



НЕВРОКОПСКА ПРОФЕСИОНАЛНА ГИМНАЗИЯ "ДИМИТЪР ТАЛЕВ"

гр. Гоце Делчев, бул. "Гоце Делчев" №36, тел.: 0884280707, e-mail: info-10200@edu.mon.bg, www.npg.bg

УТВЪРДИЛ: /П/

Директор
/Мария Георгиева/

ВЪТРЕШНИ ПРАВИЛА ЗА МРЕЖОВА И ИНФОРМАЦИОННА СИГУРНОСТ

В НЕВРОКОПСКА ПРОФЕСИОНАЛНА ГИМНАЗИЯ

„Димитър Талев“

гр. Гоце Делчев

2024/2025 г.



СЪДЪРЖАНИЕ

РАЗДЕЛ I. ОБЩИ ПОЛОЖЕНИЯ	3
РАЗДЕЛ II. КЛАСИФИКАЦИЯ НА ИНФОРМАЦИЯТА	3
РАЗДЕЛ III. КОНТРОЛ НА ДОСТЪПА И ПРАВИЛА ЗА РАБОТА С НОСИТЕЛИ	5
РАЗДЕЛ IV. РАБОТНО МЯСТО	7
РАЗДЕЛ V. ПОЛЗВАНЕ НА КОМПЮТЪРНАТА МРЕЖА И ИНТЕРНЕТ	9
РАЗДЕЛ VI. ЗАЩИТА ОТ КОМПЮТЪРНИ ВИРУСИ И ДРУГ ЗЛОВРЕДЕН СОФТУЕР.....	10
РАЗДЕЛ VII. НЕПРЕКЪСНАТОСТ НА РАБОТАТА.....	10
РАЗДЕЛ VIII. ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ	11



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 26.07.2019г.) и имат за цел осигуряването на контрол и управление на работата на информационните системи в НПП „Димитър Талев“ гр. Гоце Делчев. 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 НПП „Димитър Талев“ гр. Гоце Делчев 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 (приета с ПМС № 186 от 26.07.2019г.).

РАЗДЕЛ II. КЛАСИФИКАЦИЯ НА ИНФОРМАЦИЯТА

Чл.4. ал.(1) Всяка информация, която стане достъпна за служителите при изпълнение на служебните им задължения, ако са свързани с НПП „Димитър Талев“ и негова дейност, клиенти или партньори за сътрудничество, се счита за собствена и поверителна информация на НПП „Димитър Талев“, като по този начин се подчинява на защита в съответствие с приложените закони и правната уредба относно защитата на поверителна информация, търговската тайна и личните данни.

ал.(2). За да се установи подходяща защита на информацията, НПП „Димитър Талев“ извършва класификация на информацията. Информацията подлежи на защита, независимо от това дали тя е на разположение на служители под формата на печатни материали, устройства за съхранение на данни, аудио/видео материали или по друг начин.



ал.(3). Обща класификация на информацията, приложима в рамките на НПП „Димитър Талев“:

Категория	Описание	Примери
Публична информация	Информация, която може да бъде обработвана и разпространявана в рамките на НПП „Димитър Талев“ или извън него без никакво отрицателно въздействие върху НПП „Димитър Талев“, някой от партньорите, клиентите и/или свързани лица на НПП „Димитър Талев“.	<ul style="list-style-type: none">- Финансови отчети, публикувани до обществени органи;- Информация, достъпна чрез публични ресурси 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 информация.
Вътрешна информация	Всяка потреба на информация по какъвто и да е начин, в случай, че е извършена в нарушение на изискванията на приложимите закони или подзаконовни актове, тези Правила или всяка друга регулация, приета от НПП „Димитър Талев“, може да навреди на интересите на НПП „Димитър Талев“ и/или неговите служители, партньори, клиенти;	<ul style="list-style-type: none">- Документи, разработени и/или изготвени от който и да е служител на НПП „Димитър Талев“;- Всякакви вътрешни работни бележки, изявления, становища, разработени за нуждите на НПП „Димитър Талев“ или с цел ефективност на дейността на НПП „Димитър Талев“ ;
Поверителна информация	Всяка информация от такова значение за НПП „Димитър Талев“, неоторизираното разкриване на която би могло да окаже неблагоприятно въздействие върху дейността, операциите, репутацията, цялостното състояние на НПП „Димитър Талев“, клиенти и партньори, която би причинила сериозни вреди/щети на някое от тези лица.	<ul style="list-style-type: none">- Политики, процедури, вътрешни правила, управленски решения;- Информация, за която е указано на служителя, че търговска тайна на НПП „Димитър Талев“;- Друга информация от финансово, кадрово, правно или планово естество;- Данни за лична идентификация;- Информация, която подлежи на защита по силата на споразумение за поверителност, което се подписва от дадения служител;- Информация, която подлежи на защита по силата на споразумение за поверителност или споразумение за сътрудничество, които НПП „Димитър Талев“ е случило в хода на дейността си.



РАЗДЕЛ III. КОНТРОЛ НА ДОСТЪПА И ПРАВИЛА ЗА РАБОТА С НОСИТЕЛИ

Чл.5. 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 административно звено, отговарящо за мрежовата и информационната сигурност
6. Не се позволява използването на внесени отвън софтуер и хардуер.
7. Използването на внесени отвън информационни носители (оптични дискове, дискети, флаш памет 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 представителите на звеното, отговарящо за мрежовата и информационната сигурност. Не се допуска достъпа на външни лица до компютърната техника в административната част в основната сграда на НПГ „Димитър Талев“ гр. Гоце Делчев.
9. Служителите не могат да отстъпват паролите си за достъп до системата на други служители, външни лица, роднини и приятели.
10. Всеки потребител трябва периодично да подменя паролите си за достъп до служебните информационни системи и приложения с цел намаляване рисковете от неправомерни действия.

Чл.6. 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.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 носители на лични данни се съхраняват в безопасна и сигурна среда с ограничен и контролиран достъп;

Чл.10. На служителите на НПГ „Димитър Талев“ гр. Гоце Делчев, които използват електронни бази данни и техни производни (текстове, разпечатки, карти и скици) се забранява:

1. да ги изнасят под каквато и да е форма извън служебните помещения преди извеждане от деловодството (извършване на услуга);
2. да ги използват извън рамките на служебните си задължения;
3. да ги предоставят на външни лица без да е заявена услуга.

Чл.11. За нарушение цялостта 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.12. При изнасяне на носители извън физическите граници на НПГ „Димитър Талев“ гр. Гоце Делчев, те се поставят в подходяща опаковка и в запечатан плик;

Чл.13. На служителите е строго забранено да използват 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.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. 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 IV. РАБОТНО МЯСТО

Чл.16. Работното място се състои от работно помещение, работна маса и стол, компютърна и периферна техника /или интерактивен дисплей/, комуникационни средства;

Чл.17. Всеки служител отговаря за цялостта 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 не трябва да запазва на локалния диск устройството електронни ресурси с чувствителна информация, освен ако същите нямат ниво на достъп чрез защитена парола;

Чл.19. Забранява се на външни лица работата с персоналните компютри в НПГ „Димитър Талев“ гр. Гоце Делчев, 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;
- провеждане на обучения на външни педагогически специалисти по програми и проекти на МОН или РУО;

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 Административно звено, отговарящо за мрежовата и информационната сигурност, което 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 Административно звено, отговарящо за мрежовата и информационната сигурност;

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 НПГ „Димитър Талев“ гр. Гоце Делчев, освен в случаите, в които това се разрешава от оторизираното Административно ниво;

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, като: 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 V. ПОЛЗВАНЕ НА КОМПЮТЪРНАТА МРЕЖА И ИНТЕРНЕТ

Чл.29. Поддържане и подобряване ефективната и непрекъсната работа на разделената логически локалната мрежа на три отделни мрежи – локална мрежа за администрация, локална мрежа за учители и локална мрежа за ученици /с неограничен достъп за учители, с ограничения в достъп и за ученици, като е създадена и защитна виртуална стена, с цел блокиране на достъпа до определени зловредни уебсайтове/;

Чл.30. Ползването на компютърната мрежа и електронните платформи /Школо, Уча се, електронни учебници и други/ от служителите става чрез техните индивидуални служебни потребителски имена и пароли;

Чл.31. 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.32. 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 електронна поща при използване на предоставените им потребителски имена и пароли;

Чл.33. Използването на комуникатори (MS Teams, Skype, Facebook, Messenger, Viber, Zoom и други подобни), осигуряващи достъп извън рамките на компютърната мрежа на НПГ „Димитър Талев“ гр. Гоце Делчев 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.34. Компютрите, свързани в мрежата на НПГ „Димитър Талев“ гр. Гоце Делчев използват интернет само от доставчик, с когото НПГ „Димитър Талев“ гр. Гоце Делчев има сключен договор за доставка на интернет;

Чл.35. Забранява се свързването на компютри едновременно в мрежата на НПГ „Димитър Талев“ гр. Гоце Делчев и в други мрежи, когато това позволява разкриване и



достъп до IP адреси от мрежата на НПГ „Димитър Талев“ гр. Гоце Делчев и/или е в противоречие с изискванията на Наредбата за минималните изисквания за мрежова и информационна сигурност;

Чл.36. Забранява се съхраняването на компютрите на НПГ „Димитър Талев“ гр. Гоце Делчев на лични файлове с текст, изображения, видео и аудио;

Чл.37. Забранява се отварянето без контрол от страна на системния администратор:

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.

РАЗДЕЛ VI. ЗАЩИТА ОТ КОМПЮТЪРНИ ВИРУСИ И ДРУГ ЗЛОВРЕДЕН СОФТУЕР

Чл.38. С цел антивирусна защита се прилагат следните мерки:

ал. (1) Всички персонални компютри имат инсталиран антивирусен софтуер в реално време.

РАЗДЕЛ VII. НЕПРЕКЪСНАТОСТ НА РАБОТАТА

Чл.39. 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. служителите включени в звено, отговарящо за мрежовата и информационната сигурност, започват процедура по поэтапно спиране на устройствата за съхранение на данни.

4. 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.



5. При промяна местоположението на ИКТ инфраструктурата, същото да става със следната процедура:

- Издаване на протокол от РНИКТ, съдържащ списък с елементите на ИКТ инфраструктурата, които да бъде преместени, както и местоположението /от и към/ което става промяната.
- Подпис за съгласие от директора.

РАЗДЕЛ VIII. ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

1. Ръководителите и служителите в НПГ „Димитър Талев“ гр. Гоце Делчев са длъжни да познават и спазват разпоредбите на тези правила.
2. Контролът по спазване на правилата се осъществява от ръководството на НПГ „Димитър Талев“ гр. Гоце Делчев
3. Настоящите вътрешни правила се разглеждат и оценяват периодично с оглед ефективността й, като НПГ „Димитър Талев“ гр. Гоце Делчев, 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 **заповедта** на Директора на НПГ „Димитър Талев“ гр. Гоце Делчев.