ПРОФЕСИОНАЛНА ГИМНАЗИЯ ПО ТРАНСПОРТ
гр. София, район "Искър", ул. Мюнхен, №12
тел: 973-26-57; 973-28-64; 973-28-73

ВЪТРЕШНИ ПРАВИЛА ЗА МРЕЖОВА И ИНФОРМАЦИОННА СИГУРНОСТ

В ПРОФЕСИОНАЛНА ГИМНАЗИЯ ПО ТРАНСПОРТ

гр. София

Приети с решение на Общо събрание № 4 / 05.04.2023 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 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 ПГТ – 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 под друг начин, както и да обменят информация чрез съответните устройства и програми.

Чл. 2. Потребителите на информационни системи в ПГТ – 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 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 отговорника „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 интернетвръзка, с изключение на техници от оторизирани фирми и то само придружени от отговорника „ИКТ"

9. Не се допуска достъпа на външни лица до компютърната техника в канцеларииите в сградата на училището.

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 отговорника „ИКТ". 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 чрез средствата на активна директория с конкретно потребителско име, осигурено от отговорника „ИКТ", който контролира компютрите, използвани за достъп до мрежи и мрежови услуги.

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 задава и не се осигурява достъп на неоторизирани лица.

Чл. 8. Лицата, които обработват лични данни, използват уникални пароли с достатъчна степен 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 ПГТ – гр. София, 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 училището, 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.

1. Движението на служебни мобилни компютърни средства се отбелязват в контролен лист.

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 ПГТ – гр. София, 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 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 отговорника „ИКТ".

Чл. 21. След края на работния ден всеки служител задължително изключва служебния компютър, на който работи.

Чл. 22. При загуба на данни или информация от служебния компютър, служителят незабавно уведомява отговорника „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 стройства се извършва само след съгласуване с отговорника „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 ПГТ – гр. София.

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 ограничава по възможност само до специализиран по поддръжката им персонал.

РАЗДЕЛ IV. ПОЛЗВАНЕ НА КОМПЮТЪРНАТА МРЕЖА И ИНТЕРНЕТ

Чл. 30. Компютрите, свързани в мрежата на ПГТ – гр. София, използват интернет само от доставчик, с когото училището има сключен договор за доставка на интернет.

Чл. 31. 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 на две отделни мрежи – локална мрежа за администрация и учители и локална мрежа за ученици и гости, и 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 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 ПГТ – гр. София 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 ПГТ – гр. София 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. 37. Забранява се съхраняването на компютрите на ПГТ – гр. София 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 имат инсталиран антивирусен софтуер в реално време, който се обновява.

➢ Отговорника „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 отговорника „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 липса на ел. захранване за повече от 10 мин., отговорника „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. 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;
- база данни на програмата НЕИУСПО;
- база данни от програма ФСД и ТРЗ на „Информационно обслужване“

РАЗДЕЛ VIII. ПРИЛОЖЕНИЯ

Приложение № 1 към чл. 40

УВЕДОМЛЕНИЕ ЗА ИНЦИДЕНТ

към РНИКТ в ПГТ

Необходима информация	Детайли	Данни
(до 2 часа)		
Лице, подаващо уведомлението	Име и фамилия	
Вашият телефонен номер	(GSM)	
Служебна електронна поща		
Организация	Наименование на организацията, засегната от инцидента	
Лице за контакт (за	Име, телефонен номер и	

целите на разрешаването на инцидента)	електронна поща на компетентното лице от институцията	
Дата и час	Вписват се датата и часът на възникване на инцидента, ако не е възможно – датата и часът на откриването му	
Тип на инцидента		0 Virus 0 Trojan 0 Botnet 0 Dos/DDos 0 Malware 0 Port Scan 0 Spam 0 Phishing 0 Pharming 0 Probe 0 Crack 0 Copyright 0Ransomware 0 Defacement 0 Exploiting known Vulnerabilities 0 Application Compromise 0 Login Attempts 0 SQL injections 0 Unknown 0 Other
Кратко описание на инцидента	Вписва се кратко описание на инцидента, като се включва всяка практическа/ техническаинформация (тази информация се предоставя, в случай, че е налична)	
Трансгранично въздействие	•Вписва се информация за евентуално трансгранично въздействие и се посочват държавите •Вписва се информация за услугите, които са засегнати	
Въздействие върху други съществени услуги	Вписва се информация на кои други съществени услуги евентуално ще окаже въздействие	
Засегната система (попълва се, ако е налична информацията)	IP Address: DNS: Operating System:	
Предприети действия	Описват се първоначалните действия, предприети до момента - до 2 часа от засичането на инцидента	

ПРОФЕСИОНАЛНА ГИМНАЗИЯ ПО ТРАНСПОРТ
гр. София, район "Искър", ул. Мюнхен, №12
тел: 973-26-57; 973-28-64; 973-28-73

Приложение № 2 към чл. 12, ал. 1

Контролен лист за движение на служебни мобилни компютърни средства

Във връзка с вътрешния правилник за мрежова и информационна сигурност и приемно предавателен протокол за лаптоп от с-ка……, № ……

на

……

Изнесен от сградата на институцията на дата	Върнат в сградата на институцията на дата	ПОДПИС

РАЗДЕЛ IX. ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

§ 1. Ръководителите и служителите в ПГТ – гр. София, са длъжни да познават и спазват разпоредбите на тези правила.

§ 2. Контролът по спазване на правилата се осъществява от ръководството на ПГТ – гр. София.

§ 3. Настоящите вътрешни правила се разглеждат и оценяват периодично с оглед ефективността им, като ПГТ 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.) и влизат в сила от датата на извеждане на

Заповед № ……..