МИНИСТЕРСТВО НА ОБРАЗОВАНИЕТО И НАУКАТА
НАЦИОНАЛНА ТЪРГОВСКА ГИМНАЗИЯ
✉ 4002 Пловдив, бул."Руски" № 50, ☎ (032) 64 23 63 – Директор, (032) 64 23 23 – Зам.-директори, (032) 64 38 22 Секретар, e-mail: info-1690175@edu.mon.bg / tgschool@ntg-plovdiv.net

Утвърдил:
д-р Петя Герасимова
Директор на НТГ-Пловдив

ВЪТРЕШНИ ПРАВИЛА ЗА МРЕЖОВА И ИНФОРМАЦИОННА СИГУРНОСТ
на Национална търговска гимназия – Пловдив

I. ОБЩИ ПОЛОЖЕНИЯ

Чл. 1. (1) Настоящите вътрешни правила определят политиката на мрежова и информационна сигурност на НТГ – Пловдив и имат за цел осигуряването на управление и контрол на работата на информационните системи в НТГ – Пловдив.
(2). В настоящите вътрешни правила 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 (1) Потребителите в информационната система на НТГ – Пловдив са задължени с отговорни действия да гарантират ефективното и ефикасно използване на системите.
(2). Системата за сигурност на информацията има за цел да защитава учениците, учителите, служителите, партньотите и клиентите на НТГ – Пловдив 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 определено оборудване за изпълнение на служебните им задължения.
(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 при спазване на Наредбата за минималните изисквания за мрежова сигурност (приета с ПМС 186/26.07.2019г.)

II. МЕРКИ ЗА МРЕЖОВА И ИНФОРМАЦИОННА СИГУРНОСТ
Управление, роли и отговорности

Чл. 3. Мрежовата и информационна сигурност се осъществява чрез мерки пропорционални на рисковете за постигане на основните цели:

1. Организационни мерки
2. Технологични мерки
3. Технически мерки

Чл. 4. Мерките, които се прилагат във връзка с осигуряване на мрежова и информационна сигурност са насочени към запазване на достъпността, интегритета (цялост и наличност) и конфиденциалността на информацията по време на целия й жизнен цикъл, включващ създаването, обработването,

съхранението, пренасянето и унищожението й в и чрез информационните и комуникационни системи в НТГ – Пловдив.

Чл. 4. (1) Директорът на НТГ – Пловдив носи пряка отговорност за мрежовата и информационната сигурност;

1. създава условия за прилагане на комплексна система от мерки за управление на тази сигурност по смисъла на международен стандарт БДС ISO/IEC 27001; системата обхваща всички области на сигурност, които засягат мрежовата и информационната сигурност, включително физическата сигурност на информационните и комуникационните системи;
2. осигурява необходимите ресурси за прилагане на пропорционални и адекватни на рисковете организационни, технически и технологични мерки, гарантиращи високо ниво на мрежова и информационна сигурност;
3. упражнява контрол върху нивото на мрежовата и информационната сигурност чрез:

а) организиране на одити по смисъла на чл. 35, ал. 1, т. 1 и 3 за доказване на съответствието на предприетите мерки с изискванията на нормативните актове и приетите стандарти;
б) провеждане минимум веднъж в годината на периодичен преглед на мрежовата и информационната сигурност и на адекватността на предприетите мерки;

4. определя, документира и налага отговорности по изпълнението, контрола и информираността за всички процеси и дейности, свързани с развитието, поддръжката и експлоатацията на информационните и комуникационните системи, като се спазва принципът, че едно лице не може да контролира собствената си дейност.

(2) Директорът определя служител, отговарящ за мрежовата и информационната сигурност, като:

1. служителят, отговарящ за мрежовата и информационната сигурност, е на пряко подчинение на ръководителя на НТГ - Пловдив, с цел пряко информиране за състоянието и проблемите в мрежовата и информационната сигурност;
2. Функции на служителя, отговарящ за мрежовата и информационната сигурност – Ръководител направление ИКТ:

- Ръководи дейностите, свързани с постигане на високо ниво на мрежова и информационна сигурност
- Участва в изготвянето на политиките и документираната информация.
- Консултира ръководството във връзка с информационната сигурност.
- Ръководи периодичните оценки на рисковете за мрежовата и информационната
- Периодично (не по-малко от веднъж в годината) изготвя доклади за състоянието на мрежовата и информационната сигурност в административното звено и ги представя на ръководителя.
- Предлага санкции за лицата, нарушили мерките за мрежовата и информационната сигурност.

Чл. 5. Документирана информация

(1) За намаляване на загубите от инциденти чрез намаляване на времето за реагиране и разрешаването им, както и за намаляване на вероятността от възникване на инциденти, породени от човешки грешки, НТГ - Пловдив поддържа следната документация:

1. опис на информационните активи;
2. документация на структурната кабелна система;
3. техническа, експлоатационна и потребителска документация на информационните и комуникационните системи и техните компоненти;

(2) Документацията по ал. 1 трябва да е:

1. еднозначно идентифицирана като заглавие, версия, дата, автор, номер и/или др.;
2. поддържана в актуално състояние, като се преразглежда и при необходимост се

обновява поне веднъж годишно;
3. достъпна само до тези лица, които е необходимо да я ползват при изпълнение на служебните си задължения.

Чл. 6. Класификация на информацията

(1) Всяка информация, която стане достъпна за служителите при изпълнение на служебните им задължения, ако са свързани с НТГ – Пловдив и дейността й, клиенти или партньори за сътрудничество, се счита за собствена и поверителна информация на НТГ – Пловдив, като по този начин се подчинява на защита в съответствие с приложимите закони и правната уредба, относно защита на поверителна информация, търговската тайна и личните данни.

(2) за да се установи подходяща защита на информацията, НТГ – Пловдив извършва класификация на информацията. Информацията подлежи на защита, независимо от това дали такава информация 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 НТГ – Пловдив:

КАТЕГОРИЯ	ОПИСАНИЕ	ПРИМЕРИ
Публична информация	Информация, която може да бъде обработвана и разпространявана в рамките на НТГ – Пловдив или извън нея, без никакво отрицателно въздействие, някой от нейните партньори, клиенти и/или свързани лица.	1. Финансови отчети, публикувани до обществени органи. 2. Информация, достъпна чрез публични регистри 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 информацията.
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 НТГ, може да навреди на НТГ и/или на нейните служители, партньори и клиенти.	1. Документи разработени и/или изготвени от който и да е служител на НТГ. 2. Всички директории (информация за връзка) и т.н., установени и/или използвани за бизнес целите на НТГ. 3. Всякакви вътрешни работни бележки, изявления, становища, разработени за бизнес нуждите на НТГ или с цел ефективност на дейността на НТГ.
Поверителна информация	Всяка информация от такова значение за НТГ, за нейните клиенти, партньори и/или свързани лица, неоторизираното разкриване на която, може да окаже неблагоприятно	1. Политики, процедури, вътрешни правила, управленски решения. 2. Информазия, за която е указано на служителя, че е търговска тайна.

	въздействие върху дейността, репутацията, цялостното състояние на НТГ, клиенти, партньори, като последиците биха причинили сериозни вреди/щети на някое от тези лица.	3. Друга информация от финансово, кадрово, правно, маркртингово естество, планове и операции. 4. Данни за лична идентификация. 5. Информация, която подлежи на защита по силата на споразумение за поверителност или споразумения за сътрудничество.

III. КОНТРОЛ НА ДОСТЪПА И ПРАВИЛА ЗА РАБОТА С НОСИТЕЛИ. ОЦЕНКА НА РИСКА

Чл. 7. Защитата и контролът на информационните и конпютърните 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. Техниката се използва изключително и само за служебни цели
4. Не се позволява инсталирането на нов и реконфигурирането от потребителите на вече инсталиран софтуер и хардуер, както и самостоятелни опити за поправка или подобрения. При съмнение за възникнал пробле, незабавно се уведоява лицет, отговарящо за мрежовата и информационна сигурност.
5. Не се позволява използването на внесени отвън софтуер и хардуер.
6. Използването на внесени отвън информационни носители (дискове, дискети, флаш памет) и др. става при условие, че те се сканират за наличието на вируси.
7. Не се допускат външни лица до комуникационната техника и техниката за интернет, с изключение на техници от оторизирани фирми, придружени от представител на НТГ.
8. Служителите не могат да преотстъпват паролите си за достъп до системата на други служители, външни лица, роднини и приятели.
9. Паролите за достъп на всички служители се променят периодично.
10. Учениците в НТГ – Пловдив са длъжни:

- Да използват училищната мрежа и интернет само за образователни цели.
- Забранено е използването на мрежата за извършване на стопанска или незаконна дейност.
- Учениците не трябва да предоставят лична информация за себе си и за своите родители като име, парола, адрес, телефон, месторабота и служебен телефон на родителите, без предварително разрешение от тях.
- Учениците не трябва да приемат срещи с лица, с които са се запознали в интернет, освен след съгласието на родителите.
- Учениците не трябва да изпращат или да отговарят на съобщения, които са обидни, заплашващи или неприлични.
- Забранено е изпращането на анонимни или верижни съобщения.
- Забранено е извършването на дейност, която застрашава сигурността на училищната компютърна мрежа или атакува други системи.
- Забранява се използването на чуждо потребителско име, парола и електронна поща.
- При работа в мрежата, учениците трябва да уважават правата на другите и да пазят доброто име на училището.

Чл. 8. Управление на риска

1. Извършването на анализ и оценка на риска за мрежовата и информационната сигурност се извършва регулярно, но не по-рядко от веднъж годишно, или когато се налагат съществени изменения в целите, вътрешните и външните условия на работа, информационната и комуникационната инфраструктура, дейностите или процесите.
2. Анализът и оценката на риска се документират
3. На основание на анализа и оценката на риска, се изготвя план за намаляване на неприемливите рискове, който включва:

- подходящи и пропорционални мерки за смекчаване на неприемливите рискове;
- необходими ресурси за изпълнение на тези мерки;
- срок за прилагане на мерките;
- отговорни лица.

Чл. 9. Управление на информационните активи

1. Всеки служител отговаря за целостта на компютърната и периферна техника, програмните продукти и данни, инсталирани на компютъра на неговото работно място.
2. Служителят има право да работи на служебен компютър като достъпът до данните се осъществява от него с въвеждането на потребителско име и парола.
3. Забранява се на външни лица работата с персонални компютри на НТГ.
4. След края на работния ден всеки служител задължително изключва компютъра си.
5. При загуба на информация от служебния компютър незабавно се уведомява лицето, отговарящо за мрежовата и информационна сигурност.
6. Забраняват се опити за достъп до компютърна информация и база данни, до които не са предоставени права, съобразно заеманата длъжност, както и извършването на каквито и да е действия, които улесняват трети лица за несанкциониран достъп.
7. Инсталирането и разместването на компютърни конфигурации и части от тях, на периферна техника, на активни и пасични компоненти на локални компютърни мрежи, на комуникационни устройства, се извършва само след съгласуване с лицето, отговарящо за мрежоват и информационна сигурност в НТГ.
8. Забранява се използването на преносими магнитни, оптични и други носители за презаписване на данни за прехвърляне на файлове между компютри, свързани в компютърната мрежа на НТГ.
9. Достъпът до компютърна информация, база данни и софтуер се ограничава посредством технически методи – идентификация на потребител, пароли, забрана за копиране, проследяване и неконтролиран достъп.

IV. ПОЛЗВАНЕ НА КОМПЮТЪРНАТА МРЕЖА И ИНТЕРНЕТ

Чл. 10. Ползването на компютърната мрежа и интернет в НТГ, се осъществява чрез спазването на следните правила:

1. Разделяне логически локалната мрежа на три отделни мрежи – локална мрежа за администрацията, локална мрежа за учителите и локална мрежа за учениците.
2. Плзването на компютърната мрежа и електронните платформи от служителите става чрез потребителско име и парола.
3. Служителите 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, достъпът до интернет или електронна поща.
4. Компютрите, свързани в мрежата на НТГ – Пловдив ползват интернет само от доставчик, с когото училището има сключен договор.

5. Забранява се свързването на компютрите едновременно в мрежата на НТГ и в други мрежи, когато това позволява идентифициране на IP адреси от мрежата на НТГи/или в противоречие с изискванията на Наредбата за минималните изисквания за мрежова и информационна сигурност.
6. Забранява се съхраняване на служебните компютри на лични файлове с текст, изображения, видео и аудио.

V. ЗАЩИТА ОТ КОМПЮТЪРНИ ВИРУСИ И ДРУГ ЗЛОВРЕДЕН СОФТУЕР

Чл. 11. С цел антивирусна защита, всички персонални компютри в НТГ имат инсталиран антивирусен софтуер в реално време, който се обновява ежедневно.

VI. НЕПРЕКЪСНАТОСТ НА РАБОТА

Чл. 12. Следните мерки се прилагат с цел антивирусна защита:
1. Всички устройства за съхранение на данни да са свързани към устройство за непрекъсната работа.
2. При липса на електрозахранване повече от 10 мин. се уведомява лицето, отговорно за мрежова и информационна сигурност и започва процедура за поетапно спиране на устройствата.
3. При срив в локалната компютърна мрежа, всеки потребител следва да запише файловете, за да избегне загуба на информация.

VII. ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

1. Служителите от педагогическия и непедагогическия персонал на НТГ – Пловдив са длъжни да познават и спазват разпоредбите на тези правила.
2. Контролът по спазването на правилата се осъществява от ръководството на НТГ.
3. Настоящите вътрешни правила се разглеждат и оценяват периодично с оглед ефективността им, като НТГ може да приема и прилага допълнителни мерки и процедури, които са целесъобразни и необходими.
4. Тези правила са разработени съгласно Наредбата за минималните изисквания за мрежова и информационна сигурност (приета с ПМС 186/26.07.2019г.) и влизат в сила със Заповед РД-06- 1356/08.07.2021 г. на Директора на НТГ – Пловдив.

ПЛАН ЗА ДЕЙСТВИЕ ПРИ ИНЦИДЕНТИ

Отговорник при настъпване на инцидент	
Ред за информиране	
Мерки, които трябва да се предприемат и отговорното за това лице	
Ред за консултиране	
Ред за следене на параметрите по време на инцидента	

Служител, който ще събира и съхранява необходимата информация	