СРЕДНО УЧИЛИЩЕ „КОНСТАНТИН КОНСТАНТИНОВ“ – СЛИВЕН

УТВЪРДИЛ:

Весела Паскалева

Директор на СУ „К. Константинов“ - Сливен

ВЪТРЕШНИ ПРАВИЛА ЗА МРЕЖОВА И ИНФОРМАЦИОННА СИГУРНОСТ В СУ "КОНСТАНТИН КОНСТАНТИНОВ", ГР. СЛИВЕН

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 "Константин Константинов", гр. Сливен.

Понятието информационна система се определя като съвкупност от компютърна и периферна техника, програмни продукти, данни и обслужващ персонал, свързани в локална мрежа или по друг начин.

Чл. 2. Потребителите на информационни системи в СУ "Константин Константинов", гр. Сливен 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 при спазване на Наредбата за минималните изисквания за мрежова сигурност.

РАЗДЕЛ II. 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 нов и реконфигурирането на вече инсталиран софтуер и хардуер от потребителите. При съмнение за възникнал проблем незабавно се уведомява Ръководителят 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 само след сканиране за вируси. При наличие на вируси, 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 достъпът на външни лица до компютърната техника в канцеларииите в сградата на СУ "Константин Константинов", гр. Сливен.
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 се съхраняват от Ръководителя на направление ИКТ.
12. 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. Не е разрешено използването на групови профили.

Чл. 6. Контролът на управлението и защитата на достъпа до мрежови връзки и мрежови услуги се извършва чрез активна директория с конкретно потребителско име, осигурено от Ръководителя на направление ИКТ.

Чл. 7. Предоставянето на достъп става по дефиниран вътрешен ред, като се задават определени права на достъп до конкретни информационни ресурси, според заеманата длъжност и функция. Не се осигурява достъп на неоторизирани лица.

Чл. 8. Лицата, които обработват лични данни, използват уникални пароли с достатъчно сложност, които не се записват или съхраняват онлайн.

Чл. 9. Всички пароли за достъп на системно ниво се променят периодично.

Чл. 10. Всички носители на лични данни се съхраняват в безопасна и сигурна среда с ограничен и контролиран достъп.

Чл. 11. На служителите на СУ "Константин Константинов", гр. Сливен, които използват електронни бази данни и техни производни, 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. 12. 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. 13. При изнасяне на носители извън физическите граници на СУ "Константин Константинов", гр. Сливен, те се поставят в подходяща опаковка и в запечатан плик.

Чл. 14. 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. 15. 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. 16. След като повече не са необходими, носителите се унищожават сигурно и безопасно. Физическото унищожаване на информационните носители става със счупване, след като се провери, че необходимата информация е копирана и цялата информация е изтрита от тях преди унищожаване.

РАЗДЕЛ III. РАБОТНО МЯСТО

Чл. 17. Работното място се състои от работно помещение, работна маса и стол, компютърна и периферна техника, комуникационни средства.

Чл. 18. Всеки служител отговаря за целостта на компютърната и периферна техника, програмните продукти и данни, инсталирани на компютъра на неговото работно място.

Чл. 19. 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. 20. Забранява се на външни лица работата с персоналните компютри на СУ "Константин Константинов", гр. Сливен, освен за:

1. упълномощени фирмени специалисти в случаите на първоначална инсталация, програми и сервизна намеса, но задължително в присъствие на Директор, Заместник-директор или Ръководителя на направление ИКТ;
2. 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. 21. След края на работния ден всеки служител задължително изключва компютъра, на който работи.

Чл. 22. При загуба на данни или информация от служебния компютър, служителят незабавно уведомява Ръководителя на направление ИКТ. Ръководителят на направление ИКТ оказва съответната техническа помощ или организира ремонт, ако е необходимо.

Чл. 23. Забраняват се опити за достъп до компютърна информация и бази данни, до които не са предоставени права, както и извършването на каквито и да е действия, които улесняват трети лица за несанкциониран достъп.

Чл. 24. Инсталиране и разместване на компютърни конфигурации и части от тях, на периферна техника и на мрежови компоненти се извършва само след съгласуване с Ръководителя на направление ИКТ.

Чл. 25. 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 "Константин Константинов", гр. Сливен.

Чл. 26. Служителите имат право да обменят компютърна информация посредством вътрешна компютърна мрежа само във връзка с изпълнение на служебните си задължения.

Чл. 27. Архивирана компютърна информация се предоставя само на служители, които имат право на достъп, съгласно заеманата от тях длъжност и изпълнявана задача.

Чл. 28. 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. 29. Достъпът до помещенията с комуникационните шкафове се ограничава по възможност само до Ръководителя на направление ИКТ и специализиран по поддръжката им персонал.

РАЗДЕЛ IV. ПОЛЗВАНЕ НА КОМПЮТЪРНАТА МРЕЖА И ИНТЕРНЕТ

Чл. 30. Компютрите, свързани в мрежата на СУ "Константин Константинов", гр. Сливен, използват интернет само от доставчик, с когото училището има сключен договор за доставка на интернет.

Чл. 31. Ръководителят на направление ИКТ:

1. избира техническите устройства, извършва необходимите настройки за достъп до интернет, като използва необходимите мрежови комутатори, VLAN, рутери, защитни стени и VPN;
2. разделя логически локалната мрежа на четири отделни мрежи: локална мрежа за администрация, локална мрежа за учители, локална мрежа за ученици и локална мрежа за гости;
3. създава потребителски имена и пароли за работа с компютърната мрежа.

Чл. 32. Ползването на компютърната мрежа и електронните платформи (Школо, Уча се, Електронни учебници и др.) от служителите става чрез получените потребителско име и парола.

Чл. 33. Ползването на интернет и служебна електронна поща се ограничават съобразно скоростта на достъп и служебните задължения на служителите.

Чл. 34. Служителите са длъжни да не споделят своите потребителски имена и пароли с трети лица и носят дисциплинарна отговорност при неправомерно ползване на ресурсите.

Чл. 35. Забранява се свързването на компютри едновременно в мрежата на СУ "Константин Константинов", гр. Сливен и в други мрежи, когато това позволява разкриване на IP адреси или противоречи на Наредбата за минималните изисквания за мрежова и информационна сигурност.

Чл. 36. Използването на комуникатори (Skype, Facebook Messenger, Viber, Zoom и др.), които създават предпоставки за достъп на злонамерен софтуер, да е ограничено и единствено и само за служебна цел.

Чл. 37. Забранява се съхраняването на компютрите на СУ "Константин Константинов", гр. Сливен на лични файлове с текст, изображения, видео и аудио.

Чл. 38. Забранява се отварянето без контрол от страна на Ръководителя на направление ИКТ 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 знаци.

Чл. 39. Не се толерира влизането в Интернет сайтове с неизвестно съдържание.

РАЗДЕЛ V. ЗАЩИТА ОТ КОМПЮТЪРНИ ВИРУСИ И ДРУГ ЗЛОВРЕДЕН СОФТУЕР

Чл. 40. С цел антивирусна защита се прилагат следните мерки:

1. Всички персонални компютри имат инсталиран антивирусен софтуер в реално време, който се обновява.
2. 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;
    - активира защитата на различните програмни продукти и настройва защитната стена на система;
    - проверява за правилно настроен софтуер за автоматично обновяване на операционната система и инсталирания софтуер.
3. При поява на съобщение от антивирусната програма за вирус, всеки служител задължително информира Ръководителя на направление ИКТ.

РАЗДЕЛ VI. НЕПРЕКЪСНАТОСТ НА РАБОТАТА И УПРАВЛЕНИЕ НА ИНЦИДЕНТИ

Чл. 41. Прилагат се следните мерки с цел непрекъсваемост на работата:

1. Всички устройства за съхранение на данни да са свързани към устройство за непрекъсваемост на ел. снабдяването (UPS).
2. При срив в локалната компютърна мрежа, всеки потребител следва да запише отворените файлове на локалния си компютър, за да се избегне загуба на информация.

Чл. 42. При възникване на инцидент, свързан с мрежовата или информационната сигурност (напр. неоторизиран достъп, пробив в сигурността, загуба на данни), служителите са длъжни незабавно да уведомят Ръководителя на направление ИКТ.

Чл. 43. Ръководителят на направление ИКТ отговаря за:

1. Идентифициране, анализ и ограничаване на инцидента.
2. Възстановяване на засегнатите системи и данни.
3. Документиране на инцидента и предприетите мерки.
4. Вземане на решение за привличане на външна фирма за поддръжка или ремонт, когато това надхвърля вътрешните компетенции или изисква специализиран сервиз.

РАЗДЕЛ VII. 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.

РАЗДЕЛ VIII. ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

1. Ръководителите и служителите в СУ "Константин Константинов", гр. Сливен са длъжни да познават и спазват разпоредбите на тези правила.

2. Контролът по спазване на правилата се осъществява от ръководството на СУ "Константин Константинов", гр. Сливен.

3. Настоящите вътрешни правила се разглеждат и оценяват периодично с оглед ефективността им, като СУ "Константин Константинов", гр. Сливен може да приема и прилага допълнителни мерки и процедури.

4. Тези правила са разработени съгласно Наредбата за минималните изисквания за мрежова сигурност (приета с ПМС № 186 от 26.07.2019 г.) и са утвърдени със заповед на директора на СУ "Константин Константинов", гр. Сливен.