ПГИТ "АЛЕКО КОНСТАНТИНОВ"
ВЕЛИНГРАД
бул. "Съединение" №49, тел./факс 0359 5-40-75
e-mail:pgit_vd@abv.bg, HTTP://WWW.PGIT-VELINGRAD.COM/

ЗАПОВЕД

№ РД-04-1059/12.04.2021г

На основание чл.258, ал.1,чл. 259, ал. 1 от Закона за предучилищното и училищното образование, във връзка с чл. 31, ал. 1, т. 1 от Наредба №15/ 2019 г. за статута и професионалното развитие на учителите, директорите и другите педагогически специалисти, чл.1, ал.1, т.1 от Наредбата за минималните изисквания за мрежова сигурност /приета с ПМС №186/26.07.2019г./

УТВЪРЖДАВАМ:

Вътрешни правила за мрежова и информационна сигурност в ПГИТ „Ал.Константинов"Велинград.

Препис от заповедта да се сведе до знанието на учителите за сведение и изпълнение.

Контрол по изпълнение на заповедта ще осъществявам лично.

Директор:
/Л.Байлова/

Професионална гимназия по икономика и туризъм
"Алеко Константинов" Велинград
бул. "Съединение" №49, тел./факс 0359 5-40-75
e-mail:pgit_vd@abv.bg, http://www.pgit-velingrad.com

ВЪТРЕШНИ ПРАВИЛА

ЗА МРЕЖОВА И

ИНФОРМАЦИОННА

СИГУРНОСТ

В ПГИТ

„АЛ. КОНСТАНТИНОВ"

ВЕЛИНГРАД

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 ПГИТ „Алеко Константинов" Велинград. 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 ПГИТ „Алеко Константинов" Велинград 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

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 административното звено.
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 административното звено или с член на екипа за "Дигитализация".
9. Не се допуска достъпа на външни лица до компютърната техника в канцеларите в сградата на ПГИТ „Алеко Константинов" Велинград.
10. Служителите не могат да отстъпват паролите си за достъп до системата на други служители, външни лица, роднини и приятели.
11. Паролите и правата за достъп всеки служител съхранява лично и отговаря за тях. 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. Контрол на управлението и защитата на достъпа до мрежови връзки и мрежови услуги се извършва от външна фирма само чрез разрешение на Директора, екипа за Дигитализация и 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 заемната длъжност и функция. Не се задава и 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 ПГИТ „Алеко Константинов“ Велинград, 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. 12. 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. 13. При изнасяне на носители извън физическите граници на ПГИТ „Алеко Константинов“ Велинград, 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. Потребителите на мобилни компютърни средства и мобилни телефони отговарят за защитата им от кражба и не ги оставят без наблюдение

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 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 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 ПГИТ „Алеко Константинов“ Велинград, 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, екип за дигитализация 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.

Чл. 21. След края на работния ден всеки служител задължително изключва компютъра, на който работи или го привежда в режим log off;

Чл. 22. При загуба на данни или информация от служебния компютър, служителят незабавно уведомява, административното звено, екипа по дигитализация и ръководителя на направление „ИКТ“, който му оказва съответна техническа помощ.

Чл. 23. 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. 24. 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. 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 ПГИТ „Алеко Константинов“ Велинград

Чл. 26. 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. 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 осъществява след разрешение на Директора, екипа за Дигитализация и ръководител ИКТ.

РАЗДЕЛ IV. ПОЛЗВАНЕ НА КОМПЮТЪРНАТА МРЕЖА И ИНТЕРНЕТ

Чл. 30. Компютрите, свързани в мрежата на ПГИТ „Алеко Константинов“ Велинград, използват интернет само от доставчик, с когото училището има сключен договор за доставка на интернет.

Чл. 31. Фирмата, доставчик на интернет услугата, в договора си да допълни контрамерки предприети срещу кибератаки, включително и /D/DoS такива.

1. Фирмата за инсталиране и поддръжка на видеонаблюдението в ПГИТ „Алеко Константинов“ Велинград, избира техническите устройства, извършва необходимите настройки за достъп.
2. Фирмата за инсталиране и поддръжка на турникети за контрол на достъпа в ПГИТ „Алеко Константинов“ Велинград, избира техническите устройства, извършва необходимите настройки за достъп, съхранява данните на сигурно място.
3. Фирмата за изграждане, инсталиране и поддръжка на Wi-Fi в ПГИТ „Алеко Константинов“ Велинград, извършва необходимите настройки за достъп на техническите устройства съвместно с фирмата изградила Интернет мрежата.
4. Фирмата изграждаща вътрешната 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 четири отделни мрежи – локална мрежа за администрация, локална мрежа за учители, локална мрежа за ученици и локална мрежа за гости и създава потребителски имена и пароли за работа с компютърната мрежа. Физически и отдалечен достъп.

Да се изисква от външните фирми да направят преглед на мерките, които са взети за защита на всяко приложение, сървър, мрежови устройства, включително и на конфигурациите им. В договорите да се посочат технически мерки за да станат по устойчиви на кибератаки.

Чл. 32. Ползването на компютърната мрежа и електронните платформи /Школо, Уча се, Електронни учебници, всички платформи на МОН 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 ползвания достъп до интернет, броя на откритите работни места и необходимостта от ползване на тези услуги съобразно служебните задължения на служителите.

Чл. 34. 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. 35. Забранява се свързването на компютри едновременно в мрежата на ПГИТ „Алеко Константинов" Велинград 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. 36. Използването на комуникатори (skype, facebook, messenger, viber, zoom и др. подобни), осигуряващи достъп извън рамките на компютърната мрежа на ПГИТ „Алеко Константинов" Велинградиздаващи 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. 37. Забранява се съхраняването на компютрите на ПГИТ „Алеко Константинов" Велинград на лични файлове с текст, изображения, видео и аудио.

Чл. 38. 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. 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:

- Всички персонални компютри в администрацията имат инсталиран антивирусен софтуер в реално време, който се обновява.
- 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. 41. 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 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. 42. Всеки служител, който работи с класифицирана информация, осигурява автоматично създаване на архивни копия всекидневно.

Чл. 43. 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 следните програми се архивират всеки ден в края на работното време:
   - база данни на програмата Админ Про и Админ РД; Школо, НЕИСПУО
   - база данни от програма и платформи ТРЗ и Счетоводство
   - база данни от модул „Граждански договори";
   - Платформи по НП и Европейски проекти и др.

Следните служители отговарят за дейността си и информацията които предоставят: Л. Байлова, В. Цурева, П. Веселинов, С. Похлупкова, Е. Гергова, А. Илинова, Й. Николва, Р. Райчев, В. Папанова, Л. Таратаева, М. Джокова, В. Папаркова.

РАЗДЕЛ VIII. ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

§ 1. Ръководителите и служителите в ПГИТ „Алеко Константинов" Велинград са длъжни да познават и спазват разпоредбите на тези правила.

§ 2. Контролът по спазване на правилата се осъществява от ръководството на ПГИТ „Алеко Константинов" Велинград.

§ 3. Настоящите вътрешни правила се разглеждат и оценяват периодично с оглед ефективността им, като ПГИТ „Алеко Константинов" Велинград 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.) и влизат в сила от датата на извеждане на Заповед № ..... на Директора на ПГИТ „Алеко Константинов" Велинград.

ПРЕПОРЪКА

1. Становище на Комисията за регулиране на съобщенията относно това дали доставчиците на електронна поща попадат в обхвата на ЗЕС. "Под „електронна поща" се разбират два вида услуги. Едната услуга е web-базирана електронна поща, която не включва предоставяне на услуга за достъп до интернет – например популярните услуги като **„абв-поща" или gmail.** Този вид електронна поща не представлява обществена електронна съобщителна услуга съгласно действащия ЗЕС…" Това ясно показва, че всички училища следва да спазват разпоредбите на чл. 28 от Регламент (ЕС) 2016/679 и

да имат подписано писмено споразумение за обработване на лични данни с доставчика на електронна поща.

Предлагаме, като официална електронна поща на ПГИТ „Алеко Константинов“ да стане 1304231@edu.mon.bg поради по-голяма сигурност и защита.

2. Организиране на регулирани обучения на екипа относно киберхигиена и добри практики за мрежова информационна сигурност.
3. Да се изготви план за действие при инциденти и атаки.

Изготвил:

Сн. Похлупкова

Й. Николова

В. Кривулев

Л. Таратаева-Мизурска

В. Папанова