ПОЛИТИКА ЗА МРЕЖОВА И ЗА ИНФОРМАЦИОННА СИГУРНОСТ

НА ДГ №140 „ЗОРНИЦА“

РАЗДЕЛ ПЪРВИ
ОБЩИ ПОЛОЖЕНИЯ

Чл. 1. (1) Настоящата политика цели да регламентира и осигури : правила и процедури за използване на информационните системи и активи ,както и мрежова и информационната сигурност на ДГ №140 „Зорница“.

1. от страна на служителите ;
2. запазване на конфиденциалността на информацията чрез осигуряване на мерки за защита от неправомерно придобиване, неправомерно модифициране, унищожаване или загубване;
3. развитие и поддържане на сигурни и надеждни информационни системи, осигуряващи цялост и достъпност на информацията;
4. мерки за реакция в случай на злоупотреба, загуба или неупълномощено придобиване на информация, както и при бедствия, и аварии;
5. осигуряване на непрекъснатост на работните процеси;
6. информиране на педагогическия и непедагогическия персонал и на други лица, имащи достъп до информационните системи и активи на ДГ №140 „Зорница“ за техните отговорности и задължения;

(2) Политиката обхваща:

1. информационните системи на образователната институция;
2. информацията, съдържаща се в системите;
3. потребителите на информацията.

(3) Политиката на мрежова и информационна сигурност в ДГ №140 „Зорница“ не налага ограничения, противоречащи на установената култура на откритост и доверие в институцията.

(4) Целта на описаните в политиката контроли е да защитават служителите на образователната институция, потребителите, децата , както и външните заинтересовани страни, имащи отношения с институцията, от незаконни и увреждащи действия, извършени предумишлено или несъзнателно.

Чл. 2. Информационните системи и активи включват:

1. информацията, създавана и използвана от образователната институция:
2. бази данни;
3. сървъри, компютри, мобилни устройства, комуникационни устройства, устройства за копиране и всякакви периферни устройства;
4. WEB базирани и други информационни системи и софтуерни активи (програми), в това число операционни системи, вътрешна и интернет страница, имейли и др

5. локална мрежа и инфраструктура (окабеляване, захранване и др.);
6. носители на информация (дискови масиви, дискове, USB памети и др.).

Чл. 3. При управление на сигурността на информацията, образователната институция прилага стандарт БДС EN ISO/IEC 27001 – Информационни технологии – Методи за сигурност – Системи за управление на сигурността на информацията – Изисквания.

Чл.4.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. Мерките, които ДГ № 140“Зорница” 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 и жизнен цикъл, включващ създаването, обработването, съхранението, пренасянето и унищожението и в и чрез информационните и комуникационните системи на детската градина.

РАЗДЕЛ ВТОРИ
ОТГОВОРНОСТИ

Чл. 4. В Детска градина №140“Зорница“ се прилага и спазва принципът на разпределение на задълженията и отговорностите като средство за намаляване на риска от случайна или умишлена злоупотреба с информационните системи и активи.

Чл. 5. (1) Директорът на ДГ №140“Зорница“ е отговорно лице за осигуряване на мрежовата и информационна сигурност

1. утвърждава настоящата политика и свързаните с нея документи, както и промените в тях;
2. разпределя правата за използване на информационните системи и ролите и отговорностите, свързани с опазване на информационните активи и сигурността на информацията;
3. координира прилагането на мерки за осигуряване на информационна сигурност;
4. оценява потребностите и планира необходимите ресурси за осигуряване на информационната сигурност;
5. утвърждава план за осигуряване непрекъснатостта на дейността и планове за обучение на служителите на институцията, във връзка с използването на информационните системи и активи и информационната сигурност.

(2) Директорът на образователната институция проследява и осигурява актуалността на настоящата политика и свързаните с нея документи.

(3) Директорът на образователната институция отговаря за подходящото оповестяване на актуалната версия на настоящата политика и свързаните с нея

документи. Той отговаря служителите на ДГ №140 „Зорница“ да бъдат подходящо инструктирани и мотивирани за изпълнение изискванията на политиката.

.

Чл. 6. Специалистът по информационни технологии/системният администратор отговаря за:

1. управление и поддържане на информационните системи и активи на ДГ №140 „Зорница“ и предоставяне на нужните нива на достъп;
2. архивиране на данни и информация;
3. осигуряване на защита от злонамерен софтуер;
4. мониторинг на уязвимости и инциденти;
5. изготвяне на нужната документация, свързана с администрирането на информационната система и активи.

Чл.7. 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. 8. (1) Потребителите на информационните системи в ДГ №140 „Зорница“, са задължени да следват правилата, инструкциите и заповедите, свързани с използването на информационни системи и активи и с информационната сигурност.

(2) Потребителите са длъжни да докладват за проблеми и инциденти с информационните системи и активи.

(3) Под потребители на информационни системи в настоящата политика се разбират всички лица, които имат достъп до системите по силата на своите служебни или договорни отношения, както и всички учащи, ползващи информационните системи на институцията.

(4) Педагогическите специалисти и непедагогическият персонал използват информационните системи и активи в ДГ №140 „Зорница“,с цел увеличаване на продуктивността и ефективността на работата.

(5) Всички потребители се запознават с тези части от настоящата политика и свързаните с нея документи, които отговарят на техните роли и отговорности. Потребителите потвърждават, че са запознати и че разбират задълженията си по тези документи.

(6) Правата и задълженията на потребителите и служителите на ДГ №140“Зорница“ по отношение на информационните системи и активи и информационната сигурност в образователната институция, се определят в съответствие с настоящата политика, в правила, заповеди или в длъжностните им характеристики.

РАЗДЕЛ ТРЕТИ

ИНФОРМАЦИОННА СИГУРНОСТ И ЧОВЕШКИ РЕСУРСИ

Чл. 8. При необходимост, е възможно правата и достъпът до информационните

системи и активи на служители, лица, с които институцията е сключила договор, и на учащите, да се продължат и за определен период след края на договора/напускане на образователната институция. В този случай лицето подписва декларация за конфиденциалност.

Чл. 9. При напускане на специалиста по информационни технологии или при прекратяване на договора с него, знанията за информационните системи и активи и за информационната сигурност на ДГ №140"Зорница" се документират по подходящ начин и се предават на образователната институция.

Чл.9.Всеки служител има лична парола и персонална идентификация, която не предоставя за използване от други лица и е достатъчно защитена .

Чл.10. На служителите на ДГ № 140 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.11 При извършване на работа от разстояние служителите на ДГ № 140 спазват всички изисквания за осигуряване защитата на данните, в т.ч. лични данни на трети лица и/или по класификацията на информацията

Чл.12.При съмнение за нарушение на сигурността на личните данни, лицето, което е установило несъответствието (случайно или неправомерно унищожаване на лични данни, загуба, промяна, неразрешено разкриване или нерегламентиран достъп, незабавно уведомява директора

РАЗДЕЛ ЧЕТВЪРТИ

ИЗПОЛЗВАНЕ И УПРАВЛЕНИЕ НА ИНФОРМАЦИОННИТЕ СИСТЕМИ И АКТИВИ

Чл. 31. (1) Информационните системи и активи на ДГ №140"Зорница", в това число вътрешната мрежа (интранет), интернет, компютърното оборудване, операционните системи, приложният софтуер, електронната поща и други, описани в чл. 2 на настоящата политика, са собственост на образователната институция.

(2) Данните и информацията, които служителите и потребителите обработват и съхраняват при изпълнение на служебните си задължения или в рамките на учебния процес чрез използване на информационните системи на ДГ №140"Зорница", са собственост на образователната институция.

(3) Информационните системи и активи на образователната институция са предназначени да се използват единствено за постигане на целите и в интерес на образователната институция.

(4) Образователната институция поддържа пълен списък на информационните си системи и активи.

Чл. 14. (1) Работниците/служителите в институцията нямат право да вземат програмни продукти с цел инсталацията им на домашните им компютри и преносими устройства, с изключение на електронни учебници/познавателни книжки и създадените

за он-лайн обучение софтуери.

(2) Изключения от разпоредбата на ал. 1 са допустими при изрично разрешение на директора на институцията и за целите на работния или образователния процес.

Чл. 15. При напускане на институцията, работниците/служителите нямат право да копират или унищожават файлове с данни, които са създадени във връзка с тяхната работа.

Чл. 16. (1) Забранява се ползването на информационните системи и активи на образователната институция в следните случаи:

1. Заобикаляне на системите за сигурност, с цел разрушаване или намаляване сигурността на учебната локална мрежа или бази данни.
2. Ползване на информационните системи за извършване на престъпление.
3. За подпомагане дейността на частни лица, в това число търговски дружества, техните продукти, услуги или бизнес практика.
4. Електронната поща на институцията не може да се ползва за комерсиални лични цели, религиозни цели или да се подпомага бизнес, който не е свързан с дейността на образователната институция.
5. За политическа дейност, която пряко или косвено би подпомогнала кампанията за избиране на даден кандидат.
6. Подправяне на електронна поща с цел скриване на самоличността на подателя или фалшифициране на тази самоличност. Всички електронни писма, пращани от персонала трябва да са лично подписани.
7. Свалянето от интернет на аудио и видео файлове.
8. Сваляне и инсталиране на компютърни програми от интернет без разрешение на компютърните специалисти.
9. Копиране на лицензираните компютърни програми на институцията с цел лична употреба.

(2) Този списък на забранените дейности във връзка с информационните технологии не е изчерпателен и към него може да се добавят допълнителни забрани със заповед на директора.

Чл. 17 (1) Неоторизираното разкриване на служебна информация може да доведе до негативни последици за образователната институция и накърняване на нейния имидж и репутация.

(2) Работник/служител, който е копирал и използвал информация от локалната мрежа на институцията за лична изгода или за да причини вреда на институцията, носи съответната дисциплинарна и имуществена отговорност по Кодекса на труда.

Чл. 18 (1) Ръководството насърчава ползването на интернет от работниците/служителите за обмяна на информация, извършване на проучвания и събиране на данни във връзка с дейността им.

(2) Заместник-директорите и други оторизирани длъжностни лица отговарят за уместната употреба на интернет от персонала.

Чл. 19. Всички електронни писма и важни съобщения, които имат отношение към дейността на образователната институция, трябва да се принтират и представят за завеждане с входящ номер в Дневника за входяща кореспонденция от определеното

длъжностно лице, като екземпляр се съхранява в съответния класьор и в електронната поща.

РАЗДЕЛ ПЕТИ

КОНТРОЛ ВЪРХУ РАБОТАТА С ИНФОРМАЦИОННИТЕ СИСТЕМИ И АКТИВИ

Чл. 20. (1) Ръководството на институцията има право да контролира ползването на програмните продукти, електронната поща, интернет и базите данни, създадени от педагогическите специалисти и непедагогическия персонал в образователната институция.

(2) Ръководството на образователната институция има право да проверява изцяло служебните компютри, предоставени за учебни цели на персонала в институцията, както и техниката, която ползват учители и служители във връзка с изпълнение на служебните им задължения.

(3) Служителите и потребителите са наясно, че работата и използването на информационните системи и активи подлежи на непрекъснато наблюдение.

(4) Образователната институция има право да деинсталира всякакъв софтуер или файлове, които не са свързани със служебните задължения на потребителя или с учебния процес, като (но не само) игри, музикални файлове, изображения, видеоклипове, споделени и безплатни програми, и др.

(5) Служителите и потребителите, имащи достъп до информационните системи, спазват политика за чисто бюро, чист екран и защита на ненадзиравани устройства.

(6) Служителите и потребителите прилагат изключително внимание при работа с информационните системи, в това число работа в интернет и работа с електронна поща, за да се предпазят от вируси, троянски коне и друг злонамерен софтуер.

Чл. 21. Резултатите от извършения контрол върху работата с информационните системи и активи на образователната институция се считат за конфиденциални и не се разгласяват от ръководството.

РАЗДЕЛ ШЕСТИ

ЗАЩИТА НА ИНТЕЛЕКТУАЛНА СОБСТВЕНОСТ

Чл. 22. (1) При придобиване на софтуерни продукти, за целите на образователната институция, се гарантира, че са налице ясни договорни клаузи относно правата за интелектуалната им собственост;

(2) При разработване на нови или промяна на съществуващи софтуерни продукти за целите на образователната институция, в договорите за разработка се включват ясни клаузи, гарантиращи, че правата за интелектуалната собственост остават за институцията;

(3) Образователната институция инсталира и използва само лицензирани продукти, като адекватно преценява и осигурява срока, броя потребители и др. Ръководството на образователната институция и специалистът по информационни технологии осъществяват проверки за целта.

РАЗДЕЛ СЕДМИ

ФИЗИЧЕСКА СИГУРНОСТ

Чл. 23. Информационните системи и оборудването на ДГ 140“Зорница“, в това

число копирни машини, факсове и мрежови принтери, се защитават физически от заплахи за сигурността и влияние на рискове от околната среда, с цел предотвратяване на загуби, щети или излагане на риск на активи и затрудняване или прекратяване на дейността на институцията.

Мерките за физическа защита не трябва да възпрепятстват и затрудняват служебния и учебния процес.

Чл. 24. Изнасянето извън сградите на институцията на информационни активи принадлежащи на институцията се извършва с разрешение от директора или оправомощено лице.

Чл. 25. Служебна информация не се оставя без надзор или контрол, което означава видима на екран.

Чл. 26. Физическият достъп на външни лица, в това число и на служителите, до информационните системи и активи на институцията се извършва от и/или в присъствие на служители на образователната институция.

РАЗДЕЛ ОСМИ

КОНТРОЛ НА ДОСТЪПА, УПРАВЛЕНИЕ НА ИНЦИДЕНТИ И ЗАЩИТА ОТ ЗЛОНАМЕРЕН СОФТУЕР

Чл. 27. (1) Достъпът до информационните системи и активи на институцията е индивидуален и се осъществява на база персонален потребителски профил.

(2) Персоналният потребителски профил съдържа следните данни:

1. лични данни;
2. потребителско име и парола;
3. права за достъп.

Чл. 28. (1) Паролите следва да съдържат малки и големи букви, цифри и специални символи, дължината им трябва да е не по-малко от 8 символа за потребителските и 12 символа за администраторските профили.

(2) Паролите на потребителските профили трябва да се сменят регулярно на период не по-голям от шест месеца.

(3) Паролите на административните профили трябва да се сменят регулярно на период не по-голям от три месеца.

(4) Потребителите трябва да пазят своите лични пароли в тайна.

Чл. 29. Правата за достъп са две основни групи – потребителски и административни. Администраторски права на достъп се определят със заповед на директора на институцията.

Чл. 30. При настройка на информационните системи на институцията се препоръчва да се прилага следният подход:

1. след 3 (три) неуспешни опита за влизане в системата, съответният профил се „заключва“. Отключването на профила се извършва от администратора, след изясняване на причините за заключването.
2. определя се максималното време на сесия без активност от страна на потребителя, след което профилът автоматично излиза от системата.

Чл. 31. (1) Информационните системи на ДГ 140“Зорница“осигуряват записи на действията на потребителите и на други събития (инциденти), свързани със сигурността на информацията.

(2) Записите се осъществяват във файлове за регистрация (log–files) на системно и приложно ниво. Файловете са защитени от манипулации на потребители и са достъпни само за упълномощени от директор на институцията лица и се съхраняват за определен период от време.

(3) Лицето с администраторски права не трябва да има възможност да изтрива или деактивира записи на свои собствени действия.

Чл. 32. (1) Информационните системи и активи на ДГ 140"Зорница" трябва да бъдат надеждно защитени от проникване на злонамерен код (напр. вируси), хакерски атаки и др. Подобно проникване може да се осъществи както през Интернет, така и от неправилно използване на преносими информационни носители (дискове, външна памет и др.).

(2) Специалистът по информационни технологии на институцията отговаря за поддържане на системите за защита от злонамерен код. За целта се използват като минимум:

1. системи за защита;
2. софтуер за откриване на вируси, сканиращ както входящия трафик към външни (интернет) страници и платформи на институцията, така и към потребителските персонални компютри използвани в институцията.

Чл. 33. (1) Специалистът по информационни технологии на образователната институция носи пълната отговорност за избирането и инсталирането на антивирусната програма, както и за нейната актуализация на всеки индивидуален компютър. Служителите също трябва да следят дали тяхната антивирусна програма се осъвременява периодично с най-новата версия.

(2) Потребителите на информационните системи на институцията трябва да приемат всяко съобщение за злонамерен софтуер или друго злонамерено събитие изключително сериозно и да следват вътрешните процедури за реакция в такъв случай.

(3) Преднамереното разпространяване на данни, за които потребителят знае, че са заразени с вирус е нарушение на служебните задължения, което се санкционира по дисциплинарен ред.

(4) В случай на злонамерена атака потребителят трябва незабавно да информира специалиста по информационни технологии, без да предприема никакви действия самостоятелно.

Чл.34. 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.

Чл.35. При съмнение за възникнал проблем при работа с програмен продукт , незабавно се уведомява експертът по Информационно осигуряване в РУО-София , екипът на АдминСофт , ръководител на проект „Програмни продукти за детски заведения" , съответните оторизирани фирми , разработили програмния продукти.

Чл.36. Използването на внесени отвън информационни носители(оптични дискове, дискети, 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;

Чл.37. Инсталирането на софтуерни програми ,не съответсващи към пряката служебна работа е ЗАБРАНЕНО

(5) Входящата електронна поща трябва да се третира с особено внимание поради потенциалната възможност да е заразена със злонамерен софтуер. Отварянето на

приложения да се прави само след предварителното им сканиране с антивирусна програма.

(6) Ползването на външни носители (дискове, външна памет и др.) на информация е допустимо само след предварителното им сканиране с антивирусна програма.

Чл. 38. (1) ДГ №140"Зорница"събира и анализира данни за вида и броя на инцидентите, свързани със сигурността на информацията. Въз основа на анализа се прави преценка на разходите за защита. Също така, въз основа на анализа се идентифицират повтарящи се инциденти или инцидентите с голямо влияние и на тази база се оптимизират мерките за защита.

Чл.39. Достъпът до Интернет става чрез инсталирани на персоналните компютри браузър

Чл.40. Не се разрешава използването на Интернет връзката за гледане на видео или филми от служителите, което значително намаляват скоростта на връзката на другите служители.

Чл.41. Правилата за достъп на служителите до Интернет включват следните задължителни изисквания:

1.Не се толерира влизането в Интернет - сайтове с неизвестно съдържание;

2.Използването на чат - програми е единствено и само за служебна цел;

3.Не се разрешава инсталирането на други чат-програми, освен Skype;

4.Не се разрешава тегленето на файлове с неизвестно съдържание от Интернет.

5.Ползването (отварянето) на изтеглени файлове от Интернет пространството (сайтове, лични пощи, форуми, чат-програми и др.) във връзка с изпълнение на служебните задължения, става при условие, че първо те се сканират за наличието на вируси.

Ако антивирусният софтуер намери такива, файловете се изтриват незабавно;

Чл.42. Достъпът до електронна поща на ДГ № 140 „Зорница"-dg140@abv.bg се осъществява от директора ,а гл.счетоводител, касиер-домакини имат служебна електронн поща

1.Постъпилата информация по ел. поща , касаеща дейността на, гл.счетоводител ,ЗАС / писма ,справки НАП , съобщение РМС , фактури , извлечения ЦКБ , информация за банкови преводи , искания за справки и др. / се препраща към техните лични служебни имейли

2.Съобщения , изпратени от ел. поща на ДГ – dg140@abv.bg - са законосъобразни и подлежат на изпълнени

3.Всяко съобщение , което ЗД ,главен счетоводител , ЗАС изпращат в изпълнение на отговорности от техните служебни ел.адреси , е подписано от тях с имена и длъжност .

4.При отсъствие на директора , в заповедта се конкретизира длъжностно лице , на което е даден достъп до ел. поща на ДГ №140"Зорница"

Чл.42. Правилата за достъп и използването на електронната поща, включват следните задължителни изисквания:

1.Служителите не трябва да отварят съобщения, получени от неизвестен получател или неизвестна Интернет страница. Такива съобщения се изтриват незабавно;

2.Прикачените файлове към съобщенията, получени в служебните пощи ,не се отварят при съмнение за вируси

Чл.43. Служителите преместват важната информация от получените съобщения в отделни файлове върху техните компютри.

Информацията от извършваните по предходната алинея анализи се взема

предвид в процеса по управление на риска в организацията.

Чл. 44. При работа от разстояние и необходимост от достъп до информационните системи на образователната институция дистанционно – извън вътрешната мрежа:

1. се използва двуфакторна автентикация на достъп;
2. се използват само канали с висока степен на защита като Virtual Private Network (VPN);

РАЗДЕЛ ДЕВЕТИ

ПОДДЪРЖАНЕ НА ПЪЛНОТАТА, ИНТЕГРИТЕТА И КОНФИДЕНЦИАЛНОСТТА НА ИНФОРМАЦИЯТА

Чл. 45. (1) Основна отговорност за достоверността, актуалността и пълнотата на информацията, носят служителите, които имат право да я създават и записват в информационните системи на образователната институция.

(2) Промени във вече записана в информационните системи информация правят служителите, на които са дадени съответните права за това.

(3) В случай че вече записана в информационните системи информация е затворена за редактиране през стандартния потребителски интерфейс, промените се извършват само след писмено разрешение на директора на образователната институция и след като специалистът по информационните технологии „отключи" възможността за редактиране.

(4) Конфиденциалността на информацията е лична отговорност на всеки, чийто профил осигурява достъп до нея, в съответствие с предоставените му права.

РАЗДЕЛ ДЕСЕТИ

АРХИВИРАНЕ И ВЪЗСТАНОВЯВАНЕ НА ИНФОРМАЦИЯТА

Чл. 46. (1) Сривовете в компютърното оборудване, вирусите и случайното изтриване на файлове могат да причинят загуба на данни, поради което е необходимо информацията във всяка компютърна система да бъде архивирана.

(2) Целта на архивирането е да се възстанови работата възможно най-бързо в случай на прекъсване по технически причини. По този начин се минимизират възможните проблеми и загуби.

(3) Специалистът по информационни технологии в институцията осигурява на потребителите адекватна система за архивиране на данните от тяхната работа на подходящи технически носители (дискове, USB и др.).

(4) Честотата на архивирането се определя от директора в писмена процедура и зависи от броя транзакции и тяхната значимост за системата.

(5) Задължително архив (архивиране на файлове) се прави веднъж месечно.

Чл.47. (1) Направените архивни копия се съхраняват по възможност извън основната сграда на образователната институция, в специално предназначен за целта заключен шкаф.

(2) Архивните копия се обозначават със следните данни:

1. име на информацията;
2. дата на създаване;
3. срок на съхранение;

4. име на служителя, извършил архивирането.

(3) Архивните копия се проверяват периодично за пълнота на архивираната информация и възможност за възпроизвеждането ù. Копията се проверяват поне веднъж годишно, а носители с информация от ключово значение за дейността на образователната институция – поне веднъж на 6 месеца.

Чл. 48. (1) При срив в информационните системи, специалистът по информационни технологии предприема нужните действия за възстановяване на нормалното функциониране на системите.

(2) При загуба или повреждане на информация, специалистът по информационни технологии я възстановява, като използва последното актуално архивно копие.

РАЗДЕЛ ЕДИНАДЕСЕТИ

РАЗРАБОТВАНЕ И ВНЕДРЯВАНЕ НА ИНФОРМАЦИОННИ СИСТЕМИ

Чл. 49. С цел предотвратяване на увреждане или загуба на информация или грешки в информационните системи на образователната институция, при разработени и внедряване на нови или при усъвършенстване на съществуващи информационни системи, се планират подходящи мерки, които се залагат в договорите с разработчиците.

Чл. 50. (1) За всяка информационна система се поддържат отделни една от друга среда за тестване и продукционна среда, в която системата функционира.

(2) Дейности по разработване не се извършват в тестовата и продукционна среда на системата.

(3) Не се допуска пряк достъп на разработчиците до продукционната среда.

РАЗДЕЛ ДВАНАДЕСЕТИ

ОЦЕНКА НА РИСКА

Чл. 51. (1) Като част от дейността по управление на риска, образователната институция идентифицира и оценява рисковете, свързани с използването на информационните системи и информационната сигурност.

(2) При оценката на риска се идентифицират рискове за всяка система и актив, описани в списъка по чл. 12, ал. 4 на настоящата политика.

(3) Въз основа от резултатите от оценката на риска, се прецизират и предприемат конкретните мерки, във връзка с областите на прилагане и защита на информационните технологии и информацията, описани в настоящата политика.

Чл.52. Управлението на риска за сигурността на информационните и комуникационните системи е част от политиката за управлението на мрежовата и информационната сигурност в ДГ № 140. 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.53. Основните понятия, част от процеса по управление на риска са както следва:

1. конфиденциалност – свойство на информацията да не е предоставена или разкрита неоторизирани лица (т. 2.12 ISO/IEC 27000).

2. интегритет – качество на информацията за точност и пълнота (т. 2.40 ISO/IEC 2700

наличност на информация – качество да бъде достъпна и използваема при поискване оторизирано лице (т. 2.9 ISO/IEC 27000).

Чл.54. Цел на процеса за управление на риска е ДГ № 140, да минимизира загубите потенциални нежелани събития, настъпили в резултат от реализиране на заплахи кı сигурността на мрежите и информационните системи, които биха засегна конфиденциалността, интегритета и достъпността на информацията, създава обработвана, предавана и унищожавана чрез тях в общината.

Чл.55. Методиката за управление на риска има за цел да даде общ подход при анализ оценката на риска за сигурността на информационните и комуникационните систем предоставяни от ДГ № 140, с цел получаване на съизмерими, относително обективни повтарящи се резултати чрез:

1. регламентиране на дейностите и тяхната последователност при анализа и оценката риска за електронните услуги

2. определяне на критериите;

3. определяне на приоритетите на риска.

Чл.56. Анализът и оценката на риска са част от процеса за управлението му в ДГ № 140, се обосновават на познаване на всички компоненти, имащи отношение към целите.

Чл.57. За целите на управлението на сигурността на мрежите и информационните систе е необходимо да се:

1. познават всички обекти и субекти, които участват пряко или косвено в дейности попадащи в обхвата на Наредбата (информационни и комуникационни системи прилежащия им хардуер, софтуер и документация; поддържащите ги систе (електрозахранващи, климатизиращи и др.); оперативни процеси/дейности; служители външни организации), наричани за краткост "информационни активи"; идентифицират анализират всички потенциални нежелани събития с тях, наричани за краткост "заплах които биха довели до загуба на конфиденциалност, интегритет и достъпност електронните услуги и/или информацията в тях;

2. 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;

3. 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;

4. оценява рискът за сигурността;

5. набелязват мерки за смекчаване на рисковете с висок приоритет.

Чл.58. При анализ и оценка на риска ДГ № 140 използва регистър на рисковете (риск регистър).

Чл.59. 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.60. (1) За всеки от информационните активи в риск-регистъра на ДГ № 140 се нанасят заплахите/нежеланите събития, които биха довели до нарушаване на конфиденциалността, интегритета и достъпността на информацията.

(2) ДГ № 140 „Зорница“ 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.61. В риск-регистъра на ДГ № 140, за всяка заплаха се вписва какви мерки са предприети срещу нея.

Чл.62. 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.63 (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, лесnота

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.64. 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.65. За получаване на оценката на риска в ДГ№ 140се използва следната формула:

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

Чл.65. С цел прилагане на пропорционални на заплахите механизми за защита в ДГ №140, се прави приоритизация на рисковете на база на тяхната оценка и праговете, заложени в Наредбата.

Чл.66. (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 пораждат.

(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 конкретна за всяка структура: дирекция, отдел или служител, планират се мерки, които биха намалили риска от реализиране на конкретната заплаха, и се определят срокове за прилагането им.

Чл.67. (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 заплаха.

(2) Директорът на ДГ № 140 „Зорница“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.

ДОПЪЛНИТЕЛНИ И ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

§ 1. Настоящата политика се преглежда и при необходимост се актуализира поне веднъж годишно, при промени в приложимата уредба, в средата и технологиите, в организацията и дейността на образователната институция, а също така в резултат от промяна в рисковете, застрашаващи дейността на институцията.

§ 2. Директорът на ДГ 140"Зорница"създава условия за запознаването на служителите на образователната институция и всички потребители на информационните ù системи и активи с политиката, като публикува и комуникира политиката чрез подходящи комуникационни канали и организира обучения.

§ 3. Директорът на ДГ №140"Зорница" или определено от него лице упражнява контрол по прилагане на политиката.

§ 4.Ръководителите и служителите в ДГ № 140, са длъжни да познават и спазват разпоредбите на настоящата Политика.

§ 5. Контролът по спазване на приетата Политика се осъществява от директора на ДГ№ 140"Зорница" или определеното със заповед на Директора отговорно лице за гарантиране на мрежовата и информационната сигурност на използваните информационни системи в ДГ № 140.

§ 6. Настоящата Политика за мрежова и информационна сигурност се разглежда и оценява периодично с оглед ефективността и, като ДГ№ 140, може да приема и прилага допълнителни мерки и процедури, които са целесъобразни и необходими с оглед защитата на информацията.

§ 7.Тази Политика е разработена съгласно Наредба за минималните изисквания за мрежова и информационна сигурност ие утвърдена със заповед на Директора на ДГ № 140/Заповед № ...113/19.01./.2026 г./