



Средно училище „Иван Вазов“ гр. Плевен

5800 Плевен, ул. „Иван Вазов“ № 46
www.suivanvazov.com

Телефони: 064/822 280; 064/823 979
email: info-1500134@edu.mon.bg

УТВЪРЖДАВАМ /П/

ГАНКА НИНОВА ВАСИЛЕВА

Директор на СУ „Иван Вазов“ – град Плевен

ВЪТРЕШНИ ПРАВИЛА

ЗА МРЕЖОВА И ИНФОРМАЦИОННА СИГУРНОСТ

В СРЕДНО УЧИЛИЩЕ „ИВАН ВАЗОВ“ – ГРАД ПЛЕВЕН

СЕПТЕМВРИ 2024 ГОДИНА

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 Плевен. 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 Плевен 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.

Чл. 4. Системата за сигурност на информацията в СУ „Иван Вазов“ – град Плевен има за цел да защитава служителите, партньорите и учениците на СУ „Иван Вазов“ – Плевен 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 е-оборудване за изпълнение на служебните им задължения.

РАЗДЕЛ II. КЛАСИФИКАЦИЯ НА ИНФОРМАЦИЯТА

Чл. 5. (1) Всяка информация, която стане достъпна за служителите при изпълнение на служебните им задължения, ако са свързани със СУ „Иван Вазов“ – град Плевен и негова дейност или партньори за сътрудничество, се счита за собствена и поверителна информация на СУ „Иван Вазов“ – град Плевен, 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 „Иван Вазов“ – град Плевен извършва класификация на информацията. Информацията подлежи на защита, независимо от това дали такава е на разположение на служителя под формата на печатни материали, устройства за съхранение на данни, аудио/видео материали или по друг начин.

(3). Обща класификация на информацията, приложима в рамките на СУ „Иван Вазов“ – Плевен:

категория	Описание	Примери (неизчерпателни)
Публична информация	Информация, която може да бъде обработвана и разпространявана в рамките на СУ „Иван Вазов“ – Плевен или извън него без никакво отрицателно въздействие върху СУ „Иван Вазов“ – Плевен, някой от нейните партньори.	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 закони или подзаконови актове, тези Правила или всяка друга регулация, приета от СУ „Иван Вазов“ – Плевен може да навреди на интересите на организацията и/или неговите служители и партньори.	а) Документи, разработени и/или изготвени от който и да е служител на СУ „Иван Вазов“ – Плевен б) Всички директории (информация за връзка и т.н.), установени и/или използвани за нуждите на СУ „Иван Вазов“ – Плевен в) Всякакви вътрешни работни бележки, изявления, становища, разработени за нуждите на СУ „Иван Вазов“ – Плевен или с цел ефективност на дейността на организацията;
Поверителна информация	Всяка информация от такова значение за СУ „Иван Вазов“ – Плевен, неотривираното разкриване на която би могло да окаже неблагоприятно въздействие върху дейността, операциите, репутацията, цялостното състояние на СУ „Иван Вазов“ – Плевен, като последица от такова разкриване, която би причинила сериозни вреди/щети на служителите.	а) Политики, процедури, вътрешни правила, управленски решения; б) Информация, за която е указано на служителя, че е търговска тайна на СУ „Иван Вазов“ – Плевен 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 „Иван Вазов“ – Плевен е сключило в хода на дейността си.
--	--	---

РАЗДЕЛ III. КОНТРОЛ НА ДОСТЪПА И ПРАВИЛА ЗА РАБОТА С НОСИТЕЛИ

Чл. 6. 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 ръководителя на направление „ИКТ“.
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 и то само придружени от ръководителя на направление „ИКТ“.
9. Не се допуска достъпа на външни лица до компютърната техника в канцелариите в сградата на СУ „Иван Вазов“ – град Плевен. 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
10. Служителите не могат да отстъпват паролите си за достъп до системата на други служители, външни лица, роднини и приятели.
11. Паролите за достъп на всички служители, описани по видове приложения се съхраняват от ръководителя на направление „ИКТ“. Всички пароли за достъп на системно ниво се променят периодично.

Чл. 7. 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. 8. 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

ръководителя на направление „ИКТ“, който контролира компютрите, използвани за достъп до мрежи и мрежови услуги.

Чл. 9. 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. 10. Лицата, които обработват лични данни, използват уникални пароли с достатъчно сложност, които не се записват или съхраняват онлайн.

Чл. 11. Всички пароли за достъп на системно ниво се променят периодично.

Чл. 12. Всички носители на лични данни се съхраняват в безопасна и сигурна среда с ограничен и контролиран достъп.

Чл. 13. На служителите на СУ „Иван Вазов“ – град Плевен, които използват електронни бази данни и техни производни се забранява:

- да ги изнасят под каквато и да е форма извън служебните помещения преди извеждане от деловодството (извършване на услуга);
- да ги използват извън рамките на служебните си задължения;
- да ги предоставят на външни лица без да е заявена услуга.

Чл. 14. За нарушение целостта на данните се считат следните действия:

- унищожаване на бази данни или части от тях;
- повреждане на бази данни или части от тях;
- вписване на невярна информация в бази данни или части от тях.

Чл. 15. При изнасяне на носители извън физическите граници на СУ „Иван Вазов“ – град Плевен, те се поставят в подходяща опаковка и в запечатан плик.

Чл. 16. 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. 17. 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. 18. 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 IV. РАБОТНО МЯСТО

Чл. 19. Работното място се състои от работно помещение, работна маса и стол, компютърна и периферна техника, комуникационни средства.

Чл. 20. Всеки служител отговаря за целостта на компютърната и периферна техника, програмните продукти и данни, инсталирани на компютъра на неговото работно място.

Чл. 21. 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. 22. Забранява се на външни лица работата с персоналните компютри на СУ „Иван Вазов“ – град Плевен, 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 ръководителя на направление „ИКТ“;
- провеждане на обучения на външни педагогически специалисти по програми и проекти на МОН или РУО, но само след разрешението на Директора на училището и задължително в присъствието на ръководителя на направление „ИКТ“.

Чл. 23. След края на работния ден всеки служител задължително изключва компютъра, на който работи.

Чл. 24. При загуба на данни или информация от служебния компютър, служителят незабавно уведомява ръководителя на направление „ИКТ“, който му оказва съответна техническа помощ.

Чл. 25. 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. 26. 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 с ръководителя на направление „ИКТ“.

Чл. 27. Забранява се използването на преносими магнитни, оптични и други носители с възможност за записване на данни за прехвърляне на файлове между компютри, свързани в компютърната мрежа на СУ „Иван Вазов“ – град Плевен.

Чл. 28. 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. 29. Архивирана компютърна информация се предоставя само на служители, които имат право на достъп, съгласно заеманата от тях длъжност и изпълнявана задача.

Чл. 30. 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. 31. Достъпът до помещенията с комуникационните шкафове се ограничава по възможност само до специализиран по поддръжката им персонал.

РАЗДЕЛ V. ПОЛЗВАНЕ НА КОМПЮТЪРНАТА МРЕЖА И ИНТЕРНЕТ

Чл. 32. Компютрите, свързани в мрежата на СУ „Иван Вазов“ – град Плевен, използват интернет само от доставчик, с когото училището има сключен договор за доставка на интернет.

Чл. 33. Фирмата, изградила компютърната 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 следните отделни мрежи: локална мрежа за администрация; локална мрежа за компютърните кабинети (4 кабинета); локална мрежа за кабинетите в СТЕМ центъра; локална мрежа за интерактивните дисплеи, монтирани в класните стаи; безжична локална мрежа **Students** за ученици и гости и безжична локална мрежа **Teachers** за учители и служители.

Чл. 34. Ползването на компютърната мрежа и електронните платформи /Google Workspace, Школо, Уча се, Електронни учебници и др./ от служителите става чрез получените потребителско име и парола.

Чл. 35. 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. 36. 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 електронните платформи при използване на предоставените им потребителски имена и пароли.

Чл. 37. Забранява се свързването на компютри едновременно в мрежата на СУ „Иван Вазов“ – град Плевен и в други мрежи, когато това позволява разкриване и достъп до IP адреси от мрежата на училището и/или е в противоречие с изискванията на Наредбата за минималните изисквания за мрежова и информационна сигурност.

Чл. 38. Използването на комуникатори (skype, facebook, messenger, viber, zoom и др. подобни), осигуряващи достъп извън рамките на компютърната мрежа на СУ „Иван Вазов“ – град Плевен 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. 39. Забранява се съхраняването на компютрите на СУ „Иван Вазов“ – град Плевен на лични файлове с текст, изображения, видео и аудио.

Чл. 40. 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. 41. Не се толерира влизането в Интернет – сайтове с неизвестно съдържание.

РАЗДЕЛ VI. ЗАЩИТА ОТ КОМПЮТЪРНИ ВИРУСИ И ДРУГ ЗЛОВРЕДЕН СОФТУЕР

Чл. 42. С цел антивирусна защита се прилагат следните мерки:

- Всички персонални компютри имат инсталиран антивирусен софтуер в реално време,

който се обновява.

- Ръководителят на направление „ИКТ“ извършва следните дейности:
 - активира защитата на съответните ресурси – файлова система, електронна поща и извършва първоначално пълно сканиране на системата;
 - настройва антивирусния софтуер за периодични сканирания през определен период;
 - активира защитата на различните програмни продукти за предупреждение при наличие на макроси и настройва защитната стена на система;
 - проверява за правилно настроен софтуер за автоматично обновяване на операционната система и инсталирания софтуер.
- При поява на съобщение от антивирусната програма за вирус в локалната мрежа, всеки служител от съответното работно място задължително информира ръководителя на направление „ИКТ“.

РАЗДЕЛ VII. НЕПРЕКЪСНАТОСТ НА РАБОТАТА

Чл. 43. 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., ръководителят на направление „ИКТ“ започва 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.

РАЗДЕЛ VIII. СЪЗДАВАНЕ НА РЕЗЕРВНИ КОПИЯ

Чл. 44. Всеки служител, който работи с класифицирана информация, осигурява автоматично създаване на архивни копия всекидневно.

Чл. 45. 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 използвания софтуер се архивират всеки ден в края на работното време.

РАЗДЕЛ IX. ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

§ 1. Ръководителите и служителите в СУ „Иван Вазов“ – град Плевен 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 Плевен

§ 3. Настоящите вътрешни правила се разглеждат и оценяват периодично с оглед ефективността им, като СУ „Иван Вазов“ – град Плевен 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. , изм.ДВ.бр.47 от 24 юни 2022г.) и влизат в сила от датата на заповедта за тяхното утвърждаване – № РД 13 – 3331 / 13. 09. 2024 година на директора на училището.