



**ПРОФЕСИОНАЛНА ГИМНАЗИЯ ПО ПОДЕМНА, СТРОИТЕЛНА И  
ТРАНСПОРТНА ТЕХНИКА „Г. С. РАКОВСКИ” – ПЛЕВЕН**

---

**УТВЪРДЕНА**

**със заповед № РД-16-769/09.09.2024г.**

**на Директора на ПГПСТТ „Г.С.Раковски“ - Плевен**

**ПОЛИТИКА  
ЗА МРЕЖОВА И  
ИНФОРМАЦИОННА СИГУРНОСТ  
НА ПГПСТТ „Г. С. РАКОВСКИ“ – ПЛЕВЕН**

2024 година

## Раздел I ОБЩИ ПОЛОЖЕНИЯ

Чл.1. Настоящата политика за мрежова и информационна сигурност се утвърждава 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 има за цел осигуряването на мрежова и информационна сигурност в ПГПСТТ „Г. С. Раковски“. 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. Мрежовата и информационна сигурност се осигурява чрез мерки, пропорционални на рисковете за постигането на основните цели:

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

Чл.3. Мерки, които ПГПСТТ „Г. С. Раковски“ прилага във връзка с осигуряването на мрежова и информационна сигурност са насочени към запазване на достъпността, интегритета (цялост и наличност) и конфиденциалността на информацията по време на целия ѝ жизнен цикъл, включващ създаването, обработването, съхранението, пренасянето и унищожението ѝ в и чрез информационните и комуникационните системи на ПГПСТТ „Г. С. Раковски“.

Чл.4. (1) В ПГПСТТ „Г. С. Раковски“ за мрежовата и информационната сигурност е отговорно оторизираното от Директора звено на ПГПСТТ „Г. С. Раковски“, като:

1. С оглед на спазването на всички изисквания, звеното е на пряко подчинение на Директора на ПГПСТТ „Г. С. Раковски“ и пряко го информира за състоянието и проблемите в мрежовата и информационната сигурност;
2. Препоръчителни функции на звеното, отговарящо за мрежовата и информационната сигурност, са описани в приложение № 6 от Наредбата за минималните изисквания за мрежова и информационна сигурност (Наредбата).

Чл.5. Настоящата политика се преразглежда редовно, но не по-рядко от веднъж годишно, и при необходимост се актуализира.

Чл.6. 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.7. На служителите на ПГПСТТ „Г. С. Раковски“ 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.8. (1) Всеки служител на ПГПСТТ „Г. С. Раковски“ 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.

(2) 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.9. При разработването на нови информационни и комуникационни системи от

ПГПСТТ „Г. С. Раковски“ се спазват всички изисквания на Наредбата така, че те да представляват компоненти с възможност за интеграция в единна потребителска среда.

Чл.10. (1) С цел да се намалят 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, ПГПСТТ „Г. С. Раковски“ поддържа следната документация:

1. Опис на информационните активи – поддържа се актуален в регистъра на информационните ресурси на ПГПСТТ „Г. С. Раковски“;
2. Физическа схема на свързаност;
3. Логическа схема на информационните потоци;
4. Документация на структурната кабелна система;
5. Техническа, експлоатационна и потребителска документация на информационните и комуникационните системи и техните компоненти;
6. Инструкции/вътрешни правила за всяка дейност, свързана с администрирането, експлоатацията и поддръжката на хардуер и софтуер;
7. Вътрешни правила за служителите, указващи правата и задълженията им като потребители на услугите, предоставяни чрез информационните и комуникационните системи, като използване на персонални компютри, достъп до ресурсите на мрежата, генериране и съхранение на паролите, достъп до интернет, работа с електронна поща, системи за изработване на документи и други вътрешноведомствени системи, принтиране, използване на сменяеми носители на информация в електронен вид, използване на преносими записващи устройства и т. н.

(2) Документацията по ал. 1 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. Одобрена от Директора на ПГПСТТ „Г. С. Раковски“ или от упълномощено от него лице;
4. Класифицирана по смисъла на чл. 6 от Наредбата за минималните изисквания за мрежова и информационна сигурност;
5. Достъпна само до тези лица, които е необходимо да я ползват при изпълнение на служебните си задължения.

(3) ПГПСТТ „Г. С. Раковски“ поддържа информация, доказваща по неоспорим начин изпълнението на изискванията на Наредбата. Същата се поддържа в актуално състояние и е достъпна само за:

- а) тези лица, които е необходимо да я ползват при изпълнение на служебните си задължения по силата на трудови, служебни или договорни отношения;
- б) представители на съответните национални компетентни органи съгласно чл. 16, ал. 5 от Закона за киберсигурност;
- в) други организации, оправомощени с нормативен акт или договорни отношения.

Чл.11. При установяване на взаимоотношения с доставчици на стоки и услуги, които са "трети страни", ПГПСТТ „Г. С. Раковски“ договаря изисквания за мрежова и информационна сигурност, включително:

1. за сигурност на информацията, свързани с достъпа на представители на трети страни до информация и активите на ПГПСТТ „Г. С. Раковски“;
2. за доказване, че третата страна също прилага адекватни мерки за мрежова и информационна сигурност, включително клаузи за доказването на прилагането на тези мерки чрез документи и/или провеждане на одити;

3. за прозрачност на веригата на доставките; третата страна трябва да е способна да докаже произхода на предлагания ресурс/услуга и неговата сигурност;
  4. последици при неспазване на изискванията за сигурност на информацията;
  5. отговорност при неспазване на договорените срокове, количество и/или качество на услугата, което може да създаде риск за постигане на целите на мрежовата и информационната сигурност;
  6. за взаимодействие в случай на възникване на инцидент, който най-малко включва: контактни точки, начин за докладване, време за реакция, време за възстановяване на работата, условия за затваряне на инцидент.
- (2) ПГПСТТ „Г. С. Раковски“ определя служител или служители, отговарящи за спазване на изискванията по ал. 1 и параметрите на нивото на обслужване.
- (3) ПГПСТТ „Г. С. Раковски“ изготвя план за действие в случай на неспазване на уговорените дейности и клаузи с третата страна.

Чл.12. С цел повишаване на квалификацията на служителите и на осведомеността им по отношение на мрежовата и информационната сигурност, настоящата политика е сведена до знанието им.

Чл.13. Потребителите на информационни системи в ПГПСТТ „Г. С. Раковски“ са задължени с отговорни действия да гарантират ефективното и ефикасно използване на системите.

Чл.14. (1) ПГПСТТ „Г. С. Раковски“ извършва анализ и оценка на риска за мрежовата и информационната сигурност 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, влизащи в обхвата на Наредбата за минималните изисквания за мрежова и информационна сигурност.

(2) Анализът и оценката на риска са документиран процес по смисъла на чл. 5, ал. 1, т. 6 от Наредбата. В него са регламентирани нивата на неприемливия риск и отговорностите на лицата, участващи в отделните етапи на процеса.

(3) Анализът и оценката на риска се извършват по методика, гарантираща съизмерими, относително обективни и повтарящи се резултати. Методиката се одобрява от Директора на ПГПСТТ „Г. С. Раковски“ и е достъпна за лицата, на които е възложено да участват в процеса. Може да се прилага препоръчителна методика съгласно приложение № 3 от Наредбата.

(4) На основание на анализа и оценката на риска ПГПСТТ „Г. С. Раковски“ изготвя план за намаляване на неприемливите рискове, който включва минимум:

1. Подходящи и пропорционални мерки за смекчаване на неприемливите рискове;
2. Необходими ресурси за изпълнение на тези мерки;
3. Срок за прилагане на мерките;
4. Отговорни лица.

## **Раздел II**

### **АНАЛИЗ И ОЦЕНКА НА РИСКА ЗА СИГУРНОСТТА НА ИНФОРМАЦИОННИТЕ И КОМУНИКАЦИОННИТЕ СИСТЕМИ**

Чл.15. Управлението на риска за сигурността на информационните и комуникационните системи е част от политиката за управлението на мрежовата и информационната сигурност в ПГПСТТ „Г. С. Раковски“. По своята същност управлението на риска представлява съвкупност от процеси за идентифициране на потенциалните заплахи към

носителите на информация и активите, участващи в предоставянето на електронни услуги, анализ и оценка на рисковете, породени от тези заплахи.

Чл.16. Основните понятия, част от процеса по управление на риска са както следва:

1. Конфиденциалност – свойство на информацията да не е предоставена или разкрита на неоторизирани лица (т. 2.12 ISO/IEC 27000).
2. Интегритет – качество на информацията за точност и пълнота (т. 2.40 ISO/IEC 27000).
3. Наличност на информация – качество да бъде достъпна и използваема при поискване от оторизирано лице (т. 2.9 ISO/IEC 27000).

Чл.17. Цел на процеса за управление на риска е ПГПСТТ „Г. С. Раковски“ да минимизира загубите от потенциални нежелани събития, настъпили в резултат от реализиране на заплахи към сигурността на мрежите и информационните системи, които биха засегнали конфиденциалността, интегритета и достъпността на информацията, създавана, обработвана, предавана и унищожавана чрез тях в ПГПСТТ „Г. С. Раковски“.

Чл.18. Методиката за управление на риска има за цел да даде общ подход при анализа и оценката на риска за сигурността на информационните и комуникационните системи, предоставяни от ПГПСТТ „Г. С. Раковски“, с цел получаване на съизмерими, относително обективни и повтарящи се резултати чрез:

1. Регламентиране на дейностите и тяхната последователност при анализа и оценката на риска за електронните услуги;
2. Определяне на критериите;
3. Определяне на приоритетите на риска.

Чл.19. Анализът и оценката на риска са част от процеса за управлението му в ПГПСТТ „Г. С. Раковски“ и се обосновават на познаване на всички компоненти, имащи отношение към целите.

Чл.20. За целите на управлението на сигурността на мрежите и информационните системи е необходимо да се:

1. Познават всички обекти и субекти, които участват пряко или косвено в дейностите, попадащи в обхвата на Наредбата (информационни и комуникационни системи с прилежащия им хардуер, софтуер и документация; поддържащите ги системи (електрозахранващи, климатизиращи и др.); оперативни процеси/дейности; служители и външни организации, наричани за краткост "информационни активи";
2. Идентифицират и анализират всички потенциални нежелани събития с тях, наричани за краткост "заплахи", които биха довели до загуба на конфиденциалност, интегритет и достъпност на електронните услуги и/или информацията в тях;
3. оценява вероятността от настъпване на тези събития, като се вземат предвид слабостите (уязвимости) на информационните активи и мерките, които са предприети за справяне с тях;
4. Оценява въздействието (загуби на ресурси, време, хора и пари), неспазване на нормативни и регулаторни изисквания, накърняване на имидж, неизпълнение на стратегически и оперативни цели и др., от евентуално настъпване на тези нежелани събития въпреки предприетите мерки;
5. Оценява рискът за сигурността;
6. Набелязват мерки за смекчаване на рисковете с висок приоритет.

Чл.21. При анализ и оценка на риска ПГПСТТ „Г. С. Раковски“ използва регистър на рисковете (риск-регистър).

Чл.22. В риск-регистъра се нанасят всички информационни активи, имащи отношение

към обхвата на Наредбата:

1. информационни системи;
2. хардуерни устройства, с които са реализирани информационните системи;
3. софтуери, с които са реализирани информационните системи;
4. бази данни, включително лични данни по смисъла на GDPR;
5. записи за събитията (логове, журнали) на информационните системи;
6. документация на информационните системи (експлоатационна и потребителска);
7. комуникационни системи;
8. хардуерни устройства, с които са реализирани комуникационните системи;
9. фърмуерът на тези устройства;
10. софтуери на комуникационните системи;
11. записи за събитията (логове, журнали);
12. документация (експлоатационна и потребителска);
13. поддържащи системи (електрозахранващи, климатични);
14. системи за контрол на физическия достъп и на околната среда;
15. процеси/дейности, свързани с управлението, експлоатацията и поддръжката на информационните и комуникационните системи;
16. документация на тези процеси и дейности;
17. служители, имащи отговорности към управлението, експлоатацията и поддръжката на информационните и комуникационните системи;
18. външни организации, имащи отношение към управлението, експлоатацията и поддръжката на информационните и комуникационните системи;

Чл.23. (1) За всеки от информационните активи в риск-регистъра на ПГПСТТ „Г. С. Раковски“ се нанасят заплахите/нежеланите събития, които биха довели до нарушаване на конфиденциалността, интегритета и достъпността на информацията.

(2) ПГПСТТ „Г. С. Раковски“ отчита всички потенциални заплахи, произтичащи вътре или извън администрацията, настъпили случайно или преднамерено, като се има предвид уязвимостта на информационния актив към съответната заплаха.

Чл.24. В риск-регистъра на ПГПСТТ „Г. С. Раковски“ за всяка заплаха се вписва какви мерки са предприети срещу нея.

Чл.25. В риск-регистъра за всяка заплаха се вписва оценката за нейното въздействие – щетите (материални и нематериални), които може да причини, ако се реализира. За оценка на въздействието се използва петстепенна скала от 1 до 5, като при 1 щетите са незначителни, а при 5 са най-големи.

Чл.26 (1) Определя се вероятността за възникване на дадена заплаха, като се вземат предвид предприетите вече мерки. Колкото повече са предприетите защитни мерки, толкова по-ниска е вероятността от възникване на заплахата. При оценка на вероятността се вземат предвид следните фактори:

1. за реализиране на преднамерени заплахи: ниво на необходимите умения, леснота на достъпа, стимул и необходим ресурс;
2. за реализиране на случайни заплахи: година на производство на хардуера и софтуера, ниво на поддръжката им, квалификация на поддържащия персонал, ресорно обезпечаване на експлоатационните процеси, контрол върху тях и др.

(2) В риск-регистъра за всяка заплаха се нанася оценката за нейното въздействие.

Чл.27. За оценка на въздействието се използва петстепенна скала от 1 до 5 и като се има предвид определен период, например една година:

1. вероятността от реализирането на заплахата е под 10 %;
2. вероятността от реализиране на заплахата е от 10 % до 30 %;
3. вероятността от реализиране на заплахата е от 30 % до 50 %;
4. вероятността от реализиране на заплахата е от 50 % до 70 %;
5. вероятността от реализиране на заплахата е над 70 %.

Чл.28. За получаване на оценката на риска в ПГПСТТ „Г. С. Раковски“ се използва следната формула:

(Оценка на въздействие x Оценка на вероятност) = Оценка на риска

Чл.29. С цел прилагане на пропорционални на заплахите механизми за защита в ПГПСТТ „Г. С. Раковски“ се прави приоритизация на рисковете на база на тяхната оценка и праговете, заложи в Наредбата.

Чл.30. (1) Приема се, че за рискове с приоритет 3 по смисъла на Наредбата не се изисква предприемане на допълнителни мерки за смекчаване на заплахите, които ги пораждаат.

(2) За рисковете с приоритет 2 по смисъла на Наредбата се прави анализ на възможните мерки, които биха могли да се предприемат за смекчаването им, и се преценява дали разходът на ресурси за прилагането им е пропорционален на щетите от реализиране на заплахата. В случай че щетите са повече от разходите, се определят отговорно лице и срок за прилагане на тези мерки.

(3) За всички рискове с приоритет 1 се определят отговорни лица от Директора на ПГПСТТ „Г. С. Раковски“, планират се мерки, които биха намалили риска от реализиране на конкретната заплахата, и се определят срокове за прилагането им.

Чл.31. (1) Отговорните лица за съответните рискове организират прилагането на планираните мерки за защита и наблюдават инцидентите и щетите, свързани с тях. При необходимост инициират нов анализ и оценка на риска за тази заплахата.

(2) Директорът на ПГПСТТ „Г. С. Раковски“ организира периодично, но не по-малко от веднъж в годината, анализ и оценка на риска, както и при всяко изменение в информационната и/или комуникационната инфраструктура промяна на административната структура и функциите.

### **Раздел III**

#### **ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ**

§1. Ръководството и служителите в ПГПСТТ „Г. С. Раковски“ са длъжни да познават и спазват разпоредбите на настоящата Политика.

§2. Контролът по спазване на приетата Политика се осъществява от оторизираното звено за гарантиране на мрежовата и информационната сигурност на използваните информационни системи в ПГПСТТ „Г. С. Раковски“.

§3. Настоящата Политика за мрежова и информационна сигурност се разглежда и оценява периодично с оглед ефективността ѝ, като ПГПСТТ „Г. С. Раковски“ може да приема и прилага допълнителни мерки и процедури, които са целесъобразни и необходими с оглед защитата на информацията.

§4. Тази Политика е разработена съгласно Наредба за минималните изисквания за мрежова и информационна сигурност и е утвърдена със заповед на Директора на ПГПСТТ „Г. С. Раковски“ № РД-16-769/09.09.2024г.