани в компютърната мрежа на СГСАГ „Христо Ботев“, преди задължително тестване за зловреден софтуер с антивирусна програма.

Чл.25 Служителите имат право да обменят компютърна информация посредством вътрешна
компютърна мрежа и/или облачна услуга (съпътстваща служебните пощи – OneDrive) 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.

РАЗДЕЛ IV
ПОЛЗВАНЕ НА КОМПЮТЪРНАТА МРЕЖА И ИНТЕРНЕТ

Чл. 29 С цел допълнителна мрежова сигурност, локалната мрежа се разделя логически на три отделни подмрежи: 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.

ал. (1) Всички служители и педагогически специалисти са задължени да използват за служебни цели единствено своята електронна поща към домейна **sgcag.info.**

ал. (2) При постъпване на работа служебна поща се създава и предоставя от системните администратори в СГСАГ „Христо Ботев“.

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 (Teams, skype, facebook, messenger, viber, zoom и др. подобни), осигуряващи достъп извън рамките на компютърната мрежа на СГСАГ „Христо Ботев“ 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 единствено и само за служебна цел.

Чл**.34** Компютрите, свързани в мрежата на СГСАГ „Христо Ботев“, използват интернет само от доставчик, с когото СГСАГ „Христо Ботев“ има сключен договор за доставка на интернет.

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

Чл. 36 Забранява се съхраняването на служебните компютри в СГСАГ „Христо Ботев“ на лични файлове с текст, изображения, видео и аудио.

Чл. 37 Без контрол от страна на системен администратор, изрично се забранява отварянето на:

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 подател, тема, знаци и текст, прикачени файлове и др.

РАЗДЕЛ V
ЗАЩИТА ОТ КОМПЮТЪРНИ ВИРУСИ И ДРУГ ЗЛОВРЕДЕН СОФТУЕР

Чл. 38 С цел антивирусна защита се прилагат следните мерки:

ал. (1) Всички служебни и лични персонални компютри и лаптопи трябва да имат инсталиран антивирусен софтуер в реално време, който се обновява ежедневно. При липса на антивирусен софтуер на личните устройства следва да се инсталира подходящ такъв.

ал. (2) Потребителите на лаптопи, предоставени за ползване, обновяват и сканират за зловреден софтуер редовно с предоставените им за ползване антивирусни програми. Те се задължават да не спират или деинсталират антивирусния софтуер.

РАЗДЕЛ VI
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 минути, служителите включени в звено, отговарящо за мрежовата и информационната сигурност, започват 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 VII
ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

1. Ръководителите и служителите в СГСАГ „Христо Ботев“, са длъжни да познават и спазват разпоредбите на тези правила.

2. Контролът по спазване на правилата се осъществява от ръководството на СГСАГ „Христо Ботев“.

3. Настоящите вътрешни правила се разглеждат и оценяват периодично с оглед ефективността им, като СГСАГ „Христо Ботев“, може да приема и прилага допълнителни мерки и процедури, които са целесъобразни и необходими с оглед защита на информацията.

4. Тези правила са разработени съгласно Наредбата за минималните изисквания за мрежова и информационна сигурност (приета с ПМС № 186 от 26.07.2019г. обн., ДВ, бр. 59 от 26.07.2019 г., в сила от 26.07.2019 г.) и влизат в сила от датата на извеждане на Заповед № № РД12-465./10.09.2024 г. на Директора на СГСАГ „Христо Ботев“.

Приложение 1

Нива на достъп, обработка на информацията и конфиденциалност:

№	Електронни платформи	Право на достъп	Ниво на достъп
1	Електронна поща на училището за: - Обща кореспонденция;	• Директор • Зам. директор • Счетоводител • Технически секретар • Завеждащ адм. служба • Служител Човешки ресурси • Системни администратори	Всички възможности
	Електронна поща на училището за: - Отсъствия на ученици; - Стипендии; - Изпити	• Директор • Зам. Директор • Счетоводител • Технически секретар • Завеждащ адм. Служба • Финансов контрольор	
	Електронна поща на училището за: - Счетоводство;	• Директор • Зам. директор • Счетоводител • Финансов контрольор	
	Служебна персонална електронна поща	• Всички служители персонално	Всички възможности свързани с персоналната електронна поща
2	Сайт на училището	• Администратор уеб сайт • Системни администратори	Всички права за достъп, разрешени от домейна
3	Електронен дневник „Школо”(учители)	• Всички педагогически специалисти	Нивата на достъп до настройки, възможности за достъп до информация за ученици, учители и родители се определят от директора на училището
4	Електронен дневник „Школо” (администрация)	• Директор, зам. директори и системни администратори	Директорът дава ниво на достъп до информацията, достъпна в „Школо”
5	НЕИСПУО (Списък образец - 1)	• Директор • Зам. директор • Техн. Секретар • Служител ЧР	Пълен достъп и право на обработка на информацията
5.1	НЕИСПУО (ЛОД на учениците)	• Директор • Зам. директор • Кл. ръководител • Техн. секретар	Пълен достъп и право на обработка на информацията

№	Електронни платформи	Право на достъп	Ниво на достъп
6	Система за сигурно електронно връчване	• Директор • Зам. директор	Всички права за достъп, разрешени от системата
7	**Информационна система за администриране на финансовите процеси в системата на предучилищното и училищното образование**	• Директор • Счетоводител	Всички права за достъп, разрешени от системата.
8	Офис 365 и Тиймс	• Директор • Зам. директори • Системни администратори	Имат пълен достъп до информацията и право да я обработват
9	Регистър на дипломи и свидетелства	• Директор • Системни администратори	Пълен достъп и право на обработка на информацията
10	Информационни системи за провеждане на ДЗИ, НВО и олимпиади	• Директор • Зам. директори • Системни администратори	Пълен достъп и право на обработка на информацията
11	Други платформи на МОН по национални и оперативни програми	• Директор • Зам. директор • Счетоводител	Пълен достъп и право на обработка на информацията