УТВЪРЖДАВАМ:

РУЖКА ГЕНОВА
директор на СУ „Васил Левски“ - Пловдив

Заповед № РД-06-782/22.12.2021 г.

X
РУЖКА ГЕНОВА
директор на СУ "Васил Левски" - Пловдив

ВЪТРЕШНИ ПРАВИЛА ЗА МРЕЖОВА И ИНФОРМАЦИОННА СИГУРНОСТ НА СПОРТНО УЧИЛИЩЕ „ВАСИЛ ЛЕВСКИ“ - ПЛОВДИВ

СЪДЪРЖАНИЕ	Страница
1. РАЗДЕЛ I. ОБЩИ ПОЛОЖЕНИЯ	4
2. РАЗДЕЛ II. КОНТРОЛ НА ДОСТЪПА И ПРАВИЛА ЗА РАБОТА С НОСИТЕЛИ И ПРОГРАМНИ ПРОДУКТИ	4
3. РАЗДЕЛ III. РАБОТНО МЯСТО	6
4. РАЗДЕЛ IV. ПОЛЗВАНЕ НА КОМПЮТЪРНАТА МРЕЖА И ИНТЕРНЕТ	7
5. РАЗДЕЛ V. ЗАЩИТА ОТ КОМПЮТЪРНИ ВИРУСИ И ДРУГ ЗЛОВРЕДЕН СОФТУЕР	8
6. РАЗДЕЛ VI. НЕПРЕКЪСНАТОСТ НА РАБОТАТА	9
7. РАЗДЕЛ VII СЪЗДАВАНЕ НА РЕЗЕРВНИ КОПИЯ	9
8. РАЗДЕЛ VIII. ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ	9

ИСТОРИЯ НА ДОКУМЕНТА

№ по ред	Наименование на документа[1]	Дата на утвърждаване от директора на училището	Свързани документи
1	Вътрешни правила за мрежова и информационна сигурност в СУ „Васил Левски“ – Пловдив (Н)	РД-06-782/22.12.2021 г.	Приложение към: „Вътрешни правила за системата за финансово управление и контрол в СУ „Васил Левски“ - Пловдив – реф. елемент – реф. елемент IV „Информация и комуникация“.

[1] нов (Н); актуализиран (А)

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 Спортно училище „Васил Левски“ – 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 СУ „Васил Левски“ – 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 И ПРОГРАМНИ ПРОДУКТИ

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 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 канцеларите в сградата на СУ „Васил Левски“ – Пловдив.

10. Служителите не могат да отстъпват паролите си за достъп до системата на други служители, външни лица, роднини и приятели.

11. 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 достатъчно 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 „Васил Левски“ – Пловдив, 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. 11. 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. 12. При изнасяне на носители извън физическите граници на СУ „Васил Левски“ –
Пловдив, те се поставят в подходяща опаковка и в запечатан плик.

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. 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 СУ „Васил Левски“ – 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 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. 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 ръководителя на направление „ИКТ“, който 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 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 ръководителя на направление „ИКТ“.

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 „Васил Левски“ – 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.

РАЗДЕЛ IV. ПОЛЗВАНЕ НА КОМПЮТЪРНАТА МРЕЖА И ИНТЕРНЕТ

Чл. 29. Компютрите, свързани в мрежата на СУ „Васил Левски“ – Пловдив, използват интернет само от доставчик, с когото училището има сключен договор за доставка на интернет.

Чл. 30. 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.

Чл. 31. Ползването на компютърната мрежа и електронните платформи /Теамс, Школо, Уча се, Електронни учебници и др./ от служителите става чрез получените потребителско име и парола.

Чл. 32. 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. 33. 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. 34. Забранява се свързването на компютри едновременно в мрежата на СУ „Васил Левски“– Пловдив 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 минималнитеизисквания за мрежова и информационна сигурност.

Чл. 35. Използването на комуникатори (skype, facebook, messenger, viber, zoom и др. подобни), осигуряващи достъп извън рамките на компютърната мрежа на СУ „Васил Левски“ – 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. 36. Забранява се съхраняването на компютрите на СУ „Васил Левски“ – Пловдив налични файлове с текст, изображения, видео и аудио.

Чл. 37. 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. 38. Не се толерира влизането в Интернет – сайтове с неизвестно съдържание.

РАЗДЕЛ V. ЗАЩИТА ОТ КОМПЮТЪРНИ ВИРУСИ И ДРУГ ЗЛОВРЕДЕН СОФТУЕР

Чл. 39. С цел антивирусна защита се прилагат следните мерки:

- Всички персонални компютри (лаптопи) 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 VI. НЕПРЕКЪСНАТОСТ НА РАБОТАТА

Чл. 40. 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., ръководителя на направление „ИКТ“ започва 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 СЪЗДАВАНЕ НА РЕЗЕРВНИ КОПИЯ

Чл. 41. Всеки служител, който работи с класифицирана информация, осигурява създаване на архивни копия.

Чл. 42. 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.

РАЗДЕЛ VIII. ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

1. Ръководителите и служителите в СУ „Васил Левски“ – Пловдив са длъжни да познават и спазват разпоредбите на тези правила.

2. Контролът по спазване на правилата се осъществява от ръководството на СУ „Васил Левски“ – Пловдив.

3. Настоящите вътрешни правила се разглеждат и оценяват периодично с оглед ефективността им, като СУ „Васил Левски“ – 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 26.07.2019 г.) .

5. Настоящите правила са част от системата за финансово управление и контрол в училището - реф. елемент IV „Информация и комуникация“ и влизат в сила от датата на на утвърждаването им със Заповед №782/22.12.2021 г. на Директора на СУ „Васил Левски“ – Пловдив.