ДЕТСКА ГРАДИНА „ПЪРВИ ЮНИ”, ГР.КЮСТЕНДИЛ,
КВ. „ЗАПАД”, ТЕЛ: 078/55 20 73, e-mail: info-1000060@edu.mon.bg

УТВЪРЖДАВАМ:

АНЕЛИЯ СТОЙМИРОВА
Директор на ДГ „Първи юни”

Заповед № 60 /15.09.2025г.

РЪКОВОДСТВО И ПОЛИТИКИ ЗА УПРАВЛЕНИЕ НА ИНФОРМАЦИОННАТА СИГУРНОСТ

на ДГ „Първи юни”, гр. Кюстендил

СЪДЪРЖАНИЕ:

I.Политика за информационна сигурност

1. ВЪВЕДЕНИЕ

Настоящото Ръководството описва целите, обхвата, отговорностите и процедурите на Системата за управление на информационната сигурността в ДГ“Първи юни“, град Кюстенил.

ОСНОВАНИЕ

При разработване на Системата за управление на информационната сигурността се използвани изисквания, указания, насоки, термини и понятия нормативните изисквания на Закона за електронното управление (ЗЕУ) и подзаконовите нормативни актове, Закона за киберсигурност и Наредба за минималните изисквания за мрежова и информационна сигурност (НМИМИС) и на действащите международни стандарти.

Системата за управление на информационната сигурността е разработена съгласно конкретните цели на осъществяваната дейност, като са отчетени особеностите на утвърдената структура и броя на служителите в ДГ“Първи юни“, град Кюстенил

2. ОРГАНИЗАЦИОННА СТРУКТУРА

Организационната структура е дадена в Приложение 1.

Отговорностите и пълномощията на служителите по отношение на информационната сигурност в обучителната организация са регламентирани чрез:

- Длъжностни характеристики;
- Политика за мрежова и информационна сигурност;
- Политики на Системата за управление на информацията сигурност.

3. ЦЕЛИ

Целите на Система за управление на информационната сигурност включват:

- Защита на информационните активи от неоторизиран достъп, унищожаване, промяна и изтичане на информацията.
- Гарантиране на непрекъснатостта и наличността на информационните системи.
- Осигуряване на спазването на приложимите закони, регулации и стандарти за информационна сигурност.
- Поддържане на доверие в на клиенти, партньори и други заинтересовани страни в образователната институция.

4. ОБХВАТ

- Системата за управление на информационната сигурност защитава информацията, която се съдържа в образователната институция, като защитата се осъществява на всички етапи на информационния процес. Системата се прилага за всички информационни активи и

процеси, свързани с тях, включително:

- Информацията, получена, обработена и съхранена от ДГ“Първи юни“, град Кюстенил Информационните системи, включително хардуер, софтуер и мрежова инфраструктура.
- Всички служители, подизпълнители и трети лица, които имат достъп до информационните активи на образователната институция.
- Прилагането на конкретни механизми за контрол, както и изключенията е посочено в Декларацията за приложимост.

5. ОТГОВОРНОСТИ

5.1. Ангажираност на ръководството

- Установяване на политики и цели за информационната сигурност.
- Определяне на ресурсите и отговорностите за изпълнение на СУИС.
- Подкрепа и ангажимент към постоянното подобряване на информационната сигурност.

5.2. Сигурност на информацията

- Идентифициране, класифициране и установяване на мерки за защита на информационните активи.
- Изграждане и поддръжка на механизми за управление на достъпа до информационните активи.
- Изграждане и поддръжка на механизми за откриване, предотвратяване и реагиране на инциденти в информационната сигурност.

5.3. Обучение и осведоменост

- Предоставяне на обучение и осведоменост на персонала относно политиките, процедурите и практиките за информационна сигурност.
- Усъвършенстване на знанията и уменията на персонала за ефективно изпълнение на задачите си.

5.4. Система за управление на информационната сигурност включва:

- Изграждане, внедряване и поддръжка на СУИС,.
    - Преглеждане и подобряване на СУИС чрез систематични одити и прегледи.

6. ПОЛИТИКИ, ПРОЦЕДУРИ И ПРАВИЛА

Ръководството за СУИС включва редица политики, процедури и правила, които се изпълняват и включват като минимум следните основни елементи на информационната сигурност:

- Идентификация и класификация на информационните активи.

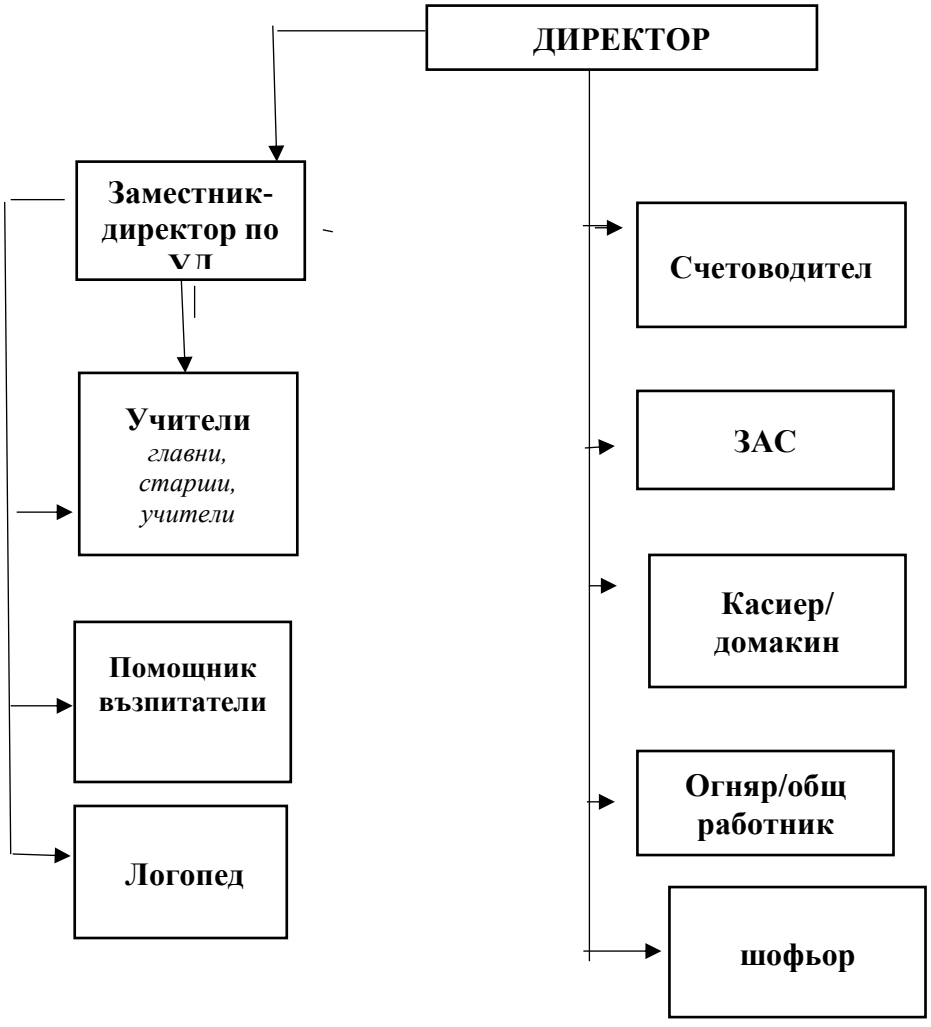
- Управление на активите.
- Управление на достъпа до информационните активи.
- Изграждане и поддръжка на политики и процедури за сигурността на информацията.
- Управление на риска в информационната сигурност.
- Управление на доставчиците.
- Управление на инциденти в информационната сигурност.
- Обучение и осведоменост на персонала.
- Преглед и подобряване на СУИС

ПРИЛОЖЕНИЕ 1.

ОРГАНИЗАЦИОННА СТРУКТУРА

НА

ДГ“Първи юни“, град Кюстенил



II.Методика за оценка на риска

7. ВЪВЕДЕНИЕ

Настоящото Ръководството описва целите, обхвата, отговорностите и процедурите на Системата за управление на информационната сигурността в ДГ“Първи юни“, град Кюстенил.

ОСНОВАНИЕ

При разработване на Системата за управление на информационната сигурността се използвани изисквания, указания, насоки, термини и понятия нормативните изисквания на Закона за електронното управление (ЗЕУ) и подзаконовите нормативни актове, Закона за киберсигурност и Наредба за минималните изисквания за мрежова и информационна сигурност (НМИМИС) и на действащите международни стандарти.

Системата за управление на информационната сигурността е разработена съгласно конкретните цели на осъществяваната дейност, като са отчетени особеностите на утвърдената структура и броя на служителите в ДГ“Първи юни“, град Кюстенил

8. ОРГАНИЗАЦИОННА СТРУКТУРА

Организационната структура е дадена в Приложение 1.

Отговорностите и пълномощията на служителите по отношение на информационната сигурност в обучителната организация са регламентирани чрез:

Длъжностни характеристики;

- Политика за мрежова и информационна сигурност;
- Политики на Системата за управление на информацията сигурност.

9. ЦЕЛИ

Целите на Система за управление на информационната сигурност включват:

- Защита на информационните активи от неоторизиран достъп, унищожаване, промяна и изтичане на информацията.
- Гарантиране на непрекъснатостта и наличността на информационните системи.
- Осигуряване на спазването на приложимите закони, регулации и стандарти за информационна сигурност.
- Поддържане на доверие в на клиенти, партньори и други заинтересовани

страни в образователната институция.

10. ОБХВАТ

- Системата за управление на информационната сигурност защитава информацията, която се съдържа в образователната институция, като защитата се осъществява на всички етапи на информационния процес. Системата се прилага за всички информационни активи и процеси, свързани с тях, включително:
- Информацията, получена, обработена и съхранена от ДГ“Първи юни“, град Кюстенил Информационните системи, включително хардуер, софтуер и мрежова инфраструктура.
- Всички служители, подизпълнители и трети лица, които имат достъп до информационните активи на образователната институция.
- Прилагането на конкретни механизми за контрол, както и изключенията е посочено в Декларацията за приложимост.

11. ОТГОВОРНОСТИ

5.1. Ангажираност на ръководството

- Установяване на политики и цели за информационната сигурност.
- Определяне на ресурсите и отговорностите за изпълнение на СУИС.
- Подкрепа и ангажимент към постоянното подобряване на информационната сигурност.

5.2. Сигурност на информацията

- Идентифициране, класифициране и установяване на мерки за защита на информационните активи.
- Изграждане и поддръжка на механизми за управление на достъпа до информационните активи.
- Изграждане и поддръжка на механизми за откриване, предотвратяване и реагиране на инциденти в информационната сигурност.

5.3. Обучение и осведоменост

- Предоставяне на обучение и осведоменост на персонала относно политиките, процедурите и практиките за информационна сигурност.
- Усъвършенстване на знанията и уменията на персонала за ефективно изпълнение на задачите си.

5.4. Система за управление на информационната сигурност включва:

- Изграждане, внедряване и поддръжка на СУИС,.
- Преглеждане и подобряване на СУИС чрез систематични одити и прегледи.

12. ПОЛИТИКИ, ПРОЦЕДУРИ И ПРАВИЛА

Ръководството за СУИС включва редица политики, процедури и правила, които се изпълняват и включват като минимум следните основни елементи на информационната сигурност:

- Идентификация и класификация на информационните активи.
- Управление на активите.
- Управление на достъпа до информационните активи.
- Изграждане и поддръжка на политики и процедури за сигурността на информацията.
- Управление на риска в информационната сигурност.
- Управление на доставчиците.
- Управление на инциденти в информационната сигурност.
- Обучение и осведоменост на персонала.
- Преглед и подобряване на СУИС.

Приложение към методика за оценка на риска

.....

(наименование на образователната институция, населено място, адрес, телефон, е-поща)

ИЗЯВЛЕНИЕ ЗА ПРИЕМАНЕ НА РИСК

НА

.....

(наименование на образователната институция)

ВАЖНО: *Това е най-малко желаната опция и означава, че образователната институция приема определения риск, без да направи нищо. Желателно е тази опция да се използва, само ако разходите за намаляване на риска биха били по-големи от щетите, които инцидентът би нанесъл!*

Въз основа на извършената оценка на риска и уязвимостта на информационните активи, свързани с ..... *(име на проекта/системата)*, образователната институция посочва следното становище относно приемането на риск:

Идентифицирани рискове:

.....
.....
.....

(Описват се идентифицираните рискове, свързани с информационните активи и проекта/системата)

Причини за приемане на риска:

.....
.....
.....

(Пояснява се причините и обстоятелствата, които довеждат до решението за приемане на риска)

Оценка на риска:

.....
.....
.....

(Представя се оценката на риска, включително нивото на вероятност и

въздействие, както и обосновка за тях)

Последици от приемането на риск:

.....
.....
.....

(Описват се предвидените последици и възможните вреди, които могат да възникнат в резултат от приемането на риска)

Определение на мерки за намаляване на риска:

.....
.....
.....

(Указват се предприетите мерки за намаляване на риска, включително контроли и процедури)

Съгласие и одобрение:

.....
.....
.....

..... *(име на упълномощено лице)*, в качеството си на ..... *(длъжност на упълномощеното лице)*, приема и одобрява риска, свързан с ..... *(име на проекта/системата)*.

Дата: **..... ..... 20..... г.** **Подпис**:

.....

.....
(име и фамилия на упълномощено лице)

III. Инструкция за унищожаване на информация

1. ЦЕЛ И ОБХВАТ

Целта на тази инструкция е да определи ясни насоки за унищожаване на информацията в образователната институция. Тази инструкция се прилага върху физически документи, електронни и други носители на информация, които съдържат чувствителни данни или информация, подлежащи на защита съгласно изискванията на националното законодателство и международни стандарти.

2. ПОДГОТОВКА НА ИНФОРМАЦИЯТА ЗА УНИЩОЖАВАНЕ

2.1. Идентифицира се информацията, която трябва да бъде унищожена, и се съобразява с класификацията ѝ според нейната важност и степен на поверителност.

2.2 Идентифицираните физически носители на информация се съхраняват на сигурно място, подходящо за унищожаване.

2.3. Въз основа на носителя на информация и класификацията се определят подходящия метод за унищожаване на информацията:

- **"Ниво 0" - TLP-WHITE** - Няма специални изисквания за унищожаване.
- **„Ниво 1" - TLP-GREEN**

- Унищожаване на хартиените носители.
- Изтриване на електронните копия по начин, не позволяващ възстановяването им.
- Надеждно изтриване или физическо унищожаване на медии.

- **„Ниво 2" - TLP-AMBER**

- Унищожаване на хартиените носители.
- Изтриване на електронните копия по начин, не позволяващ възстановяването им.
- Надеждно изтриване или физическо унищожаване на медии.

- **„Ниво 3" - TLP-RED**

- Унищожаване на хартиените носители.

· Изтриване на електронните копия по начин, не позволяващ възстановяването им.

- Надеждно изтриване или физическо унищожаване на медии.

3. МЕТОД ЗА УНИЩОЖАВАНЕ

3.1. Физическо унищожаване на хартиени документи

Физическото унищожаване на хартиени документи е един от най-разпространените методи за унищожаване на чувствителна информация. Този метод може да включва накъсване, нарязване на дребни части, унищожаване, чрез шредери или изгаряне на хартиени документи. Образователната институция разполага с подходящи средства или услуги за унищожаване на хартиени документи, за да гарантират, че процесът се извършва в по сигурен начин.

3.2. Надеждно изтриване на електронна информация

За надеждно изтриване на електронна информация се използват софтуерни инструменти, които гарантират безвъзвратно изтриване на данните. Това включва използването на специализирани програми, които премахват всяка възможност за възстановяване на информацията. Образователната институция е избрала надеждни софтуерни инструменти за трайно изтриване, включително и с многократно презаписването на носителите. Използват се софтуери като: EaseUS BitWiper Free, Blancco Drive Eraser, CCleaner, DBAN и други, утвърдени и регистрирани в регистъра на разрешеният за използване софтуер на образователната институция.

3.3. Физическо унищожаване на носители на информация

Ако информацията е съхранена на физически носители на информация като CD, DVD, USB флаш устройства или телефонни SIM карти, те могат да бъдат физически унищожени. Този процес може да включва физическо удряне, смачкване, изгаряне или разсичане на носителя. Образователната институция е взела предпазни мерки, за осигуряване на сигурността на тези процеси и избягване на нежелано разпространение на чувствителна информация.

3.4. Унищожаване на магнитни носители

Унищожаването на информация, съхранена на магнитни носители като твърди дискове, магнитни ленти или флопи дискове, освен чрез физическо унищожаване може да се извършва със силно магнитно поле, което изтрива всички данни, правейки ги не четими и невъзстановими. За да се гарантира ефективността на унищожаването, обучителната институция може да използва подобни подходящи устройства, като за унищожаването следва указанията и препоръките на производителя.

3.5. Унищожаване на информация в облака или виртуални среди

За унищожаване на информация, съхранена в облакови услуги или виртуални среди, са необходими специализирани методи. В случай на необходимост при този

вид унищожаване, образователната институция може да се свърже с доставчика на услугата и да следва предоставените от него процедури за безвъзвратно изтриване на данните. Важно е да се увери, че информацията е била успешно унищожена и не може да бъде възстановена.

4. ПРОВЕРКА НА УСПЕШНОТО УНИЩОЖАВАНЕ

4.1. След приключване на процеса на унищожаване, се проверява дали информацията е била успешно унищожена и дали не може да бъде възстановена.

4.2. Проверка на медиите и носителите се прави, за да се гарантира, че информацията е изцяло унищожена и не остават следи от нея.

4.3. Резултатите от унищожаването се документира, за бъдеща проследяемост и отчетност.

5. ОТЧЕТНОСТ И ПРОВЕРКА

Документират се всички дейности, свързани с унищожаването на информацията, включително дата, час, тип на унищожената информация, използван метод за унищожаване и имената на определено от директора лице, отговорно за правилното унищожаване, като за целта се попълва и протокол за унищожаване на информацията - ПРИЛОЖЕНИЕ 1.

6. ПРЕГЛЕД И ПОДОБРЕНИЕ

Инструкцията за унищожаване на информация се преглежда и актуализира периодично, поне веднъж годишно. Резултатите от прегледите се документират и използват за подобряване на процесите на управление на действията при унищожаване на информацията.

ПРИЛОЖЕНИЕ 1

ПРОТОКОЛ

за унищожаване на информация

Днес, ... 20..... г. *(дата), в* ..... часа, в ..... *(зала, стая №.., др.)*, подписаният/ата ..... *(име и фамилия)*, на длъжност: ....., извърших унищожаване на информация и носители на информация и съставих настоящия протокол за унищожаването на информация с изтекъл срок за съхранение, включително и резервни копия от тях, както следва:

1. Данни съхранявани на магнитни носители за многократен запис, чрез трайно изтриване, вкл. презаписването на носителите.
2. Данни съхранявани на хартиен носител, чрез: нарязване.
3. Данни съхранявани на оптични носители за еднократен запис, чрез физическо унищожаване на носителите.

Унищожените данни: ..... *(Не са обработвани чрез облачни услуги).*

Служител: ....., ..., ...
(име и фамилия) *(длъжност)* *(подпис)*

IV.Инструкция за обозначаване на информацията

1.ЦЕЛ И ОБХВАТ

Целта на тази инструкция е да определи ясни насоки за обозначаване на информацията в образователната институция. Тази инструкция се прилага върху физически документи, електронни данни и други носители на информация, които съдържат чувствителни данни или информация, подлежащи на защита съгласно изискванията на националното законодателство и международните стандарти.

2.ОБОЗНАЧАВАНЕ И КЛАСИФИКАЦИЯ НА ИНФОРМАЦИЯТА

Образователната институция идентифицира информацията, която се обозначена, въз основа на нейната чувствителност и важност.

Електронните документи в четим вид се обозначават във долната част (Footer), а всички преносими информационни активи (USB памети, CD, DVD, външни дискове и др.) имат външен етикет с не изтриваема маркировка. Всеки един информационен актив следва да бъде обозначен със съответната класификация. За класифициране на електронните данни в системи се използват софтуерни механизми.

Класификацията на електронните данни е ясна и видима за потребителите и съответните системи за управление на информацията.

За гарантиране на правилният достъп, разпространение, съхранение, архивиране и унищожаване на информацията в образователната институция се определят следните нива на класификация на информацията в съответствие на действащите законови разпоредби, в частност на Наредбата за минималните изисквания за мрежова и информационна сигурност (НМИМИС).

3.НИВА ПРИ ОБОЗНАЧАВАНЕ НА ИНФОРМАЦИЯТА

TLP (traffic light protocol) - използва се при обмен на информация

[TLP-RED] - Само за определени получатели: в контекста на една среща например информацията се ограничава до присъстващите на срещата. В повечето случаи тази информация се предава устно или лично.
[TLP-AMBER] - Ограничено разпространение: получателят може да споделя тази информация с други хора от институцията, но само ако е спазен принципът „необходимост да

се знае“. Честа практика е източникът на информацията да уточни веднага след маркировката на кого може да се споделя информацията или да предвиди ограничения на това споделяне. Ако получателят на информацията иска да я разпространява, задължително трябва да се консултира с източника.
[TLP-GREEN] - Широка общност: информацията в тази категория може да бъде разпространявана широко в рамките на дадена общност. Въпреки това информацията не може да бъде публикувана или поствана в интернет, както и изнасяна извън общността.
[TLP-WHITE] - Неограничено: предмет на стандартните правила за авторско право; тази информация може да се разпространява свободно, без ограничения.

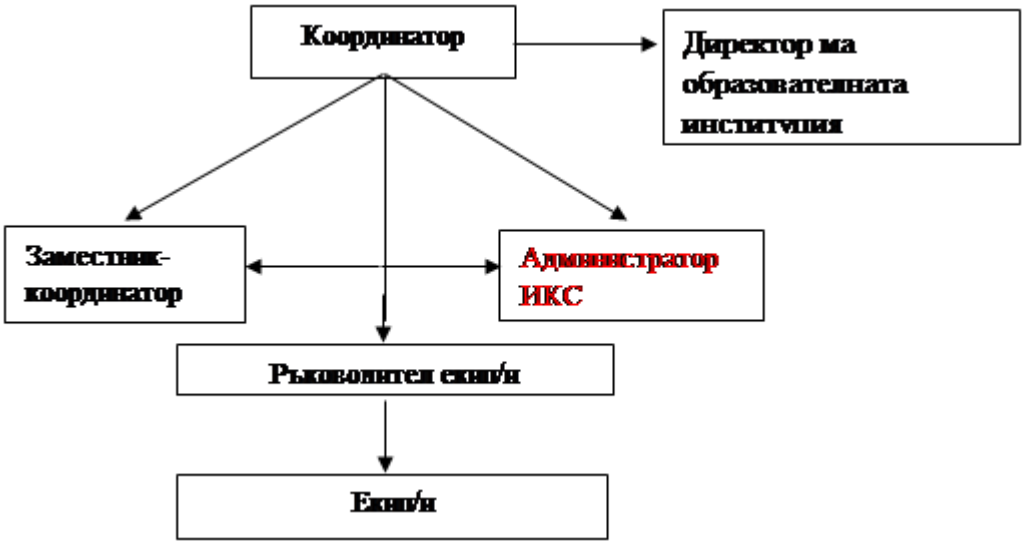
1. **"Ниво 0"** обхваща открита и общодостъпна информация (например публикувана на интернет страниците). Предполага анонимно ползване на информацията и липса на средства за защита на конфиденциалността й. Отговаря на **TLP-WHITE.**
   - Оповестяването на информация с класификация **"Ниво 0"** не е ограничено.
   - Източниците могат да използват класификация **"Ниво 0"**, когато информацията носи минимален или никакъв предвидим риск от злоупотреба, в съответствие с приложимите правила и процедури за публично оповестяване.
   - При спазване на стандартните правила за авторски права информация с класификация **"Ниво 0"** може да се разпространява без ограничения.
   - Унищожаването на информацията маркирана с това ниво се извършва съгласно инструкцията утвърдена в образователната институция.
2. **„Ниво 1"** Споделянето на информация с класификация **„Ниво 1"** е ограничено само до дадена общност. Отговаря на **TLP-GREEN.**
   - Източниците могат да използват класификация **„Ниво 1"**, когато информацията е полезна за информираността на всички участващи организации, както и с партньори от широката общност или сектор.
   - Получателите могат да споделят информация с класификация **„Ниво 1"** с партньорски организации в рамките на своя сектор или общност, но не и чрез обществено достъпни канали. Информацията в тази категория може да се разпространява широко в дадена общност, но не и извън нея.
   - Унищожаването на информацията маркирана с това ниво се извършва съгласно инструкцията утвърдена в образователната институция.

3. **„Ниво 2"** Разпространението на информация с класификация **„Ниво 2"** е разрешено само в рамките на организациите на участниците, обработващи, съхраняващи или обменящи информацията. Отговаря на **TLP-AMBER** с допълнително уточнение за ограничение на достъпа.
   - Източниците могат да използват класификация **„Ниво 2",** когато информацията изисква защита, за да бъде ефективно обменена и носи риск за неприкосновеността на личния живот, репутацията или операциите, ако се споделя извън съответните организации.
   - Получателите могат да споделят информация с класификация **„Ниво 2"** с членове на собствената си институция и с потребители или клиенти, които трябва да са запознати с нея, за да се защитят или да предотвратят допълнителни щети. Източниците имат правото да определят допълнителни планирани граници на споделянето, които трябва да се спазват.
   - Унищожаването на информацията маркирана с това ниво се извършва съгласно инструкцията утвърдена в образователната институция.
4. **„Ниво 3"** Информация с класификация **„Ниво 3"** не е за оповестяване и разпространението й е ограничено само до участниците, обработващи, съхраняващи или обменящи информацията. Отговаря на **TLP-RED.**
   - Източниците могат да използват класификация **„Ниво 3",** когато информацията не може да бъде ефективно обменяна с други страни и би могла да доведе до въздействия върху неприкосновеността на личния живот, репутацията или операциите на дадена страна, ако с нея бъде злоупотребено.
   - Получателите не могат да споделят информация маркирана с **„Ниво 3",** с която и да е страна извън конкретния обмен, обработка или съхранение. Достъпът до информацията с класификация **„Ниво 3"** е ограничен само до лицата, участващи в обработката й. В повечето случаи информация с класификация **„Ниво 3"** трябва да се предава лично.
   - Унищожаването на информацията маркирана с това ниво се извършва съгласно инструкцията утвърдена в образователната институция.

4.ПРЕГЛЕД И ПОДОБРЕНИЕ

Инструкция за обозначаване на информацията се преглежда и подобрявани редовно, минимум веднъж в годината от определеният служител по информационна сигурност. Прегледът включва анализ на ефективността на предприетите мерки и идентифициране на възможности за подобрение.

V.ПЛАН НЕПРЕКЪСНАТОСТ НА ДЕЙНОСТТА



VI. ПОЛИТИКИ:

- Политиката по мрежова и информационна сигурност

1. ВЪВЕДЕНИЕ

1.1. Цел и обхват

Политиката по мрежова и информационна сигурност има за цел да установи рамката и принципите за защита на информационните активи в образователната институция, съгласно изискванията на стандарт ISO 27001 и приложимата нормативна уредба. Тя обхваща всички аспекти на мрежовата и информационна сигурност (МИС), включително управлението на активите, физическата сигурност, управлението на достъпа, управлението на риска, комуникационната и оперативна сигурност, управлението на инциденти, непрекъснатостта на дейността и управлението на сигурността на информацията, взаимоотношения с трети страни и други.

1.2. Приложимост

Политиката по мрежова и информационна сигурност се прилага за всички служители, подизпълнители и външни потребители, които имат достъп до информационните активи на образователната институция.

2. ОБЩИ ПРИНЦИПИ

2.1. Сигурност на информацията

Осигуряваме адекватна защита на информационните активи, която включва поверителност, цялостност и наличност на информацията. Информацията е защитена от неоторизиран достъп, увреждане, загуба или разкриване.

2.2. Риск-ориентиран подход

Използваме риск-ориентирания подход за управление на мрежовата и информационна сигурност. Идентифицираме и оценяваме рисковете за информационните активи и предприемаме подходящи мерки за справяне с тях. При вземането на решения относно сигурността, вземаме предвид актуалните потенциални рискове и предимствата за образователната институция.

2.3. Съответствие със законовите и регулаторни изисквания

Поддържаме нашите политики в съответствие на всички приложими законови и регулаторни изисквания, свързани с мрежовата и информационна сигурност, които се отнасят до нашата образователна институция и дейност, а така също и с международните стандартите.

2.4. Непрекъснато подобрение

Преглеждаме периодично и подобряваме политиката и практиките си за мрежова и информационна сигурност. Актуализираме и развиваме мерките си в отговор на нови заплахи, технологии и други изисквания, за да осигурим постоянна и висока защита на мрежовата и информационна сигурност.

3. ЧОВЕШКИ РЕСУРСИ

3.1 Наемане на работа

Преди да публикуваме обяви за работа, осигуряваме ясно определение на ролите и отговорностите на служителите, които ще имат достъп до информационните активи. Това ни позволява да определим необходимите компетенции и умения за успешното изпълнение на задачите.

При наемане на работа извършваме проверка на референции, свързани с предишни работодатели и образователни институции, за да потвърдим професионалния и образователен опит на кандидатите. Когато кандидатите ще имат достъп до чувствителна информация, изискваме проверка за извършени криминални прояви.

3.2 Обучение и осведоменост

Осигуряваме подходящо обучение на всички служители относно политиките и процедурите по мрежова и информационна сигурност. Служителите ни са информирани и осведомени, както за рисковете от нарушенията на политиките ни така и за начина им на действие и докладване на инциденти и нарушения на сигурността.

4. УПРАВЛЕНИЕ НА АКТИВИТЕ

4.1. Идентификация на активите

Идентифицираме информационните активи в нашата образователната институция като поддържаме Регистър на активите и ги класифицираме според тяхната важност и чувствителност. Имаме ясно разбиране за стойността на всякаква информация, която обработваме и съхраняваме.

4.2. Собственост и отговорности

Определяме ясно собствеността и отговорности за информационните активи. Всеки служител и изпълнител има задължението да се грижи за информационните активи, с които работи, и да ги използва само в рамките на правомощията и отговорностите си.

5. ФИЗИЧЕСКА ЗАЩИТА И ОКОЛНА СИГУРНОСТ

5.1. Физическа защита

Осигуряваме физическа защита на информационните активи, включително учебните стай и кабинети, центровете за данни и другите физически обекти. Имаме контроли за достъп, видеонаблюдение, ограничаване на физическия достъп и други мерки за физическа сигурност.

5.2. Обезопасяване на оборудването

При инсталиране и използване на мрежово и информационно оборудване, прилагаме добрите практики. Защитаваме оборудването от физически увреждания, кражби и неоторизиран достъп.

6. УПРАВЛЕНИЕ НА ЛОГИЧЕСКИЯ ДОСТЪП

6.1. Идентификация и удостоверяване

Използваме механизми за идентификация и удостоверяване на потребителите, за да контролираме достъпа до информационните активи. Изискваме силни пароли и многофакторно удостоверяване на потребителите, където е необходимо.

6.2. Авторизация и контрол на достъпа

Предоставяме само необходимите привилегии на потребителите, в съответствие с техните роли и отговорности. Имаме контроли за отчитане на достъпа и мониторинг на активността, за да предотвратим неоторизиран достъп и злоупотреби.

7. КОМУНИКАЦИОННА И ОПЕРАТИВНА СИГУРНОСТ

7.1. Защита на мрежовата инфраструктура

Прилагаме мерки за защита на мрежовата инфраструктура, включително сигурни конфигурации, защитни устройства и контрол на трафика. Редовно обновяваме и актуализиране на софтуера и хардуера, за да се предотврати уязвимости.

7.2. Защита на информацията при обмен

Осигуряваме сигурен обмен на информация, включително използване на криптиране и сигурни протоколи. Използваме защитени връзки, виртуални частни мрежи и други технологии, за да защитим информацията при обмен.

8. УПРАВЛЕНИЕ НА ИНЦИДЕНТИ

8.1. Управление на инциденти

Разработваме и поддържаме процедури и планове за бързо и ефективно управление на инциденти в областта на мрежовата и информационна сигурност. Разполагаме с комуникационни пътища и процеси за своевременно откриване, докладване и реагиране на инцидентите.

8.2. Откриване и реагиране

Имаме системи и механизми за откриване на инциденти и своевременна реакция в случай на нарушение на сигурността. Провеждаме редовен мониторинг и анализ на събитията, за да открием потенциални инциденти и да предприемем необходимите действия.

9. НЕПРЕКЪСНАТОСТ НА ДЕЙНОСТТА

9.1. Планиране действия при бедствия

Разработваме и поддържаме планове за непрекъснатост, които да осигурят непрекъснатост на операциите при бедствени ситуации. Извършваме оценка на риска и тестване на плановете, за да сме готови да реагираме и възстановим дейността ни възможно най-бързо.

9.2. Резервни копия и възстановяване

Периодично правим резервни копия на информацията и използваме механизми за възстановяване, за да запазим целостта и наличността на информацията при повреди или загуби. Провеждаме редовно тестване и възстановяване на системите и данните.

10. УПРАВЛЕНИЕ НА СИГУРНОСТТА НА ИНФОРМАЦИЯТА

10.1. Политики и процедури

Изготвяме, прилагаме и поддържаме политики и процедури за управление на сигурността на информацията. Обучаваме служителите и изпълнителите за техните отговорности и задължения по отношение на сигурността на информацията.

10.2. Вътрешен контрол

Извършваме редовна проверка и преглед на ефективността на мерките за сигурност на информацията. Провеждаме вътрешни одити и прегледи, за да се уверим, че се спазват политиките и процедурите.

11. НАРУШЕНИЯ И НАКАЗАНИЯ

Всички потребители осъзнават своята роля и отговорности по отношение въпросите свързани с МИС и защита на информационните активи. Всяко действие на потребител, несъответстващо на тази политика, което води до разкриване, нарушение на целостта, конфиденциалността и наличието на информацията е обвързано с предприемането на дисциплинарни мерки, включително прекратяване на трудовите или договорните взаимоотношения, както и с търсене на имуществена или друга отговорност, съобразно с действащото законодателство.

12. ВЗАИМООТНОШЕНИЯ С ТРЕТИ СТРАНИ

12.1 . Обменът на информация в електронен формат със заинтересовани страни

Обменяме информация при спазване на разпоредбите на съответните закони, регламентиращи условията и реда за събиране, съхраняване, използване и разкриване на информация, представляващи лични данни или друга защитена от закон информация.

12.2. Сигурност на информацията при взаимодействие с доставчици. Договори с доставчици

При обмяна на информация с доставчици извършваме подходящи проверки и въвеждаме специфични изисквания, във всеки конкретен случай. В договорите с доставчици, които имат отношение към използване на информация, съхранявана и/или пренасяна включително и по електронен път поставяме клаузи за не разкриване на информацията станала им известна при изпълнението на договора. Предприемаме конкретни мерки и подходяща защита към всички доставчици и дейностите, които те извършват.

12.3. Защита на информацията на трети страни

Защитаваме конфиденциалността на информацията, собственост на трети страни, през целия период на съществуването й. При обработването на лични данни, стриктно спазваме основните принципи: законосъобразност, добросъвестност и прозрачност, целесъобразност и точност, пропорционалност, отчетност, цялостност и поверителност. Всички служители, които имат достъп до такава информация, спазват конфиденциалността на тази информация и не я разкриват на други лица.

13. УПРАВЛЕНИЕ НА РИСКА

13.1. Оценка на риска

Извършваме оценка на риска периодично, но не по-рядко от веднъж годишно, или когато са на лице съществени изменения в условията на работа, инфраструктурата или процесите ни. Това правим посредством утвърдена методика за оценката на риска, като се съобразяваме с актуалните заплахи и уязвимости, които могат да повлияят на сигурността.

13.2. Управление на риска

Непрекъснато наблюдаваме за промени в средата, които биха довели до заплаха за информационните активи, и правим необходимите промени за поддържане на приемливо ниво на риска и поддържаме баланс между процесите ни и сигурността.

14. ОРГАНИЗАЦИЯ И УПРАВЛЕНИЕТО НА МИС

14.1. Организация на МИС

Прилагаме принципа на разпределение на задълженията на служителите, съгласно който едно лице не може да има правомощията и задълженията за управление на данните и системите и управление на механизмите по сигурността, които защитават същите данни и системи.

14.2. Управлението на МИС

Отговорни за реализирането и контрол по изпълнението на Политиката, както и за вземане на решения по стратегически въпроси, свързани с мрежовата и информационната сигурност, са:

1. Съвет по информационна сигурност – консултативен и координиращ орган по мрежова и информационна сигурност/4 членен/.
2. Служителя отговорен за МИС – лицето отговорно за МИС в образователната институция/ Емилия Сотирова-ЗАС/
3. Администратор на ИКС в образователната институция /Десислава Костова-зам.директор.
4. Собственици на системите в образователната институция.
5. Потребители на системите в образователната институция.

15. УПРАВЛЕНИЕ НА ИНФОРМАЦИОННИТЕ СИСТЕМИ

15.1. Поддръжка на информационните системи

Поддържаме информационните системи в работоспособно състояние и ги наблюдаваме за прекъсвания в работата им. В случай на прекъсване уведомяваме за това отговорните лица. Поддържането се извършва само от оправомощени за това лица.

15.2. Крайни работни станции.

Работните ни станции могат да бъдат стационарни или преносими компютри. Служителите носят материална отговорност за компютри, които им се предоставят за ползване. Забранено е инсталирането на нелицензиран софтуер и такъв, който не е утвърден за използване в обучителната ни организация.
Работните ни станции са защитени с използването на антивирусен софтуер с актуални антивирусни дефиниции.
15.3. Използване на Интернет и електронна поща
За изпълнение на служебните си задължения всеки служител има право на достъп до Интернет, но сме забранили посещението на сайтове свързани с нарушение на интелектуалната собственост, такива който съдържат порнографски материали или съдържат информация свързана с насилие.
Забранили сме използването на служебни пощи за лични цели.
16. ПРИДОБИВАНЕ УПРАВЛЕНИЕ И УСЪВЪРШЕНСТВАНЕ НА ИНФОРМАЦИОННИ АКТИВИ
16.1. Придобиване/създаване на информационен актив (ИА).
Всички изисквания към сигурността на ИА задаваме още във фазата на създаването на изискванията за проекта, като част от цялостния процес по създаването на информационна система.
16.2. Управление на промените на информационен актив.
При управлението на промените включваме задължително оценяване на риска, анализ на влиянието на промените и изисквания към необходимите действия за контрол на сигурността. За особено критични приложения сме предвидили възможност за дву етапно въвеждане в експлоатация - в тестова и в продуктивна среда.
16.3. Въвеждане в експлоатация на информационен актив.
Одобряваме за въвеждане в експлоатация нови информационни системи след успешно проведени и документирани тестове, доказващи защитата на информацията от загуба на достъпност, интегритет и конфиденциалност. Критериите за приемане и тестване на информационните системи задаваме преди всяка нова инсталация/доставка на информационния актив.

➢ Политика за управление на непрекъснатостта на дейността

1.ВЪВЕДЕНИЕ И ОБХВАТ:

Образователната институция се ангажира да осигури непрекъснатост на дейността, като прилага проактивни и реактивни мерки за преодоляване на възникнали събития, които биха могли да повлияят на функционирането ѝ. Тази политика се прилага върху всички аспекти на институцията, включително хора, процеси и технологии.

2.ОТГОВОРНОСТИ:

2.1. Директорът на образователната институция е отговорен за разработването, поддръжката и непрекъснатото подобряване на политиката за управление на непрекъсваемостта на дейността.

2.2.Определеният служител по информационна сигурност е отговорен за мониторинга и оценката на съответствието на политиката за управление на непрекъсваемостта, както и за предоставянето на необходимото обучение на служителите относно тази политика.

2.3. Отделните служители са отговорни за спазването на политиката и изпълнението на плана и дейностите, свързани с непрекъсваемостта на процесите.

2.4. Неспазването на политиката може да доведе до дисциплинарни мерки и/или правни последици в зависимост от сериозността на нарушението.

3.РИСКОВ АНАЛИЗ И УПРАВЛЕНИЕ:

Образователната институция извършва систематичен рисков анализ, за да идентифицира потенциалните заплахи и уязвимости, които могат да доведат до нарушаване на непрекъснатостта на дейността и процесите, които осъществява. Базирано на този анализ, се разработва, утвърждава и изпълнява план за управление на риска, който включва мерки за намаляване на рисковете и подобряване на възстановителните способности.

4.ПЛАНОВЕ ЗА НЕПРЕКЪСНАТОСТТА НА ДЕЙНОСТТА:

Образователната институция разработва, поддържа и актуализира планове за непрекъснатост на дейността за всички критични процеси в образованието. Плановете трябва да включват процедури за възстановяване, комуникация, достъп до резервни ресурси и възстановяване на информационните технологии.

➢ ПОЛИТИКА ЗА УПРАВЛЕНИЕ НА ЧОВЕШКИТЕ РЕСУРСИ

I. ВЪВЕДЕНИЕ И ОБХВАТ

Настоящата политика за управление на човешките ресурси е разработена в съответствие с изискванията на международни стандарти свързани с мрежовата и информационна сигурност (МИС) и има за цел да гарантира сигурността на информационните активи в образователната институция чрез ефективно управление на хората, които имат достъп до тези активи.

Тази политика важи за всички служители, външни изпълнители и други заинтересовани страни, които имат достъп до информационните активи на образователната институция.

II. ОТГОВОРНОСТИ

1. Директорът на образователната институция е отговорен за утвърждаването и поддържането на политиката за управление на човешките ресурси.

2. Служителят, отговорен за човешките ресурси, разработва и поддържа политики, и процедури, свързани с управлението на персонала на образователната институция.

3. Определеният служител по информационна сигурност е отговорен за мониторинга и оценката на съответствието с политиките и процедурите за управление на човешките ресурси, както и за предоставянето на необходимото обучение на служителите относно тези политики и процедури.

4. Служителите спазват всички приложими политики, свързани с управлението на човешките ресурси, и да съдействат в осъществяването на сигурността на информационните активи.

5. Неспазването на политиката може да доведе до дисциплинарни мерки и/или правни последици в зависимост от сериозността на нарушението.

III. ИЗИСКВАНИЯ ЗА НАЕМАНЕ

1. Определение на роли и отговорности:

Преди публикуване обяви за работа, се осигурява ясно определение на ролите и отговорностите на служителите, които ще имат достъп до информационните активи. Това позволява да се определят необходимите компетенции и умения за успешното изпълнение на задачите.

2. Проверка за референции

При провеждане на процеса на наемане се извършва проверка за референции, свързани с предишни работодатели и образователни институции, за да се потвърди професионалния и образователен опит на кандидатите.

3. Проверка за наличие криминални прояви.

При наемане на служители, които ще имат достъп до чувствителна информация, се изисква и проверка за криминалния прояви на кандидатите, в съответствие с приложимите законови разпоредби.

IV. ИЗИСКВАНИЯ ПРИ НАПУСКАНЕ/ПРЕКРАТЯВАНЕ НА РАБОТА

При напускане на работа от всеки служител се изисква предоставяне на трудовата книжка, с цел отбелязване и приключване на трудовия стаж в ДГ“Първи юни“, град Кюстендил.

V. УПРАВЛЕНИЕ НА ДОСТЪПА ДО ИНФОРМАЦИОННИТЕ АКТИВИ

Правата за достъп до информационните активи са зададени на базата на принципа на най-малките привилегии (принципът на "необходимостта да се знае за изпълнение на служебните задължения").

Използването на информационните активи е проследено и контролирано, за да се гарантира отговорно използване и защита на активите.

Информацията за достъпа до информационните активи се поддържана актуална и се ревизира периодично минимум веднъж в годината, за да е сигурно, че достъпът се предоставя само за изпълнение на служебните задължения.

Всички промени в персонала, включително започване, промяна или прекратяване на работната позиция, са подложени на проверки, за да се осигури подходящо уведомление и преглед на съответните достъпни права.

VI. ОБУЧЕНИЕ И ОСВЕДОМЕНОСТ

1. Обучения по информационна сигурност

Образователната институция осигурява подходящо обучение на всички служители (включително новопостъпващи) относно политиките и процедурите за управление на човешките ресурси и сигурността на информационните активи.

На служителите се осигурява информация или обучения за рисковете от несъответствие с политиките и процедурите, и за докладване на инциденти и нарушения на сигурността.

2. Подписване на специфични споразумения

Всички служители (включително новите), които имат достъп до информационни активи, се задължават да подпишат декларация за опазване на информацията (ПРИЛОЖЕНИЕ 1), с която се ангажират да спазват политиките и процедурите за информационна сигурност, както и да запазят поверителността на информацията, до която имат достъп.

VII. СПАЗВАНЕ НА ЗАКОНОВИТЕ ИЗИСКВАНИЯ

Образователната институция спазва всички приложими закони и регулации, свързани с управлението на човешките ресурси и защитата на информационните активи.

ПРИЛОЖЕНИЕ 1

Д Е К Л А Р А Ц И Я

от

……..……..……..……..
(име, презиме и фамилия)

на длъжност…….……

ДЕКЛАРИРАМ, че:

1. Съм запознат/а с **Политиката по мрежова и информационна сигурност в обучителната ни организация**, утвърдени със заповед на директора и ще спазвам всички политики, процедури, указания, и установените с тях права, задължения и ограничения в областта на мрежовата и информационна сигурност.

2. Известно ми е, че неспазването на установените изисквания в областта на мрежовата и информационна сигурност в обучителната организация е достатъчно основание да ми бъде наложено наказание (включително прекратяване на служебно, трудово или договорно взаимоотношение), както и да ми бъде търсена имуществена или друга отговорност, в съответствие с действащото законодателство.

3. Няма да разпространявам станалата ми известна информация, касаеща мрежовата и информационна сигурност в обучителната ни организация пред други лица, включително и след прекратяване на правоотношенията ми.

Дата: …… ….. 2025 г. **ДЕКЛАРАТОР:**……
(подпис)

<u>ПОЛИТИКА ЗА ФИЗИЧЕСКА СИГУРНОСТ</u>

ВЪВЕДЕНИЕ И ОБХВАТ

Настоящата политика за физическа сигурност е разработена в съответствие с изискванията на международни стандарти свързани с мрежовата и информационна сигурност (МИС) и има за цел да осигури опазването и защитата на физическата инфраструктура и активи на образователната институция.

Тази политика важи за всички физически обекти, инфраструктура и активи, свързани с информационните активи на образователната институция, както и за всички служители, външни изпълнители и други заинтересовани страни, които имат достъп до тези обекти и активи.

I. ОТГОВОРНОСТИ

1.Директорът на образователната институция е отговорен за създаването на политики и процедури, които се отнасят до физическата сигурност.

2.Заместник-директорът по административно стопанската дейност е отговорен за разработването, изпълнението и поддържането на политики, процедури и системи, и Регистър на събития, свързани с физическата сигурност.

3.Определеният служител по информационна сигурност е отговорен за мониторинга и оценката на съответствието с политиките и процедурите за физическа сигурност, както и за предлагане на теми за обучения на служителите, относно тези политика.

4.Служителите спазват всички приложими политики и процедури, свързани с физическата сигурност, и съдействат в осъществяването на защитата на физическата инфраструктура и активите.

5.Неспазването на политиката може да доведе до дисциплинарни мерки и/или правни последици в зависимост от сериозността на нарушението.

II. ФИЗИЧЕСКИ ДОСТЪП И КОНТРОЛ

Образователната институция е предприела подходящи мерки за контрол и ограничаване на физическия достъп до информационните активи и физическата инфраструктура.

След заповед на директора за определяне на комисия по архив,само гл.счетоводител и ЗАС имат ключ от помещението-архив, по този начин само упълномощени лица имат достъп до физическите обекти и активи.

Извършват се редовни прегледи на физическата инфраструктура и контролните мерки, за да се гарантира, че те са ефективни и отговарят на изискванията за сигурност.

III. ВИДЕОНАБЛЮДЕНИЕ И МОНИТОРИНГ

Където е необходимо, се използва видеонаблюдение за защита на физическата инфраструктура и активите на образователната институция/чрез община Кюстендил/.

Мониторингът на системите за видеонаблюдение се извършва редовно от директора на детската градина, за да се засекат възможни нарушения и нередности.

IV. УПРАВЛЕНИЕ НА БЕДСТВИЯ И АВАРИЙНИ СИТУАЦИИ

Планове за управление на бедствия и аварийни ситуации са разработени и изпълнени, за да се минимизират потенциалните щети и прекъсвания на работата в случай на физически инциденти.

Редовни проверки и прегледи на плановете се извършват, за да се гарантира, че те са актуални и действащи.

➢ **ПОЛИТИКА ЗА КОНТРОЛ НА ДОСТЪП**

I. ВЪВЕДЕНИЕ И ОБХВАТ

Настоящата политика за контрол на достъпа има за цел да осигури оптимално управление и защита на достъпа до информационните активи на образователната институция.

Целта на политиката е да гарантира, че образователната институция разполага със съответните мерки за сигурност, за да предотврати неправомерен достъп до информацията си.

II. ОТГОВОРНОСТИ

Тази политика важи за всички информационни активи, системи и процеси в образователната институция, както и за всички служители, външни изпълнители и други заинтересовани страни, които имат достъп до тези активи и системи.

1. Директорът на образователната институция е отговорен за създаването на политики и процедури, свързани с контрола на достъпа, като се вземат предвид съответните изисквания на националното законодателство и международните стандарти.
2. Служителите спазват всички приложими политики и процедури, свързани с контрола на достъпа, и съдействат в осигуряването на оптималната защита на информационните активи.
3. Определеният служител по информационна сигурност е отговорен за разработването, изпълнението и поддържането на политики, процедури и системи, свързани с контрола на достъпа, за предоставяне на необходимата обучение на служителите относно тези механизми а така също и редовен преглед на актуалните достъпи/привилегии до системите.
4. Администратора на ИКС е отговорен за техническата реализация и поддръжка на механизмите за контрол на достъпа, за предоставянето на достъпите, съобразно стандартните профили за достъп до ИС и за допълнително поискани такива след получена информация по имейл от директора на образователната институция.

5. Неспазването на политиката може да доведе до дисциплинарни и административни мерки и/или правни последици в зависимост от сериозността на нарушението и съгласно действащото законодателство.

III. ИДЕНТИФИКАЦИЯ И УДОСТОВЕРЯВАНЕ

1. Всички потребители и системи са идентифицирани и удостоверени преди да им бъде предоставен достъп до информационните активи.

2. Удостоверяването на потребителите използва надеждни и сигурни методи, като пароли, токен системи, биометрични данни или други сходни механизми.

3. Уникални идентификатори са присвоени на всеки потребител и система, за да се осигури отчетността и проследяемостта на достъпа.

IV. УПРАВЛЕНИЕ НА ПРИВИЛЕГИИТЕ

1. На потребителите се осигурява достъп съгласно утвърдени от директора на образователната институция стандартни достъпи до информационните системи.

2. При достъп до поверителна или критична информация, отделни потребители са разпределени в специални роли или групи с ограничен достъп.

3. Правата и привилегиите на потребителите са определени на база на принципа на най-малките привилегии (principle of least privilege), където потребителите получават само тези права (съгласно стандартните достъпи до информационните системи), които са необходими за изпълнението на техните работни задачи.

4. Разглеждането и променянето на привилегиите са ограничени до упълномощени лица и подлежат на редовен (поне веднъж годишно) мониторинг и преглед.

V. УПРАВЛЕНИЕ НА ФИЗИЧЕСКИЯ ДОСТЪП

1. Физическият достъп до информационните активи и съответните физически обекти са стриктно контролиран и ограничен само до упълномощени лица.

2. Гарантира се, чрез ограничен достъп само на упълномощени лица до физическите обекти и активи.

3. Редовни проверки и прегледи на физическия достъп и контролни мерки се извършват, за да се уверим, че те са ефективни и отговарят на изискванията за сигурност.

VI. МОНИТОРИНГ И РЕГИСТРАЦИЯ

1. Всички активности, свързани с достъпа до информационните активи, са мониторирани и регистрирани, включително успешен и неуспешен достъп, промени в привилегиите и други съществени събития.

2. Пароли и логове са съхранявани на сигурно място като е осигурен контролиран достъп до тях.

3.Редовни проверки и анализ се извършват, за да се открият възможни нарушения и неразрешени действия.

- **ПОЛИТКА ЗА ОТДАЛЕЧЕН ДОСТЪП**

1. ВЪВЕДЕНИЕ И ОБХВАТ

Настоящата политика за отдалечен достъп е разработена в съответствие с изискванията на международни стандарти свързани с мрежовата и информационна сигурност (МИС) и има за цел да гарантира сигурността на информационните активи в образователната институция чрез ефективно управление на хората, които имат достъп до тези активи.

Тази политика важи за всички отдалечени достъпи до информационните активи на образователната институция, включително за служители, външни изпълнители и други заинтересовани страни, които имат разрешение за отдалечен достъп.

2. ОТГОВОРНОСТИ

2.1. Директорът на образователната институция е отговорен за създаването и поддръжката на политики и процедури, свързани с отдалечения достъп.

2.2. Определеният служител по информационна сигурност е отговорен за разработването, изпълнението и поддръжката на политиката за отдалечения достъп, както и за предоставянето на необходимото обучение на служителите относно тази политика.

2.3. Администратора на ИКС е отговорен за предоставянето на сигурни технически решения за отдалечен достъп, включително за конфигуриране, мониторинг и поддръжка на отдалечени достъпни системи.

2.4. Служителите, които използват отдалечен достъп, спазват всички приложими политики и процедури и съдействат за осигуряването на безопасността на информационните активи.

2.5. Неспазването на политиката може да доведе до дисциплинарни мерки и/или правни последици в зависимост от сериозността на нарушението.

3. УСЛОВИЯ ЗА ОТДАЛЕЧЕН ДОСТЪП

3.1. Потребителите преминат през идентификация и удостоверяване преди да им бъде предоставен отдалечен достъп до информационните активи.

3.2. Използването на сигурни протоколи и криптиране на данните се прилагат при отдалечен достъп, за да се гарантира сигурността на комуникациите и защитата на информацията от неоторизиран достъп.

3.3. Ограничаването на правата и привилегиите на потребителите при отдалечен достъп се основава на принципа на най-малките привилегии (principle of least privilege), като потребителите получават само необходимите права за изпълнение на техните служебни задължения.

4. ЗАЩИТА НА ОТДАЛЕЧЕНИТЕ ДОСТЪПНИ СИСТЕМИ

4.1. Администратора на ИКС предоставя сигурни технически мерки за защита на отдалечените достъпни системи, включително:

- защита от зловреден софтуер, уязвимости и неоторизиран достъп;
- най-малко двуфакторна автентикация при работа от разстояние;
- предоставя само канали с висока степен на защита като Virtual Private Network (VPN) ;
- проверява да не се използват File Transfer Protocol (FTP) и Remote Desktop Connection.

4.2. Редовни актуализации на софтуера и пачове свързани със сигурността се прилагат за отдалечените достъпни системи, за да се предотвратят потенциални уязвимости и за да се осигури актуална защита.

5. МОНИТОРИНГ И РЕГИСТРАЦИЯ

5.1. Всички активности при отдалечения достъп са регистрирани и мониторирани, включително успешни и неуспешни опити за достъп, промени в привилегиите и други съществени събития.

5.2. логове от отдалечените достъпни системи се съхраняват на сигурно място, като е осигурен и контролиран достъп до тях.

5.3. Редовни проверки и анализ на журналите от отдалечените достъпни системи се извършват, за да се открият възможни нарушения и несанкционирани действия.

➢ ПОЛИТИКА ЗА ПРИДОБИВАНЕ, РАЗВИТИЕ И ПОДДРЪЖКА НА СИСТЕМИТЕ

1. ВЪВЕДЕНИЕ И ОБХВАТ

Настоящата политика за придобиване, развитие и поддръжка на системите е разработена в съответствие с изискванията на международни стандарти свързани с мрежовата и информационна сигурност (МИС) и има за цел да осигури ефективното управление и поддръжка на информационните системи на образователната институция. Тя гарантира сигурността, наличността и надеждността на системите, които са от съществено значение за образователната институция.

2. ОТГОВОРНОСТИ

2.1. Директорът на образователната институция е отговорно за създаването и поддръжката на актуална политика за придобиване, развитие и поддръжка на системите.

2.2. Определеният служител по информационна сигурност е отговорен за разработването, изпълнението и поддръжката на технически и организационни мерки за придобиване, развитие и поддръжка на системите.
2.4. Отговорните служители спазват политиките за придобиване, развитие и поддръжка на системите, както и съдействат за осигуряването на сигурността на информацията още в етапа на разработването/придобиването на приложенията.
2.5. Неспазването на политиката може да доведе до дисциплинарни мерки и/или правни последици в зависимост от сериозността на нарушението.
3. ИДЕНТИФИЦИРАНЕ НА ИЗИСКВАНИЯТА
3.1. Образователната институция идентифицира и документира изискванията за информационните системи, които включват функционалност, сигурност, наличност, надеждност и изпълнение.
3.2. Изискванията са оценени и приоритизирани, за да се осигури адекватно управление на системите.
4. ПРИДОБИВАНЕ И РАЗРАБОТВАНЕ НА СИСТЕМИТЕ
4.1. Образователната институция следва систематичен процес за придобиране и разработване на информационните системи, съгласно процедурата за сигурно разработване и развитие на софтуерен продукт, който включва идентифициране на изискванията, включително и изискванията за сигурност, проектиране, разработване, тестване и внедряване.
4.2. Сигурността се интегрирана в процеса на придобиване и разработване, като се вземат предвид аспекти като идентификация и управление на риска, контрол на достъпа и криптографска защита.
5. ПОДДРЪЖКА НА СИСТЕМИТЕ
5.1. Образователната институция осигурява поддръжка на информационните системи, за да гарантира тяхната непрекъсната работа, актуализации и поправки на проблеми свързани със сигурността.
5.2. Поддръжката се извършва от квалифицирани служители или от одобрени доставчици на услуги.
6. ИЗПИТВАНЕ И ТЕСТВАНЕ
6.1. Системите са подложени на изпитване и тестване, за да се увери в тяхната функционалност, сигурност и изпълнение.
6.2. Резултатите от изпитванията и тестовете се документират и служат като основа за подобрения на системите.

- **ПОЛИТИКА ЗА УПРАВЛЕНИЕ НА АКТИВИ**

1. ВЪВЕДЕНИЕ И ОБХВАТ
Настоящата политика за управление на активи е разработена в съответствие с изискванията на международни стандарти свързани с мрежовата и информационна сигурност (МИС) и има за цел да предотврати загубата, повредата, кражбата и неоторизиран достъп до активите, които са от съществено значение за работата на образователната институция и информационната сигурност.
2. ДЕФИНИЦИИ
2.1. Активи – включват всички информационни активи, физически активи, софтуерни активи, интелектуална собственост и други активи, които са от значение за образователната институцията.
2.2. Класификация на активите – процесът на идентификация, класификация и етикетиране на активите в съответствие с информацията съдържана в тях.
3. ИДЕНТИФИКАЦИЯ И КЛАСИФИКАЦИЯ НА АКТИВИТЕ
3.1. Образователната институцията идентифицира всички активи, които са от значение за информационната сигурност.

3.2. Активите са класифицирани според техните стойност, значимост и чувствителност на информацията, която съдържат.
3.3. Активите са етикетирани и идентифицирани по начин, който отразява тяхната класификация и сигурност.
4. ЗАЩИТА НА АКТИВИТЕ
4.1. Образователната институцията предприема необходимите мерки за защита на активите от възможни заплахи и рискове.
4.2. Физическите активи са защитени от неоторизиран достъп, повреда или кражба.
4.3. Информационните активи са защитени от неоторизиран достъп, унищожаване, изменение или разкриване.
5. УПРАВЛЕНИЕ НА ДОСТЪПА
5.1. Образователната институцията установява контроли за управление на достъпа до активите, осигурявайки само необходимия достъп на служителите и доставчиците.
5.2. Правата за достъп до активите се базират на принципа на най-малките привилегии, като се осигурява минималният необходим достъп за изпълнение на работните задачи.
6. ФИЗИЧЕСКА И ЛОГИЧЕСКА СИГУРНОСТ
Образователната институцията осигурява физическа и логическа сигурност на активите, включително използването на контролирани достъпи, системи за видеонаблюдение и защитени мрежови връзки.
7. ИЗПОЛЗВАНЕ И ПОДДРЪЖКА НА АКТИВИТЕ
7.1. Активите са използвани и поддържани в съответствие с определените политики и процедури на образователната институцията.
7.2. Предприети са необходимите мерки за поддръжка, обновяване и актуализиране на активите, за да се осигури тяхната непрекъсната функционалност и сигурност.
8. ПРЕМАХВАНЕ НА АКТИВИТЕ
При премахване на активите, образователната институцията предприема мерки за унищожаване или безвредно извеждане на информацията, съхранена на тях, за да се предотврати неоторизиран достъп или възстановяване на информацията.

➢ <u>ПОЛИТИКА ЗА УПРАВЛЕНИЕ НА МОБИЛНИТЕ УСТРОЙСТВА</u>

1. ВЪВЕДЕНИЕ И ОБХВАТ

Настоящата политика за управление на мобилни устройства е разработена в съответствие с изискванията на международни стандарти свързани с мрежовата и информационна сигурност (МИС). Тя има за цел да осигури безопасното и отговорно използване на мобилни устройства в образователната институция и да предотврати рисковете, свързани със загуба, кражба, неоторизиран достъп и злоупотреба с информацията, съхранявана на мобилните устройства.

Тази политика важи за всички мобилни устройства на образователната институция, включително такива на служители, външни изпълнители и други заинтересовани страни, които имат разрешение за достъп до инфраструктурата.

2. ОТГОВОРНОСТИ
2.1. Директорът на образователната институция е отговорен за утвърждаването и поддържането на политиката за управление на мобилни устройства.
2.2. Определеният служител по информационна сигурност е отговорен за мониторинга и оценката на съответствието с политиката, както и за предоставянето на необходимото обучение на служителите относно тази политика.
2.3. Администратора на ИКС осигури поддръжка и конфигуриране на мобилните устройства, които се използват в работната среда.

2.4. Служителите спазват настоящата политика и отговарят на задълженията си за сигурно използване на мобилните устройства.
2.5. Неспазването на политиката може да доведе до дисциплинарни мерки и/или правни последици в зависимост от сериозността на нарушението и действащото законодателство.
3. ОПРЕДЕЛЕНИЯ
3.1. Мобилни устройства - включват, но не се ограничават само до смартфони, таблети, лаптопи и други преносими електронни устройства, които могат да съхраняват, обработват и предават информация.
3.2. BYOD (Bring Your Own Device) - практиката на допускане на служители да използват личните си мобилни устройства за работни цели.

4. УПРАВЛЕНИЕ НА ДОСТЪПА
4.1. За да се осигури контролиран достъп до информацията, мобилните устройства са защитени с пароли, PIN кодове или други механизми за удостоверяване на потребителя.
4.2. Служителите използват акаунти с ограничени права на мобилните устройства.
4.3. Служителите използват силни пароли и не споделят паролите си с други лица.
4.4. Изгубените или откраднати мобилни устройства се докладват незабавно на директора и на администратора на ИКС, за да се предприемат мерки за блокиране или изтриване на съхранената информация.
5. КОНФИГУРАЦИЯ И АКТУАЛИЗАЦИИ
5.1. Мобилните устройства са конфигурирани и актуализирани съгласно предварително определени стандарти и политики на образователната институция.
5.2. Служителите актуализират редовно софтуера на своите мобилни устройства, веднага след като са налични нови ъпдейти и пачове свързани със сигурността.
6. ЗАЩИТА НА ИНФОРМАЦИЯТА
6.1. Чувствителната информация, която се съхранява на мобилните устройства, е шифрована, особено в случаите, когато те се използват извън офиса или при BYOD практика.
6.2. Образователната институция извършва редовно резервно копиране и тестване за възстановяване на информацията, съхранявана на мобилните устройства.
7. БЕЗОПАСНОСТ ПРИ ИЗПОЛЗВАНЕ НА ОБЩЕСТВЕНИ МРЕЖИ
Забранява се използването на обществени отворени Wi-Fi мрежи. За осъществяване на комуникация с инфраструктурата на организацията се използват виртуални частни мрежи (VPN).

➢ <u>ПОЛИТИКА СРЕЩУ ЗЛОВРЕДЕН СОФТУЕР</u>

1. ВЪВЕДЕНИЕ И ОБХВАТ
Настоящата политика срещу зловреден софтуер е разработена в съответствие изискванията на международни стандарти свързани с мрежовата и информационна сигурност (МИС) и има за цел да гарантира сигурността на информационните активи в образователната институция, чрез ефективно управление на достъп и работата с активите.
Тази политика важи за всички информационните активи на образователната институция, включително за служители, външни изпълнители и други заинтересовани страни, които имат разрешение за достъп до инфраструктурата.
2. ОТГОВОРНОСТИ
2.1. Директорът на образователната институция е отговорен за утвърждаването и поддържането на политиката срещу зловреден софтуер.
2.1. Определеният служител по информационна сигурност е отговорен за мониторинга и оценката на съответствието на политиката срещу зловреден софтуер, както и за предоставянето на необходимото обучение на служителите относно тази политика.

2.3. Всички служители и заинтересовани страни спазват настоящата политика срещу зловреден софтуер.
2.4. Неспазването на политиката може да доведе до дисциплинарни мерки и/или правни последици в зависимост от сериозността на нарушението.
3. ОПРЕДЕЛЕНИЯ
3.1. Зловреден софтуер - софтуерни програми, които са създадени с цел да навредят на системата, да извършват неоторизирани действия, да откраднат информация или да причинят друг вид вреди.
3.2. Зловредни вектори - начини, по които зловредни софтуери се разпространяват и попадат в системата, включително електронни пощи, заразени уеб страници, преносими устройства и други.
4. ПРЕДОТВРАТЯВАНЕ НА ЗЛОВРЕДЕН СОФТУЕР
Образователната институция използва различни методи за предотвратяване на зловреден софтуер, включително, чрез:
- Използване на лицензиран и актуализиран софтуер от надеждни източници.
- Използване на механизми за откриване и блокиране на зловреден софтуер, като антивирусни и анти-малуерни решения.
- Редовна актуализация на операционната система и приложенията с пачове за сигурност и ъпдейти.
- Ограничаване на правата за инсталиране на софтуер и достъп до непознати източници.

5. ОТКРИВАНЕ НА ЗЛОВРЕДЕН СОФТУЕР
Образователната институция има механизми и системи за откриване на зловреден софтуер, включително:
- Използване на системи за мониторинг и регистрация на активностите в мрежата и на компютрите.
- Използване на системи за откриване на необичайни и вредни дейности, свързани със зловреден софтуер.
- Редовно сканиране на системата за наличие на зловреден софтуер.

6. РЕАКЦИЯ И УПРАВЛЕНИЕ НА ИНЦИДЕНТИ СЪС ЗЛОВРЕДЕН СОФТУЕР
Образователната институция има процедура за реакция и управление на инциденти свързани с информационната сигурност и зловреден софтуер, включваща:
- Дефиниране на отговорности и роли за откриване, докладване и управление на инциденти.
- Бързи действия за отстраняването, включително и чрез изолация и прекратяване на вредоносния софтуер, когато е открит.
- Извършване на подробен анализ на инцидентите и предприемане на мерки за предотвратяване на бъдещи атаки.
- Обучение на персонала за разпознаване и докладване на инциденти по МИС.

➢ **ПОЛИТИКА ЗА СИГУРНОСТ НА КОМУНИКАЦИИТЕ**

1. ВЪВЕДЕНИЕ И ОБХВАТ
Настоящата политика за сигурност на комуникациите е разработена в съответствие с изискванията на международни стандарти, свързани с мрежовата и информационна сигурност (МИС) и има за цел да гарантира сигурността на комуникациите в образователната институция чрез ефективно управление на хората, които имат достъп до активите за комуникация.

Тази политика важи за всички видове комуникации, включително електронни съобщения, телефонни разговори, факсове и други форми на обмен на информация.

2. ОТГОВОРНОСТИ

2.1. Директорът на образователната институция е отговорен за създаването и поддръжката на актуални политики, свързани със сигурността на комуникациите.

2.2. Определеният служител по информационна сигурност е отговорен за разработването, изпълнението и поддръжката на технически и организационни мерки за сигурност на комуникациите.

2.3. Администратора на ИКС е отговорен за предоставянето на сигурни технически решения за защита на комуникациите, включително за криптиране на данните, защита от зловреден софтуер и други съществени аспекти.

2.4. Служителите спазват политиките и процедурите за сигурност на комуникациите, както и съдействат за осигуряването на сигурността на информацията по време на комуникациите.

2.5. Неспазването на политиката може да доведе до дисциплинарни мерки и/или правни последици в зависимост от сериозността на нарушението.

3. КРИПТИРАНЕ НА КОМУНИКАЦИИТЕ

3.1. Комуникациите, които съдържат чувствителна информация или информация, която изисква поверителност, са криптирани с използването на подходящи и сигурни криптографски алгоритми и протоколи.

3.2. Всички комуникационни канали, които се използват за предаване на чувствителна информация, са сигурни и защитени от неоторизиран достъп и прехвърляне на данни.

4. ЗАЩИТА НА КОМУНИКАЦИОННИТЕ СИСТЕМИ

4.1. В комуникационните системи се използват сигурни конфигурации, които се актуализират редовно, за да се предотвратят възможни уязвимости и злоупотреби.

4.2. Защита от зловреден софтуер, като антивирусни и анти-малуерни решения, се прилагат в комуникационните системи, за да се осигури безопасност на информацията при обмена ѝ.

5. ФИЗИЧЕСКА СИГУРНОСТ НА КОМУНИКАЦИИТЕ

5.1. Физическият достъп до комуникационните инфраструктури, включително мрежови комуникационни устройства и сървъри, е ограничен само до упълномощени лица.

5.2. Защита от физически фактори, като наводнения, пожари и други бедствия, се предоставя за комуникационните системи, за да се предотврати нарушения на цялостността и конфиденциалността на информацията и прекъсване на комуникациите.

➢ <u>ПОЛИТИКА ЗА УПРАВЛЕНИЕ НА ДОСТАВЧИЦИТЕ</u>

1. ВЪВЕДЕНИЕ И ОБХВАТ

Настоящата политика за управление на доставчиците е разработена в съответствие с изискванията на международни стандарти свързани с мрежовата и информационна сигурност (МИС) и има за цел да осигури безопасността на информацията, с която доставчиците имат достъп.

Тази политика важи за всички служители, външни изпълнители и други заинтересовани страни, които имат достъп до информационните активи на образователната институция.

2. ОТГОВОРНОСТИ

2.1. Директорът на образователната институция е отговорен за създаването и поддръжката на актуална политика за управление на доставчиците.

2.2. Определеният служител по информационна сигурност е отговорен за разработването, изпълнението и поддръжката на организационни мерки за управление на доставчиците.

2.3. Определените служители отговорни за взаимоотношенията с трети страни (доставчици) отговарят за спазването на политиката.

2.4. Неспазването на политиката може да доведе до дисциплинарни мерки и/или правни последици в зависимост от сериозността на нарушението.

3. ДЕФИНИЦИИ

3.1. Доставчици - включват физически лица или организации, които предоставят стоки, услуги или технологии на образователната институция.

3.2. Информация - всякаква информация, независимо от формата или носителя, включително тази, съхранявана електронно или на хартия.

4. ОЦЕНКА НА ДОСТАВЧИЦИТЕ

4.1. Образователната институция провежда процес на оценка на доставчиците, преди да им бъде предоставена достъп до информацията на образователната институция (ПРИЛОЖЕНИЕ 1).

4.2. Оценката на доставчиците включва проверка на техните практики свързани със сигурността, политики и процедури, както и тяхната способност да спазват изискванията на стандарти свързани с МИС.

5. СКЛЮЧВАНЕ НА ДОГОВОРИ

5.1. Образователната институция сключва договори с доставчиците, като ясно определят отговорностите и задълженията на страните по отношение на сигурността на информацията.

5.2. Договореностите обхващат въпроси като защита на информацията, управление на достъпа, обработка на данни, съхранение и предаване на информацията, съответствие със законодателството за защита на данните и други изисквания свързани със сигурността на информацията. За целта клаузи свързани със сигурността се залагат във всеки договор (ПРИЛОЖЕНИЕ 2) и изпълнителите и участниците в изпълнението на договора подписват декларация за опазване на информацията (ПРИЛОЖЕНИЕ 3).

5.3. Образователната институция осъществява редовен мониторинг и преглед на дейността на доставчиците, за да се увери, че те спазват политиката за управление на информационната сигурност

ПРИЛОЖЕНИЕ 1

МЕТОДОЛОГИЯ ЗА ОЦЕНКА НА ДОСТАВЧИЦИТЕ

За всеки от критериите се дава оценка от 0 – не съответства на критерия и 1 съответства на критерия.

Крайната /комплексната/ оценка се получава от общия сбор на точките.

При комплексна оценка от 3 и повече точки, доставчикът се одобрява.

При периодична оценка на доставчиците, тези, които дадат като резултат комплексна оценка от 2 или по-малко точки, отпадат от списъка на одобрените доставчици.

Оценяването се извършва най-малко веднъж годишно от комисия, включваща: Ръководител проект, Редактор, Ръководител екип предпечат. Въз основа на оценката се изготвя списък на одобрените доставчици, който се утвърждава от У.

От одобрени доставчици могат да се купят продукти и без да има подписан договор. При големи обеми и многократни доставки може да се пристъпи към сключване на договори за закупуване /за доставка/.

Всички служители от фирмата, които извършват доставките на материали, спазват утвърдения списък на доставчиците на продукти.

Таблица за оценка на доставчици

№	Име на фирмата/ доставчика	Одобрен Да/Не	Критерии за оценяване на доставчик					Обща оценка	Дата на оценката
			Наличие на рекламации до момента от продуктите на доставчика	Цени	Условия на плащане – разсрочено плащане	Срок на доставка	Качество на продукта		
1									
2									
3									
4									

ПРИЛОЖЕНИЕ 2

Конфиденциалност

Чл. …… Всяка от Страните по този Договор се задължава да пази в поверителност и да не разкрива или разпространява информация за другата Страна, станала ѝ известна при или по повод изпълнението на Договора („**Конфиденциална информация**“). Конфиденциална информация включва, без да се ограничава до: обстоятелства, свързани с търговската дейност, техническите процеси, проекти или финанси на Страните, както и ноу-хау, изобретения, полезни модели или други права от подобен характер, свързани с изпълнението на Договора. [Не се смята за конфиденциална информацията, касаеща наименованието на изпълнения проект, стойността и предмета на този Договор, с оглед бъдещо позоваване на придобит професионален опит от ИЗПЪЛНИТЕЛЯ.]

*(**Вариант за дефиниция**: Конфиденциална информация включва, без да се ограничава до: всякаква финансова, търговска, техническа или друга информация, анализи, съставени материали, изследвания, документи или други материали, свързани с бизнеса, управлението или дейността на другата Страна, от каквото и да е естество или в каквато и да е форма, включително, финансови и оперативни резултати, пазари, настоящи или потенциални клиенти, собственост, методи на работа, персонал, договори, ангажименти, правни въпроси или стратегии, продукти, процеси, свързани с документация, чертежи, спецификации, диаграми, планове, уведомления, данни, образци, модели, мостри, софтуер, софтуерни приложения, компютърни устройства или други материали или записи или друга информация, независимо дали в писмен или устен вид, или съдържаща се на компютърен диск или друго устройство.)*

(2) С изключение на случаите, посочени в ал.3 на този член, Конфиденциална информация може да бъде разкривана само след предварително писмено одобрение от другата Страна, като това съгласие не може да бъде отказано безпричинно.

(3) Не се счита за нарушение на задълженията за неразкриване на Конфиденциална информация, когато:

1. информацията е станала или става публично достъпна, без нарушаване на този Договор от която и да е от Страните;

2. информацията се изисква по силата на закон, приложим спрямо която и да е от Страните; или

3. предоставянето на информацията се изисква от регулаторен или друг компетентен орган и съответната Страна е длъжна да изпълни такова изискване;

В случаите по точки 2 или 3 Страната, която следва да предостави информацията, уведомява незабавно другата Страна по Договора.

(4) Задълженията по тази клауза се отнасят до (ИЗПЪЛНИТЕЛЯ/съответната Страна), всички (негови/нейни) поделения, контролирани от (него/нея) фирми и организации, всички (негови/нейни) служители и наети от (него/нея) физически или юридически лица, като (ИЗПЪЛНИТЕЛЯТ/съответната Страна) отговаря за изпълнението на тези задължения от страна на такива лица.

Задълженията, свързани с неразкриване на Конфиденциалната информация остават в сила и след прекратяване на Договора на каквото и да е основание.

Публични изявления

Чл. …… ИЗПЪЛНИТЕЛЯТ няма право да дава публични изявления и съобщения, да разкрива или разгласява каквато и да е информация, която е получил във връзка с извършване на Услугите, предмет на този Договор, независимо дали е въз основа на данни и материали на ВЪЗЛОЖИТЕЛЯ или на резултати от работата на ИЗПЪЛНИТЕЛЯ, без предварителното писмено съгласие на ВЪЗЛОЖИТЕЛЯ, което съгласие няма да бъде безпричинно отказано или забавено.

Чл. …. ИЗПЪЛНИТЕЛЯ декларира, че всички негови служители, ангажирани с дейности по изпълнение на договора, преди започването на дейността им:

1. са поели задължение де не разгласява станалата му известна в изпълнение на договор информация и след приключване изпълнението на настоящия договор и/или след прекратяването на дейността им с ВЪЗЛОЖИТЕЛЯ**;**
2. са преминали подходящо обучение, за да се гарантира, че изпълняват задачите си при спазване на правилата, приложими за защита на личните данни и мрежовата и информационна сигурност.

Чл. … ИЗПЪЛНИТЕЛЯ се задължава да прилага адекватни мерки за мрежова и информационна сигурност в съответствие с действащото законодателство (Закон за киберсигурност, Наредбата за минималните изисквания за мрежова и информационна сигурност, Закон за електронното управление, Наредба за общите изисквания към информационните системи, регистрите и електронните административни услуги) и относимите вътрешни правила на образователната институция.

Чл. … ИЗПЪЛНИТЕЛЯ декларира, че прилага комплексна система от мерки за управление на информационната сигурност и защита на личните данни.

Чл. …. В случай че ИЗПЪЛНИТЕЛЯ установи нарушение на информационната сигурност (инцидент, свързан с информационната сигурност), без ненужно забавяне уведомява писмено ВЪЗЛОЖИТЕЛЯ, като му предоставя цялата налична информация във връзка с нарушението, включително и време за възстановяване на работата, условия за затваряне на инцидент.
Чл. …. С оглед на осигуряването на непрекъсната и висока степен на информационна и мрежова сигурност, ВЪЗЛОЖИТЕЛЯ си запазва правото да извършва проверка за спазване на информационната сигурност на ИЗПЪЛНИТЕЛЯ.

Чл. …. При неспазване на изискванията за сигурност на информацията, включително и договорените срокове, количество и/или качество на услугата, което може да създаде риск за мрежовата и информационната сигурност, ИЗПЪЛНИТЕЛЯ дължи неустойка в размер на ….%.

ПРИЛОЖЕНИЕ 3

Д Е К Л А Р А Ц И Я

ЗА ОПАЗВАНЕ НА ИНФОРМАЦИЯ

Долуподписаният/ та ……..,

ЕГН: ....., в качеството ми на ……., декларирам, че ще пазя в тайна, информацията станалата ми известна във връзка с изпълнението на Договор № / г., съдържаща лични данни, определена като „конфиденциална“, както и друга защитена от закон или по силата на договора информация. За неизпълнение на тези задължения ми е известно, че нося предвидената в съответните нормативни актове отговорност.

Декларирам, че ще пазя в тайна, станалата ми известна информация, относно съдържанието на документация, политики и процедури, начин на функциониране, комуникации, мрежи и информационни системи на образователната институция, както и че няма да разгласявам, използвам или предоставям на трети лица информация във връзка с изпълнението на този договор, с изключение на случаите, когато съм задължен по закон за това.

При обработването на данните се задължавам да спазвам разпоредбите на Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27.04.2016 г. относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни и за отмяна на Директива 95/46/ЕО и Закона за защита на личните данни.

Известна ми е отговорността по Глава девета „а“ „Компютърни престъпления“ от Особената част на Наказателния кодекс, относно достъп до компютърни данни в компютърна система без разрешение, добавяне, промяна, изтриване или унищожаване на компютърна програма или компютърни данни, въвеждане на компютърен вирус в компютърните системи или мрежи на обучителната организация, разпространение на пароли или кодове за достъп до компютърна система или до компютърни данни и от това последва разкриване на лични данни или информация, представляваща държавна или друга защитена от закон тайна.

Декларирам, че ще спазвам изискванията на закона за Киберсигурност и Наредбата за минималните изисквания за мрежова информационна сигурност.

Известна ми е отговорността по чл. 284 от Наказателния кодекс, а именно:

„Длъжностно лице, което във вреда на държавата, на предприятие, организация или на частно лице съобщи другиму или обнародва информация, която му е поверена или достъпна по служба и за която знае, че представлява служебна тайна, се наказва с лишаване от свобода до две години или с пробация.“

Дата: .... 20..... г. **ДЕКЛАРАТОР:** .....

(подпис, изписани саморъчно трите имена или електронен подпис)

➢ ПОЛИТИКА ЗА КЛАСИФИЦИРАНЕ НА ИНФОРМАЦИЯ

1. ВЪВЕДЕНИЕ И ОБХВАТ

Настоящата политика за класифициране на информацията е разработена в съответствие с изискванията на международни стандарти свързани с мрежовата и информационна сигурност (МИС) и има за цел да осигури опазването и защитата на информацията на образователната институция в зависимост от нейната важност и чувствителност.

Тази политика се прилага върху всички активи на образователната институция съдържащи важна за обучителната институция информация.

2. ОТГОВОРНОСТИ

2.1. Директорът на образователната институция е отговорен за утвърждаването и поддържането на политиката за класификация на информацията.

2.1. Определеният служител по информационна сигурност е отговорен за мониторинга и оценката на съответствието на политиката, както и за предоставянето на необходимото обучение на служителите относно тези политики и процедури.

2.3. Всички служители и заинтересовани страни спазват настоящата политика за класифициране на информацията

2.4. Неспазването на политиката може да доведе до дисциплинарни мерки и/или правни последици в зависимост от сериозността на нарушението.

3. ИДЕНТИФИКАЦИЯ НА ИНФОРМАЦИЯТА

3.1. Образователната институция идентифицира информацията, на която е собственик, притежание или е нейна отговорност.

3.2. Идентификацията на информацията се извършва чрез определяне на нейната собственост, отговорност, стойност и чувствителност.

4. КЛАСИФИЦИРАНЕ НА ИНФОРМАЦИЯТА

4.1. Информацията се класифицира в зависимост от нейната стойност и чувствителност.

4.2. Класификацията на информацията включва определяне на нива на класификация, като се вземат предвид критерии като поверителност, цялостност и наличност.

5. ПРАВИЛА ЗА ДОСТЪП И РАЗПРОСТРАНЕНИЕ

5.1. Правилата за достъп до класифицираната информация са определени и документирани в стандартните нива на достъп на образователната институция.

5.2. Достъпът до класифицираната информация е ограничен само до оторизирани служители, които са получили необходимите права и разрешения.

5.3. Разпространението на класифицираната информация се извършва съгласно правилата за достъп и само към упълномощени получатели.

6. ЗАЩИТА НА КЛАСИФИЦИРАНАТА ИНФОРМАЦИЯ

6.1. Образователната институция предприема необходимите мерки за защита на информация в съответствие с нейната класификация.

6.2. Защитата на класифицираната информация включва физически, технически и организационни мерки за предотвратяване на неоторизиран достъп, разкриване, промяна или унищожаване на информацията

➢ ПОЛИТИКА ЗА ПРИЕМЛИВА УПОТРЕБА

1. ВЪВЕДЕНИЕ И ОБХВАТ

Настоящата политика за приемлива употреба е разработена в съответствие с изискванията на международни стандарти свързани с мрежовата и информационна сигурност (МИС) и има за цел да установи правила и регламенти за приемливата употреба на информационните системи и ресурси на образователната институция. Тя се стреми да гарантира ефективното използване на тези ресурси и сигурността на информацията.

Тази политика важи за всички видове комуникации, включително електронни съобщения, телефонни разговори, факсове, срещи и други форми на обмен на информация.

2. ОТГОВОРНОСТИ

2.1. Директорът на образователната институция е отговорно за създаването и поддръжката на актуални политики и процедури, свързани с приемливата употреба.

2.2. Определеният служител по информационна сигурност е отговорен за разработването, изпълнението и поддръжката на технически и организационни мерки за приемлива употреба.

2.3. Потребителите на информационните системи използват ресурсите съобразно предназначението им и съгласно настоящата политика.

2.4. Неспазването на политиката може да доведе до дисциплинарни мерки и/или правни последици в зависимост от сериозността на нарушението.

3. УПОТРЕБА НА ИНФОРМАЦИОННИТЕ СИСТЕМИ И АКТИВИ

3.1. Информационните системи се използват само за служебни цели, свързани с работата на образователната институция.

3.2. Забранява се използването на информационните системи за незаконни, неморални или неприемливи дейности, които могат да навредят на репутацията на образователната институция или нарушат законодателството.

3.3. Потребителите се грижат за сигурността на своите данни, пароли и други идентификационни средства, за да се предотврати неоторизиран достъп до системите.

3.4. Потребителите използват само силни пароли (съдържащи голяма и малка буква, символ и цифра и са големина поне 10 символа). За административните акаунти паролата е с големина поне 15 символа.

3.5. Паролите се сменят периодични на максимум 6 месеца.

3.6. Забранява се използването USB флаш памет и други външни носители на информация на служебните компютри в обучителните зали. За останалите компютри е разрешено използването само служебни цели, в рамките на инфраструктурата, след задължително тестване с антивирусна програма.

4. ПРИЕМЛИВО ИЗПОЛЗВАНЕ НА ИНТЕРНЕТ И ЕЛЕКТРОННАТА ПОЩА

4.1. Използването на интернет и електронната поща се извършва съобразно целите на образователната институция при спазването на утвърдените политики.

4.2. Забранява се използването на интернет и електронната поща за разпространение на незаконна или неподходяща информация или за извършване на действия, които могат да причинят вреда на образователната институция или на други лица.

4.3. Забранява се използването на служебна електронна поща за лични цели.

4.4. Забранява се посещение на интернет сайтове съдържащо насилие, порнографски материали или са в нарушение на авторското право.

5. МОНИТОРИНГ И КОНТРОЛ

5.1. Образователната институция мониторира и контролира използването на информационните системи и ресурси, съобразно приложимите закони и правила за защита на личните данни.

5.2. Мониторингът включва записване на активността на потребителите, проверка на съдържанието на комуникациите и използването на специализирани инструменти за сигурност.

➢ ПОЛИТИКА ЗА ЧИСТО БЮРО

1. ВЪВЕДЕНИЕ И ОБХВАТ

Настоящата политика за чисто бюро е разработена в съответствие с изискванията на международни стандарти свързани с мрежовата и информационна сигурност (МИС) и има за цел да установи правила и процедури за поддържане на чистотата и безопасността на работните места и работната среда в образователната институция. Тя се стреми да гарантира съхранението на чувствителна информация и подобряването на работната ефективност.

2. ОТГОВОРНОСТИ

2.1. Директорът е отговорен за утвърждаването и поддържането на политиката за чисто бюро и осигурява средствата и ресурсите, необходими за поддръжка на безопасността на информацията в образователната институция.

2.2. Определеният служител по информационна сигурност е отговорен за мониторинга за спазването и за предоставянето на необходимото обучение на служителите относно тази политика.

2.3. Всички служители са отговорни за поддържането на политиката на своите работни места.

2.4. Неспазването на политиката може да доведе до дисциплинарни мерки и/или правни последици в зависимост от сериозността на нарушението и действащото законодателство.

3. ПОДДРЪЖКА НА РАБОТНИТЕ МЕСТА

3.1. Работните места са поддържани в чисто и организирано състояние.

3.2. Излишни и ненужни предмети са премахвани от работните места и се съхраняват правилно.

3.3. Работните места са оборудвани с контейнери за отпадъци, които се изпразват редовно.

4. СЪХРАНЕНИЕ НА ИНФОРМАЦИЯ

4.1. Документите и информацията се съхраняват в подходящи и безопасни условия.

4.2. Чувствителната информация се съхранявана в заключени шкафове или сейфове.

4.3. Чувствителната информация, като пароли, лични данни и др. се съхраняват на сигурно място и не се оставят без надзор върху бюрата.

4.4. Всички поверителни документи, които са идентифицирани да бъдат унищожени се третират съгласно Инструкцията за унищожаване на информацията.

5. БЕЗОПАСНОСТ И ЧИСТОТА

5.1. Използването на пожарогасители и други средства за спешни ситуации е достъпно за служителите.

➢ ПОЛИТИКА ЗА ОБРАБОТКА НА МЕДИИ

1. ВЪВЕДЕНИЕ И ОБХВАТ

Настоящата политика за обработка на медиите е разработена в съответствие с изискванията на международни стандарти свързани с мрежовата и информационна сигурност (МИС) и има за цел защитата на информацията от неоторизиран достъп, загуба или повреда.

Тази политика важи за всички медии на образователната институция, включително за служители, външни изпълнители и други заинтересовани страни, които имат разрешение за достъп до медии на обучителната организация.

2. ОТГОВОРНОСТИ

2.1. Директорът на образователната институция е отговорен за утвърждаването и поддържането на политиката за обработка на медиите.

2.1. Определеният служител по информационна сигурност е отговорен за мониторинга и оценката на съответствието на политиката за обработка на медиите, както и за предоставянето на необходимото обучение на служителите относно тази политика.

2.3. Всички служители и заинтересовани страни спазват настоящата политика за обработка на медиите.
2.4. Неспазването на политиката може да доведе до дисциплинарни и административни мерки и/или правни последици в зависимост от сериозността на нарушението и съгласно действащото законодателство.
3. ОПРЕДЕЛЕНИЕ НА МЕДИИ
Под медии се разбират физически носители на информация, включително хартиени документи, CD, DVD, USB флаш устройства, външни твърди дискове, фотографии и други подобни носители.
4. КЛАСИФИЦИРАНЕ И МАРКИРАНЕ
Всички медии са класифицирани съгласно политиката за класифициране на информацията и са маркирани с подходящи етикети, указващи степента на поверителност, а при необходимост и други релевантни информации.
5. ФИЗИЧЕСКА СИГУРНОСТ
5.1. Медиите с висока степен на поверителност са съхранявани в допълнително осигурени помещения или сейфове.
6. ОБРАБОТКА И ИЗПОЛЗВАНЕ
6.1. Обработката и използването на медии са извършвани само от упълномощени служители и в рамките на техните работни отговорности.
6.2. Забранява се копирането или прехвърлянето на информация от медии без предварително разрешение от компетентните лица.
7. УНИЩОЖЕНИЕ И ИЗХВЪРЛЯНЕ
7.1. Медиите с висока степен на поверителност се унищожават по сигурен начин, когато вече не са необходими или съответната информация е била прехвърлена на друг носител.
7.2. Унищожаването на медиите с висока степен на поверителност се извършва чрез физическо унищожаване или друг подходящ метод съгласно инструкцията за унищожаване на информацията.
7.3. При необходимост, изхвърлянето на медиите с висока степен на поверителност може да се извърши след като се гарантира, че информацията не може да бъде възстановена.

➢ КРИПТОГРАФСКА ПОЛИТИКА

1. ВЪВЕДЕНИЕ И ОБХВАТ
Настоящата криптографска политика е разработена в съответствие с изискванията на международни стандарти свързани с мрежовата и информационна сигурност (МИС) и има за цел да гарантира сигурността на чувствителната информация в образователната институция. Тази политика важи за всички служители, външни изпълнители и други заинтересовани страни, които имат достъп до информационните активи на образователната институция.
2. ОТГОВОРНОСТИ
2.1. Директорът на образователната институция е отговорен за утвърждаването и поддържането на криптографската политика.
2.2. Определеният служител по информационна сигурност е отговорен за мониторинга и оценката на съответствието с политиката, както и за предоставянето на необходимото обучение на служителите относно тази политика.
2.3. Служителите спазват всички изисквания на криптографската политика.
2.4. Неспазването на политиката може да доведе до дисциплинарни мерки и/или правни последици в зависимост от сериозността на нарушението.
3. КРИПТОГРАФСКА ЗАЩИТА
3.1. Използването на криптографска защита е задължително за обработката, съхранението и комуникацията на информация с висока или умерена степен на поверителност.

3.2. Криптографските механизми, алгоритми и ключове се избират и прилагат в съответствие със стандартите и препоръките, които гарантират сигурността на информацията.

4. УПРАВЛЕНИЕ НА КЛЮЧОВЕТЕ

4.1. Генерирането, съхранението, управлението и унищожаването на криптографските ключове се извършвани съгласно добрите практики и процедури, осигуряващи тяхната защита от неоторизиран достъп и загуба.

4.2. Криптографските ключове са генерирани с достатъчна дължина и случайност, като се използват сигурни методи и алгоритми.

5. УДОСТОВЕРЯВАНЕ И ИДЕНТИФИКАЦИЯ

5.1. Криптографските механизми са използвани за удостоверяване на идентичността на комуникиращите страни и за създаване на защитени канали за комуникация.

5.2. Използването на цифрови сертификати и удостоверяване на ключовете е регулирано от съответните практики.

➢ <u>ПОЛИТИКА УПРАВЛЕНИЕ НА АРХИВИРАНЕТО</u>

1. ВЪВЕДЕНИЕ И ОБХВАТ

Настоящата политика за управление на архивирането е разработена в съответствие с изискванията на международни стандарти свързани с мрежовата и информационна сигурност (МИС) и има за цел да гарантира запазването на цялостността, достъпността, конфиденциалността и дългосрочната запазеност на информацията.

Тази политика важи за всички служители, външни изпълнители и други заинтересовани страни, които имат достъп до информационните активи на образователната институция.

2. ОТГОВОРНОСТИ

2.1. Директорът на образователната институция е отговорно за създаването и поддръжката на актуална политика, свързани с архивирането.

2.2. Определеният служител по информационна сигурност е отговорен за разработването, изпълнението и поддръжката на технически и организационни мерки за управление на архивирането.

2.3. Администраторът на ИКТ осигурява извършването на архивирането съгласно настоящата политика.

2.4. Неспазването на политиката може да доведе до дисциплинарни мерки и/или правни последици в зависимост от сериозността на нарушението.

3. ДЕФИНИЦИИ

Архивирането се е процесът на запазване и съхранение на информацията на дългосрочна основа, осигурявайки ѝ подходяща защита и достъпност.

4. КЛАСИФИЦИРАНЕ НА ИНФОРМАЦИЯТА

4.1. Информацията се класифицирана и маркирана съгласно политиката за класифициране на информацията преди да бъде архивирана.

4.2. С класификацията се определя нивото на поверителност на архивираната информация.

5. ПРОЦЕДУРИ ЗА АРХИВИРАНЕ

5.1. Архивирането се извършва съгласно утвърдените практики, които гарантират запазването на цялостността, достъпността и сигурността на информацията.

5.2. Архивните носители са избирани и използвани в съответствие със стандартите и препоръките за дългосрочно съхранение на информацията.

5.3. Копията на информация да са етикетирани по начин, указващ еднозначно поне каква е информацията, за коя система, какъв метод е използван за създаване на копието, дата и час;

5.4. Копията на чувствителна информация да са в криптиран вид или поне защитени с парола;

5.5. Копията на информацията се съхраняват на записващо устройство.

5.6. Едно от копията на критична за дейността информация се съхранява off-line в помещение-Атхив;
5.7. Да се прави регулярна проверка на годността на резервните копия, дали те изпълняват целите, за които са създадени, и постига ли се необходимото време за възстановяване.
5.8. Процесите по архивиране се отразяват в приложение 1 и в Дневника на администратора.

6. ФИЗИЧЕСКА СИГУРНОСТ

6.1. Архивните материали и носители са съхранявани в сигурни помещения, където достъпът е ограничен само до упълномощени служители.
6.2. Защита се осигурява от физически фактори, като пожар, наводнение и кражба, които могат да застрашат цялостността и достъпността на архивните материали.

7. УПРАВЛЕНИЕ НА ДОСТЪПА

7.1. Само упълномощени служители имат достъп до архивните материали и информация.
7.2. Достъпът до архивите е контролиран и ограничен, съобразно принципа на най-малките привилегии.

ПРИЛОЖЕНИЕ 1

ПРОЦЕСИ ИДЕЙСТВИЯ ПРИ АРХИВИРАНЕ

	Система 1 ***информацията (бази данни, конфигурационни файлове, имиджи на системи и др.), която ще се резервира и/или архивира***	***Система 2*** ***информацията (бази данни, конфигурационни файлове, имиджи на системи и др.), която ще се резервира и/или архивира***
1. Технологията, която ще се използва за архивиране и резервиране	Архивиращо устройство	флаш памет
2. Типът на резервиране (частично, пълно и др.)	пълно	пълно
3. Периодът на извършване на архивирането и резервирането	ежедневно	при необхомимост/в края на учебната година
4. Броят на копията, които ще се правят	копие на всеки документ	-
5. Времето за съхраняване на всяко копие съгласно изискванията на	според Наредба №8 за документите в сферата на образованието	според Наредба №8 за документите в сферата на образованието

нормативните актове и оценката на риска		
6. Мястото на съхраняване на всяко копие	в арживноо устройство	помещение-Архив
7. Начинът на защита от неправомерен достъп (физическа и логическа)	поддържа се от специалист в областа	в поещението е осигурена необходимата температура и влажност
8. Случаите на използване	ежедневно	при необходимост
9. Лицето, което дава разрешение за използването	директор/ гл.счетоводител	

- **<u>ПОЛИТИКА ЗА РЕГИСТРИРАНЕ И НАБЛЮДЕНИЕ</u>**

1. ВЪВЕДЕНИЕ И ОБХВАТ

Настоящата политика за регистриране и наблюдение е разработена в съответствие с изискванията на международни стандарти свързани с мрежовата и информационна сигурност (МИС) и има за цел да установи рамката и процедурите за ефективно регистриране и наблюдение на информационните активи и събитията свързани със сигурността в образователната институция.

2. ОТГОВОРНОСТИ

2.1. Директорът на образователната институция е отговорно за създаването и поддръжката на актуални политика за регистриране и наблюдение.

2.2. Определеният служител по информационна сигурност е отговорен за разработването, изпълнението и поддръжката на технически и организационни мерки за регистриране и наблюдение

2.3. Администратора на ИКС е отговорен за регистрирането и наблюдението на информационните активи и събития свързани със сигурността.

2.4. Всички служители сътрудничат активно и да спазват политиката и процедурите за регистриране и наблюдение.

2.5. Неспазването на политиката може да доведе до дисциплинарни мерки и/или правни последици в зависимост от сериозността на нарушението.

3. РЕГИСТРИРАНЕ НА ИНФОРМАЦИОННИТЕ АКТИВИ

3.1. Образователната институция поддържа актуален регистър на информационните активи, включително хардуер, софтуер, мрежови компоненти и данни.

3.2. За всеки информационен актив са документирани минимум следните данни: идентификатор (инвентарен номер), наименование и основни характеристики, отговорен служител, класификация на информацията, местоположение и статус.

4. РЕГИСТРИРАНЕ НА СЪБИТИЯТА СВЪРЗАНИ СЪС СИГУРНОСТТА

4.1. Образователната институция поддържа система за регистриране на събития свързани със сигурността, която позволява откриването, записването и анализа на инциденти и нарушения на сигурността.

4.2. За всеки регистриран инцидент свързани със сигурността се документират минимум следните данни: дата и час на откриване, подател на сигнала, описание на инцидента,

засегнати активи, предприети действия, отговорните лица за управлението на инцидента и извлечени поуки.

5. МОНИТОРИНГ И НАБЛЮДЕНИЕ

5.1. Образователната институция извършва систематичен мониторинг и наблюдение на информационните активи и събития свързани със сигурността, за да открие евентуални атаки, нарушения или несъответствия.

5.2. При възможност използва средства за мониторинг, като IDS и/или IPS системи, системи за анализ на събития на логовете, за регулярното и им проверяване.

6. АНАЛИЗ И РЕАГИРАНЕ

6.1. Регистрираните събития свързани със сигурността се анализират, за да се определи тяхната сериозност и възможните последици за информационната сигурност.

6.2. При откриване на нарушение или инцидент свързани със сигурността, се предприема незабавна реакция, включително изолиране на засегнатите активи, блокиране на неоторизиран достъп и възстановяване на информационната сигурност.

7. СЪХРАНЕНИЕ НА РЕГИСТРИРАНАТА ИНФОРМАЦИЯ

7.1. Регистрираната информация за информационните активи и събития свързани със сигурността се съхранявана в сигурна и надеждна среда, където е достъпна само за отговорните лица.

7.2. Съхранението на регистрираната информация се извършва в съответствие с приложимите правила и регулации относно защитата на данните.

➢ ПОЛИТИКА ЗА УПРАВЛЕНИЕ НА УЯЗВИМОСТ И КОРЕКЦИИ

1. ВЪВЕДЕНИЕ И ОБХВАТ

Настоящата политика за управление на уязвимости и корекции определя принципите и процедурите, които образователната институция прилага за идентифициране, оценка, управление и отстраняване на уязвимости в информационните системи и прилагане на корекции, когато е необходимо.

Целта на политиката е да гарантира, че образователната институция разполага със съответните мерки за сигурност, за да предотврати експлоатацията на уязвимости и да реагира ефективно в случай на открити уязвимости.

2. ОТГОВОРНОСТИ

2.1. Директорът на образователната институция е отговорен за утвърждаването и поддържането на политиката за управление на уязвимости и корекции.

2.2. Определеният служител по информационна сигурност е отговорен за мониторинга и оценката на съответствието на политиката за управление на уязвимости и корекции, както и за предоставянето на необходимото обучение на служителите относно тази политика.

2.3. Администратора на ИКС е отговорен за техническото изпълнение на процеса по управление на уязвимости и корекции.

2.4. Всички служители и заинтересовани страни спазват настоящата политика за управление на уязвимости и корекции

2.4. Неспазването на политиката може да доведе до дисциплинарни мерки и/или правни последици в зависимост от сериозността на нарушението.

3. ИДЕНТИФИЦИРАНЕ НА УЯЗВИМОСТИ

3.1. Образователната институция извършва систематично и редовно идентифициране на уязвимости в информационните системи, включително хардуерните и софтуерните компоненти, операционните системи, приложенията и мрежовата инфраструктура.

3.2. Идентифицирането на уязвимости включва използване на автоматизирани инструменти за сканиране и тестване на сигурността, както и ръчни проверки и анализ.

4. ОЦЕНКА НА УЯЗВИМОСТИ

4.1. Образователната институция оценява и класифицира откритите уязвимости според техния потенциален риск и въздействие върху информационната сигурност на образователната институция.
4.2. Оценката на уязвимости включва анализ на възможните атаки, рисковите сценарии и въздействието върху поверителността, цялостността и наличността на информацията.
5. УПРАВЛЕНИЕ НА УЯЗВИМОСТИ
Образователната институция разработва и поддържа практики за управление на уязвимости, които включват следните дейности:
- Приоритизиране на уязвимостите въз основа на рисковия им потенциал и въздействие.
- Дефиниране и изпълнение на коригиращи мерки, включително пачове, ъпдейти и поправки свързани със сигурността.
- Изграждане и поддържане на процес за непрекъснато наблюдение и отстраняване на уязвимостите.
- Следене и оценка на ефективността на предприетите мерки за управление на уязвимости.

6. РЕАГИРАНЕ НА УЯЗВИМОСТИ
6.1. Образователната институция разполага с механизми за бързо реагиране и отстраняване на открити уязвимости.
6.2. Реакцията на уязвимости включва следните дейности:
- Документиране и незабавно уведомяване на Директора на образователната институция за откритите уязвимости.
- Планиране и прилагане на корекции в сътрудничество с отговорните служители/екипи или доставчици на софтуерни и хардуерни решения.
- Извършване на редовен мониторинг и проверка за установяване на ефективността на коригиращите мерки.

➢ <u>ПОЛИТИКА ЗА УПРАВЛЕНИЕ НА ПРОМЕНИ</u>

1. ВЪВЕДЕНИЕ И ОБХВАТ
Настоящата политика за управление на промените е разработена в съответствие изискванията на международни стандарти свързани с мрежовата и информационна сигурност (МИС) и има за цел да гарантира сигурността на информационните активи при промени в образователната институция чрез ефективно управление на процесите.
Тази политика важи за всички информационните активи на образователната институция, включително за служители, външни изпълнители и други заинтересовани страни, които имат разрешение за достъп до инфраструктурата на образователната институция
2. ОТГОВОРНОСТИ
2.1. Директорът на образователната институция е отговорен за създаването на политика, която се отнася до управление на промените.
2.2. Определеният служител по информационна сигурност е отговорен за мониторинга и оценката на съответствието на процеса и политиката за управлението на промените.
2.3. Всички служители сътрудничат активно и спазват политиката за управление на промените.
2.4. Неспазването на политиката може да доведе до дисциплинарни мерки и/или правни последици в зависимост от сериозността на нарушението.
3. ОПРЕДЕЛЕНИЕ НА ПРОМЕНИТЕ
3.1. Промени се определят като всяка модификация, добавяне или изтриване на компоненти на информационните системи, включително хардуер, софтуер, мрежови компоненти, процеси и процедури.

3.2. Промени могат да бъдат инициирани от вътрешни или външни фактори, включително нужди на образователната институция, законодателство, технологични изисквания или рискове свързани със сигурността.

4. ПРОЦЕС НА УПРАВЛЕНИЕ НА ПРОМЕНИТЕ

4.1. За всяка промяна е изготвен план за промяна - Приложение 1, който включва описание на промяната, засегнатите компоненти, рисковете и мерките за сигурност.

4.2. Промените са одобрени предварително от директора или упълномощеното лице, отговарящи за управлението на промените.

4.3. Изпълнението на промените е документирано и следено (Приложение 2), за да се гарантира успешната им имплементация и да се избегнат нежелани последици.

4.4. При необходимост, се извършена оценка на въздействието на промените върху информационната сигурност и се предприемат съответни мерки за намаляване на риска.

ПРИЛОЖЕНИЕ 1

ДЕТСКА ГРАДИНА „ПЪРВИ ЮНИ”, ГР. КЮСТЕНДИЛ,
КВ. ЗАПАД, ТЕЛ.: 078/ 55 20 73, e-mail: info-100060@edu.mon.bg

ПЛАН ЗА ПРОМЯНА

Обновление на софтуер за видеонаблюдение .....

(описание на промяната)

Обновлението ще се извърши на *.(например 25.09.2023 г. от Иван Иванов)* на сървъра за видеонаблюдение .....

(засегнатите компоненти)

Неправилна работа на видеонаблюдението .....

(рискове)

Направен архив с цел възстановяване на предната версията преди обновлението .....

(мерките за сигурност)

Утвърдил: .....

Гр./с. ..... **Дата**: .... 20..... г.

ПРИЛОЖЕНИЕ 2

ДЕТСКА ГРАДИНА „ПЪРВИ ЮНИ”, ГР. КЮСТЕНДИЛ,
КВ. ЗАПАД, ТЕЛ.: 078/ 55 20 73, e-mail: info-100060@edu.mon.bg

ПРОТОКОЛ ЗА ИЗВЪРШЕНА ПРОМЯНА

Днес .... 20..... г. *(дата)* г-н/г-жа ..... *(име и фамилия*), на длъжност ..... извърши обновление на сървъра за видеонаблюдение.

Софтуера бе успешно имплементиран, без нежелани последици.

Извършено е следното:

.....

.....

.....

.....

(описание на извършените промени и резултата от тях)

Извършил промяната: ....., ...

(име и фамилия) *(подпис)*

Приел промяната: ....., ...

(име, фамилия и длъжност) *(подпис)*

Гр./с. ..... **Дата**: .... 20..... г.

➢ ПОЛИТИКА ЗА УПРАВЛЕНИЕ НА ИНЦИДЕНТИ

1. ВЪВЕДЕНИЕ И ОБХВАТ

Настоящата политика за управление на инциденти определя подхода и процедурите, които образователната институция използва за откриване, реагиране, регистриране и решаване на инциденти свързани с информационната сигурност. Политиката за управление на инциденти обхваща всички информационни инциденти, които могат да засегнат активите на образователната институция, включително нарушения на сигурността, загуби на данни, злоупотреби, компрометиране на системи и други подобни инциденти.

2. ЦЕЛИ

Целите на политиката за управление на инциденти включват:

- Бързо откриване и реагиране на инциденти, свързани с информационната сигурност.
- Минимизиране на въздействието на инцидентите върху работата и активите на образователната институция.
- Регулярно регистриране и анализ на инциденти свързани с информационната сигурност.
- Подобряване на мерките за предотвратяване на бъдещи инциденти.
- Съответствие със съответните законодателство и регулации за отчетност и известяване на инциденти.

3. ПРОЦЕДУРИ ЗА УПРАВЛЕНИЕ НА ИНЦИДЕНТИ

Образователната институция е разработила и поддържа процедура за управление на инциденти, която включва:

- Класификация и приоритизация на инцидентите.
- Докладване, регистриране и известяване на инцидентите.
- Анализ и оценка на въздействието на инцидентите.
- Предприемане на коригиращи мерки и решаване на инцидентите.
- Документиране и архивиране на информацията относно инцидентите.
- Извършване на регулярни прегледи и оценки на ефективността на процедурите.

4. ИЗВЕСТЯВАНЕ И СЪТРУДНИЧЕСТВО

4.1. В случай на възникване на инциденти свързани с информационната сигурност, се изисква активно известяване на подходящите заинтересовани страни, включително директор на образователната институция, съответните отговорни служители и компетентните органи в съответствие със законодателството и регулациите.

4.2. Образователната институция си сътрудничи с външни инстанции, като правоохранителни органи, специализирани фирми и други организации, за да се разследват и разрешават информационни инциденти.

5. СПАЗВАНЕ НА ПОЛИТИКАТА

5.1. Всички служители и заинтересовани страни спазват настоящата политика и свързаните процедури за управление на инциденти.

5.2. Неспазването на политиката може да доведе до дисциплинарни мерки или правни последици в зависимост от сериозността на нарушението.

6. ОЦЕНКА И ПОДОБРЕНИЕ

Настоящата политика и свързаните процедура и съпътстващите документи към тях се преглежда и актуализира периодично, поне веднъж годишно. Резултатите от прегледите и оценките се документират и използват за подобряване на процесите на управлението на инциденти.

ПОЛИТИКА ЗА ОДИТ НА ИНФОРМАЦИОННАТА СИСТЕМА ЗА СИГУРНОСТ

1. ВЪВЕДЕНИЕ И ОБХВАТ

Настоящата политика за одит на информационната сигурност определя принципите и процедурите, които образователната институция прилага за извършване на одити на информационната сигурност, с цел оценка на ефективността и съответствието на мерки за сигурност и контроли, дефинирани във вътрешните документи и националните изисквания. Образователната институция осигурява систематични и независими одити на информационната сигурност в съответствие с националното законодателство и международни стандарти.

Одитите на информационната сигурност обхващат всички релевантни аспекти на информационната сигурност, включително физическата сигурност, управлението на достъпа, криптографията, уязвимостите и инцидентите на информационната сигурност.

2. ОТГОВОРНОСТИ

2.1. Директорът на образователната институция е отговорен за утвърждаването и поддържането на политиката за одит на информационната сигурност.

2.2. Определеният служител по информационна сигурност е отговорен за мониторинга и оценката на съответствието на политиката, както и за предоставянето на необходимото обучение на служителите относно тази политика.

2.3. Всички служители и заинтересовани страни спазват настоящата политика за одит на информационната сигурност.

2.4. Неспазването на политиката може да доведе до дисциплинарни мерки и/или правни последици в зависимост от сериозността на нарушението.

3. ЦЕЛИ НА ОДИТА

Одитите на информационната сигурност имат следните цели:

- Оценка на съответствието на информационната сигурност със законодателството, регулациите и стандартите.
- Оценка на ефективността на мерките за сигурност и контролите.
- Идентифициране на рискове и уязвимости в информационната сигурност.
- Предоставяне на препоръки и коригиращи действия за подобрение на информационната сигурност.

4. ПЛАНИРАНЕ И ИЗПЪЛНЕНИЕ НА ОДИТИТЕ

4.1. Образователната институция поддържа политика за одит на информационната сигурност включваща и планиране на одити – Приложение № 1.

4.2. Планирането на одитите включва дефиниране на обхват, цели, методи и ресурси, необходими за изпълнение на одитите.

4.3. Одитите се извършвани от независими и компетентни одитори на информационната сигурност – никой не проверява съм собствената си дейност.

4.4. Одитите се извършват в съответствие със стандарт БДС EN ISO 19011 "Указания за извършване на одит на системи за управление", изискванията на стандарт БДС EN ISO/IEC 17020 "Оценяване на съответствието".

4.5. Одитите се провеждат периодично, но не по-рядко от веднъж в годината.

4.6. Одитите се извършват от лица, притежаващи квалификация в областта на контрола и имащи необходимите знания и професионален опит в областта на мрежовата и информационната сигурност.

4.7. Одиторът не може да одитира собствената си дейност.

4.8. Резултатите от одита са с класификация TLP-AMBER.

5. ДОКЛАДВАНЕ И СЛЕДЕНЕ

5.1. След завършване на одитите, се предостави писмен доклад с резултатите и препоръките към управлението на образователната институция.

5.2. Директорът на образователната институция разглежда доклада и предприема необходимите действия за подобрение на информационната сигурност.
5.3. Резултатите от одитите се следят, като се извършва периодичен преглед на приетите коригиращи мерки и подобрения.

6. ПРЕГЛЕД И ПОДОБРЕНИЕ

Политиката за одит на информационната сигурност се преглежда и актуализира периодично, поне веднъж годишно. Резултатите от прегледите и оценките се документират и използват за подобряване на процесите на одит на информационната сигурност.

ПРИЛОЖЕНИЕ 1

ПЛАН ЗА ОДИТИ
на

ДЕТСКА ГРАДИНА „ПЪРВИ ЮНИ”, ГР. КЮСТЕНДИЛ,
КВ. ЗАПАД, ТЕЛ.: 078/ 55 20 73, e-mail: info-100060@edu.mon.bg

……
(обхват на изпълнение на одита)
…….
(цели на изпълнение на одита)

…….
(методи и ресурси, необходими за изпълнение на одита)

Утвърдил: ....., ..., ...
(име и фамилия) (длъжност) (подпис)

Гр./с. …… Дата: ….. . …… 2023 г.

- **<u>ПОЛИТИКА ЗА ИЗПОЛЗВАНЕ НА ОБЛАЧНИ УСЛУГИ</u>**

1. ВЪВЕДЕНИЕ И ОБХВАТ

Настоящата политика за използване на облачни услуги е е разработена в съответствие с изискванията на международни стандарти свързани с мрежовата и информационна сигурност (МИС) има за цел да установи рамката и процедурите за безопасно и отговорно използване на облачни услуги от страна на образователната институция.

Тази политика важи за всички служители, външни изпълнители и други заинтересовани страни, които имат достъп до информационните активи на образователната институция.

2. ОТГОВОРНОСТИ

2.1. Директорът на образователната институция е отговорен за утвърждаването и поддържането на политиката за използване на облачните услуги.

2.2. Определеният служител по информационна сигурност е отговорен за мониторинга и оценката на съответствието с политиката, както и за предоставянето на необходимото обучение на служителите относно тези политики и процедури

2.3. Всички служители на образователната институция са задължени да спазват настоящата политика и съответните процедури и насоки за използване на облачни услуги.

2.4. Неспазването на политиката може да доведе до дисциплинарни мерки и/или правни последици в зависимост от сериозността на нарушението.

3. ДЕФИНИЦИИ

3.1. Облачни услуги - предоставяне на достъп до информационни технологии и ресурси, като хардуер, софтуер и мрежова инфраструктура, чрез интернет.

3.2. Доставчик на облачни услуги - трета страна, което предоставя облачни услуги на образователната институция.

4. КЛАСИФИКАЦИЯ НА ИНФОРМАЦИЯТА

4.1. Информацията, която се обработва и съхранява в облака, е предварително класифицирана в съответствие с инструкцията за обозначаване на информацията.

4.2. Класификацията на информацията определя нейното ниво на поверителност и изискванията за защита.

5. ИЗБОР НА ДОСТАВЧИК НА ОБЛАЧНИ УСЛУГИ

5.1. При избора на доставчик на облачни услуги, образователната институция извършва преглед на сигурността на доставчика, включително неговите мерки за защита на информацията и съответствието му със стандарти и регулации за информационна сигурност.

5.2. При необходимост, се сключва договор или споразумение с доставчика на облачни услуги, в който да бъдат уточнени отговорностите и задълженията на двете страни относно защитата на информацията.

6. ОГРАНИЧЕНИЯ НА ИЗПОЛЗВАНЕТО НА ОБЛАЧНИ УСЛУГИ

6.1. Използването на облачни услуги се съобразява с политиките и процедурите на образователната институция за информационна сигурност.

6.2. Забранява се използването на облачни услуги без одобрение от диредкора и без съответствие с изискванията за сигурност на образователната институция.

7. СИГУРНОСТ НА ИНФОРМАЦИЯТА В ОБЛАКА

7.1. Информацията, предавана към и съхранявана в облака, е защитена с подходящи мерки за сигурност, включително криптиране, контрол на достъпа и мониторинг на събитията.

7.2. Доставчикът на облачни услуги предоставя подробна информация относно сигурността на своите услуги и да спазва съответните стандарти и регулации.

8. МОНИТОРИНГ И ОДИТ НА ОБЛАЧНИЯ ДОСТАВЧИК

8.1. Образователната институция осигурява мониторинг на дейността на доставчика на облачни услуги, включително проверка на съответствието му със изисквания за сигурност и условията, посочени в договора или споразумението.
8.2. Правят се периодични одити на доставчика на облачни услуги, за да се установи съответствието му със стандартите за сигурност и да се оцени ефективността на предприетите мерки за защита на информацията.
9. ОБУЧЕНИЕ НА ПЕРСОНАЛА
9.1. Всички служители, които използват облачни услуги, са обучени относно правилното и безопасно използване на тези услуги.
9.2. Обучението включва информация относно рисковете, свързани с облачните услуги, и процедурите за защита на информацията при използването им.
10. ИНЦИДЕНТИ И ИНЦИДЕНТНО УПРАВЛЕНИЕ
10.1. Образователната институция разполага с процедури и планове за инцидентно управление, които да включват специфични мерки за случаи на инциденти, свързани с облачни услуги.
10.2. В случай на съобщаване за инцидент, свързан с облачни услуги, са предприети незабавни действия за прекратяване на инцидента, ограничаване на щетите и възстановяване на нормалното функциониране.

- **<u>ПОЛИТИКА ЗА ПРЕГЛЕД ОТ РЪКОВОДСТВОТО ЗА ЕФИКАСНОСТТА НА СИСТЕМАТА ЗА УПРАВЛЕНИЕ НА ИНФОРМАЦИОННАТА СИГУРНОСТ</u>**

1. ВЪВЕДЕНИЕ И ОБХВАТ
Настоящата политика за преглед от ръководството за ефикасността на системата за управление на информационната сигурност обхваща последователността от действия и отговорностите за провеждане на преглед от страна на ръководството на образователната институция за ефикасността на Системата за управление на информационната сигурност. Целта на прегледа е да се оцени продължаващата пригодност, актуалност, адекватност и ефикасност на Системата за управление на информационната сигурност. Прегледът за ефикасност на СУИС е мярка за упражняване на контрол от ръководството върху нивото на мрежовата и информационната сигурност за доказване на съответствието на предприетите мерки с изискванията на нормативните актове и приетите стандарти.
2. ОТГОВОРНОСТИ
2.1. Директорът е отговорен за утвърждаването и поддържането на политиката и осигурява средствата и ресурсите, необходими за поддръжка на безопасността на информацията в образователната институция.
2.2. Определеният служител по информационна сигурност е отговорен за мониторинга за спазването и за предоставянето на необходимото обучение на служителите относно тази политика и участва в измерване на ефикасността на механизмите за контрол СУИС.
2.3. Отговорника по ИКС участва в измерване на ефикасността на механизмите за контрол СУИС.
2.4. Съвета по информационна сигурност е отговорен за обсъждането на стратегическите въпроси по информационната сигурност и вземането на решения по обсъдените въпроси включително и разглеждането на документите свързани с прегледа от ръководството.
2.5. Заместник-директор по Учебна дейност / Завеждащ, административна служба ИКС участва в <u>измерване на ефикасността на механизмите</u> за контрол СУИС.
2.6. Неспазването на политиката може да доведе до дисциплинарни мерки и/или правни последици в зависимост от сериозността на нарушението и действащото законодателство.
3. ОПИСАНИЕ НА ПРОЦЕСА
3.1. Вход на процеса

Взето решение от директора на образователната институция за извършване на преглед от ръководството за ефикасността на система за управление на информационната сигурност (СУИС). При провеждането на всеки преглед от ръководството за ефикасността на СУИС се взема решение за периода на провеждане на следващия такъв.
3.2. Изготвяне на заповед за извършване на преглед за ефикасността на СУИС
На база на взето решение на Директора на образователната институция за извършване на преглед на СУИС. Определеният служител по информационна сигурност подготвя, а Директора утвърждава заповед за провеждане на прегледа – ПРИЛОЖЕНИЕ 1. Основните насоки и указания за извършване на прегледа и съгласува заповедта, включват:
•Основание за издаване;
•Срок за извършване на прегледа;
•Състав на екипа;
•Срок за подготовка на входните данни за прегледа;
•Контролиращ изпълнението на заповедта.

В проекта на заповед се посочват и други обстоятелства, които имат значение за прегледа. Заповедта се изготвя и се предоставя за утвърждаване от Директора на образователната институция поне 30 дни преди датата за провеждане на прегледа на СУИС.

3.3. Извършване на подготовка на данни за преглед
Служителите, определени за подготовка на входните данни в заповедта събират, обобщават, анализират и изготвят необходимите документи и информация, както следва:
- Резултати от одити и прегледи на СУИС, действия, последвали след предишни прегледи на СУИС
- Методи, продукти или процедури, както и промени, които биха могли да бъдат използвани за подобряване на ефикасността и изпълнението на СУИС. Препоръки за подобрение, в случай, че има такива;
- Изпълнението на предприетите коригиращи действия
- Уязвими места или заплахите, които не са посочени правилно при предишни оценки на риска
- Протокол от измерване на ефикасността на механизмите за контрол СУИС – ПРИЛОЖЕНИЕ 2.

Всички документи се предоставят от служителите, определени със заповедта най-късно до 7 дни, преди датата на провеждане на прегледа.

3.4. Обсъждане от членовете на Съвет по информационна сигурност
В срока, определен в заповедта на Директора, изготвените документи се предоставят от отговорното лице по имейл на членовете на участниците за обсъждане по време на срещата.
3.5. Предоставяне на доклада от извършения преглед на СУИС на Директора за утвърждаване
В срока, определен в Заповедта за извършване на преглед на ефикасността на СУИС, Доклад за извършен преглед на СУИС - ПРИЛОЖЕНИЕ 3, се изготвя и предоставя от определеният служител по информационна сигурност на Директора на образователната институция за утвърждаване.
В случай на необходимост от подобрение и необходимост от предприемане на действия определеният служител по информационна сигурност изготвя и Заповед за предприемане на действия .

3.6. Резултат от процеса
- Утвърден доклад за извършен преглед на СУИС
- Взети решения за предприемане на действия – при необходимост.

ПРИЛОЖЕНИЕ 1

ДЕТСКА ГРАДИНА „ПЪРВИ ЮНИ”, ГР. КЮСТЕНДИЛ,
КВ. ЗАПАД, ТЕЛ.: 078/ 55 20 73, e-mail: info-100060@edu.mon.bg

ЗАПОВЕД

№ ...../..... ..... 20..... г.

На чл. 259, ал. 1 от Закона за предучилищното и училищното образование, във връзка с прилагането на Политиката по мрежова и информационна сигурност на ДГ“Първи юни“,град Кюстендил

ОПРЕДЕЛЯМ:

1. Преглед от ръководството на ДГ“Първи юни“, град Кюстендил за 2026г. да се проведе на .... 20..... г.

2. На прегледа на ръководството да присъстват следните служители *от* ***Съвет по информационна сигурност,*** за обсъждане:

Анелия Стоймирова – Директор

Десислава Костова – Заместник-директор

Донка Димитрова – главен счетоводител

Емилия Сотирова –ЗАС/домакин

3. Всички входните данни за прегледа да бъдат подготвени от . Емилия Сотирова – ЗАС/домакин , в срок до .... 20..... г.

В срок до .... 20..... г. Емилия Сотирова –ЗАС/домакин да сведе настоящата заповед до знанието на отговорните длъжностни лица срещу подпис за сведение и изпълнение.

Контрол по изпълнение на заповедта упражнявам лично.
ДИРЕКТОР: .....
Анелия Стоймрова

Запознати със съдържанието на заповедта:

№ по ред	Име и фамилия	Заемана длъжност	Дата	Подпис на лицето
1	Анелия Стоймирова	Директор		
2	Десислава Костова	зам.директор		
3	Донка Димитрова	гл.счетоводител		
4	Емилия Сотирова	ЗАС/домакин		

ПРИЛОЖЕНИЕ 2

ПРОТОКОЛ ОТ ИЗМЕРВАНЕ НА ЕФИКАСНОСТТА НА МЕХАНИЗМИТЕ ЗА КОНТРОЛ СУИС

Анализ и оценка на ефикасността на СУСИ

Една от основните цели на СУСИ е да се увеличи съществено вероятността за навременно идентифициране на потенциални вреди на значимите за ДГ“Първи юни“, гр.Кюстендил, информационни активи. За постигането й се използват множество адекватно подбрани контролни механизми.

Ефикасността на механизмите за контрол на СУСИ най-общо се определя като съотношение между постигнатите резултати и използваните за тях ресурси.

Актив	**Изводи от контролни проверки**	**Категоризиране на изводите за степента на ефикасност**
1	***2***	***3***
централна сграда и база“Зорница“	*Създадени са условия за контрол на външни лица в сградата. Въведена е система за защита на достъпа на входна врата, което изисква посрещане и придружаване на всеки посетител и прилагане на задължителните организационни мероприятия за обменяне на значима информация, с което е ограничена вероятността за несанкционирано проникване на външни лица и достъпа им до конфиденциална информация.*	*Оценява се като ВИСОКА степен на сигурност, поради отдалеченост от основните активи, контрол на достъпа, невъзможност за визуално наблюдение и посрещане и придружаване на посетителите.*
Електрозахранване на климатичната инсталация в сървърното помещение	*Захранването продължава да е единствено от съществуващата стандартна мрежа. Предвидена е система за записане на копие на всеки документ изготвен или постъпил в компютъра на директор или счетоводител.*	*Оценява се като ВИСОКА степен на сигурност, поради невъзможна реакция при продължително прекъсване.*
Управление и поддръжка на Критични ресурси/активи.	*Създадени са условия за администриране на информационната система, чрез наемане на външен изпълнител*	*Оценява се като средна степен на сигурност*

Обща оценка за периода:	**Оценява се като СРЕДНО ниво.**

Стремежа на ръководството е да поддържана **средна или висока** степен на ефикасност.

При идентифицирането на показателите е важно да се определи дали те са количествени или не.

Констатации:

Силни страни (постижения)	**Слаби страни (недостатъци и/или неизползвани възможности)**
Висока професионална подготовка на служителите	-
Мотивирано съзнание на служителите, за реакция при възникване на инциденти	-
Достъп само на директор и комисия архив до копия и документи на институцията	-
При спиране на захранването на ток има система с ups- генеартор при счетоводител	-

Показател	**Измерител**	**Оценка**
Разпределение на отговорностите	Организационна структура. съотношение на броя на длъжностните характеристики (гражданските договори, ако е приложимо) на лицата отговорни за информационната сигурност, в които тези отговорности са записани къмто общия брой лица, ангажирани в процеса на информационната сигурност.	Съответства
Декларации за конфиденциалност	съотношението на броя докладни записки относно нуждата от декларации или друг вид документи за конфиденциалност към издадените от ръководството решения по тези докладни	Всички служители подписват такава декларация
Физически контрол на достъпа	съотношението на броя на лицата имащи право на достъп до помещенията на организацията къмто общия брой на лицата, които използват тези помещения	съответства
Сигурността в договорите с трети	съотношението между договорите, в които са включени изисквания по	Задължителна клауза за всички

страни	отношение на информационната сигурност към общия брой договори, в които такива изисквания трябва да бъдат включени	резервационни системи
Инвентарен регистър на активите	Отношението на активите въведени в регистъра към обща брой активи	съответства
Отговорност за активите	отношението между общия брой активи, които имат зачислен отговорник към общия брой активи	съответства
Класификация на информацията	броя на възникналите проблеми в следствие на некоректна класификация на информацията и оценка на активите	Няма възникнали проблеми
Обозначаване на активите	броя обозначени активи (и информационни единици) към общия брой активи (и информационни единици)	съответства
Запознаване с изискванията на информационната сигурност, квалификация и обучения	общия брой подписи на инструктирани/ обучени лица към броя на лицата, които е трябвало да бъдат инструктирани/ обучени.	съответства
Контроли срещу зловреден код	откритите и неутрализирани заплахи записани в log-файла на антивирусния софтуер	до момента няма
Бекъп/ резервиране на информацията	времевия период, който е покрит от бекъп копия на данните към целия времеви период, за който се съхранява информация	съответства
Одит логове	възникналите случаи на необходимост за преглед на лог файловете на съответните системи	до момента не са възникнали случай
Логове на възникнали грешки и проблеми	броя докладни за установени проблеми или индикации за потенциални такива към общия брой установени проблеми или индикации за такива	до момента не са възникнали случай
Преглед на потребителските права за достъп	съотношението на действително проведените прегледи към общия брой прегледи, които е трябвало да бъдат проведени за конкретен период	до момента няма
Контрол на приложния софтуер	броя наложени дисциплинарни наказания за нарушаване изискването	до момента не са възникнали случай

Докладване на събития свързани с информационната сигурност	общия брой докладвани събития	до момента не са възникнали случай

Въз основа на направените констатации и изводи за сегашното състояние на системата, следва да се очертаят основните области за подобрение. Те могат да са в следните насоки:

- подобряване на постигнатите резултати;
- подобряване на ефективността при по-оптимално използването на ресурсите за постигането на същите резултати;
- оптимизиране на съотношението между постигнати резултати и използвани ресурси;
- усилия в подобряване на организационните мероприятия.

Постигнатите резултати следва да се разглеждат, като допустима честота на инциденти и намаляването на нивата на риск за активите на дружеството.

КОМИСИЯ В СЪСТАВ:

Анелия Стоймирова – Директор…….

Десислава Костова – заместник-директор ……

Донка Димитрова – главен счетоводител…….

Емилия Сотирова –ЗАС/домакин ……..

Дата: .... 20..... г.

ПРИЛОЖЕНИЕ 3

ДОКЛАД ЗА ИЗВЪРШЕН ПРЕГЛЕД НА СИСТЕМАТА ЗА УПРАВЛЕНИЕ НА ИНФОРМАЦИОННАТА СИГУРНОСТ (СУИС)

В изпълнение на Заповед № ……/..... ..... 20..... г. на директора на ДГ“Първи юни“, гр.Кюстендил на .... 20..... г. *(дата)* се извърши преглед на системата за управление на информационната сигурност (СУИС) от следните служители:

Анелия Стоймирова – Директор

Десислава Костова – заместник-директор

Донка Димитрова – главен счетоводител

Емилия Сотирова –ЗАС/домакин *)*

1. Прегледа от ръководството бе проведен при следният дневен ред:

……

Преглед на политиките и целите по качеството
Преглед на външните и вътрешни обстоятелства, изискванията на заинтересованите страни и оценката на риска и възможностите
Резултати от одити
Изпълнението на задачи от предходни прегледи
Обратна информация от клиенти и ЗС
Функционирането на процесите и съответствието на продукта
Препоръки за подобряване

……
……
……
……

2. Проведоха се обсъждания по следните документи:

- Резултати от одити и прегледи на СУИС, действия, последвали след предишни прегледи на СУИС
- Методи, продукти или процедури, както и промени, които биха могли да бъдат използвани за подобряване на ефикасността и изпълнението на СУИС. Препоръки за подобрение , в случай, че има такива;
- Изпълнението на предприетите коригиращи действия , в случай, че има такива.
- Уязвими места или заплахите, които не са посочени правилно при предишни оценки на риска
- Протокол от измерване на ефикасността на механизмите за контрол СУСИ.

3. Взеха се следните решения (изходни данни):

……
……
……

……

Няма необходимост от подобрение / Възможности за подобряване – ……..

- Подобряване на ефикасността на СУИС;
- Актуализиране на плановете за въздействие върху риска;
- Изменения на процедури и механизми за управление;
- Необходимостта от ресурси;
- Подобряване на точността на измерване на ефикасността на механизмите за управление.

……
……

ДИРЕКТОР: .....
Анелия Стоймирова

При всички описани политики се извършва:

1.ТЕСТВАНЕ И ПРЕГЛЕД:

Образователната институция извършва периодични тестове (минимум веднъж годишно) на плановете, чрез проиграване на различни сценарии –, за да провери тяхната ефективност и приложимост. Резултатите от тестовете се преглеждат и се предприемат действия за коригиране на откритите пропуски или за отстраняване на проблеми.

2.ОБУЧЕНИЕ И ОСВЕДОМЕНОСТ:

Образователната институция предоставя обучение и осведоменост на служителите относно политиките, процедурите и отговорностите . Това осигурява подготовка и готовност на персонала да действа в съответствие с плановете към всяка политика.

3.ПРЕГЛЕД И ПОДОБРЕНИЕ:

Политиките се преглежда периодично – минимум веднъж годишно, за да се гарантира, че са актуални и приложими спрямо съвременните заплахи и изисквания. Процесът на преглед допринася за непрекъснатото подобряване на политиките и свързаните с тях процедури и мерки. Резултатите от прегледите се документират и използват за подобряване на процесите на управление на непрекъсваемостта на дейността.

ДЕТСКА ГРАДИНА „ПЪРВИ ЮНИ”, ГР. КЮСТЕНДИЛ,
КВ. ЗАПАД, ТЕЛ.: 078/ 55 20 73, e-mail: info-100060@edu.mon.bg

ПЛАН ЗА НЕПРЕКЪСВАЕМОСТ НА ДЕЙНОСТТА НА

ДГ“Първи юни“,град Кюстендил

1. ВЪВЕДЕНИЕ И ОБХВАТ

Планът за непрекъсваемост на дейността се разглежда като процес на възстановяване на пълната функционалност на работните процеси и дейности, след сривове и аварии от гледна точка на способността за осигуряване на дейностите в образователната институция.

Основните цели на настоящият план за непрекъсваемост са:

- свеждане до минимум прекъсванията на дейността;
- ограничаване на прекъсванията и/или щетите;
- минимизиране на последствията от прекъсването;
- осигуряване на алтернативи за продължаване на дейността;
- обучение на персонала за действия при екстрени ситуации;
- осигуряване на възможно най-бързо и леко възстановяване на дейността в образователната институция.

2. ОТГОВОРНОСТИ

За изпълнение на Плана са създадени следните екипи за участие във възстановителните операции:

- Екип за управление, включително и координатор на Плана, който отговаря за правилното управление на плана и за докладването на състоянието на ръководството;
- Екип за оценка на щетите/прекъсването отговаря за бързата и точна оценка на щетите;
- Екип(и) за възстановяване на ИТ системи (сървър, база данни, приложения и мрежа) отговаря за възстановяването на съответните ресурси;
- Екип (и) за тестване след възстановяване отговаря за извършване на тестването след

извършеното възстановяване;

При необходимост се създават и други екипи за действие по Плана за действия при бедствия и аварии, като:

- Екип за транспорт и преместване ;
- Екип за поръчки и доставки (оборудване и консумативи);

Поименен списък на екипите, ръководителите на екипи, членовете и информацията за контакт са неразделна част от плана - ПРИЛОЖЕНИЕ 1

3. РЕД ЗА ИЗПЪЛНЕНИЕ

а. Вероятни причини за прекъсване на дейностите.

Условие за възникване причина за прекъсване	**Причина за прекъсване**	**Действие за предотвратяване на прекъсването**	**Загуби**	**Риск**	**Бележки**
1	*2*	*3*	*4*	*5*	*6*
Външен злонамерен достъп в мрежата.	Объркване на нормалния процес на работа.	Прекратяване на външния достъп и преглед и увеличение на защитите.	Имидж и финансови средства	среден	
Дефект на хардуер или съоръжения	Хардуерен дефект. Невъзможност за работа на поддържаната система поради проблем с хардуер или съоръжения.	Прехвърляне на резервен хардуер или съоръжение до възстановяване на основният	Финансови средства	среден	
Проблем мрежова комуникация	Липса на мрежова комуникация.	Преглед на инфраструктурата и възстановяване на добрата мрежова комуникация.	Финансови средства	среден	
Забележка: *Причините следва да се преглеждат на всеки 12 месеца.*					

Мероприятия осигуряващи непрекъсваемост	
Причина за прекъсване	**Описание**

Злонамерен външен достъп. Объркване на процеса на работа.	**Наблюдение на системи за сигурност и защитни стени.**
Хардуерен проблем. Невъзможност за работа на поддържаната система.	**Работа със нова техника в гаранция и двойна резервираност на някои хардуери.**
Липса на мрежова комуникация.	**Поддържане на комуникационната инфраструктура в добро състояние, редовни прегледи. Поддържане на алтернативни методи на достъп.**

b. Фази на оповестяване и активиране на плана

2.1. Процедура по оповестяване.

При възникване на критична ситуация, основната задача образователната институция е да се предпази живота и здравето и да се осигури сигурността на персонала като се прилага ПБА.

В ПРИЛОЖЕНИЕ 1 са посочени координатите за контакти на служителите на образователната институция, а ПРИЛОЖЕНИЕ 2 съдържа координатите на организации, доставчици и изпълнители по договори, които Координаторът трябва уведоми за възникналото събитие.

Последователността от действията по оповестяване за възникнало събитие, са както следва:

2.1.1. Незабавно уведомяване на Координатора по непрекъснатостта на дейността от физическата охрана. Цялата известна информация трябва да бъде съобщена на координатора и известяване на аварийните служби, тел. 112 от физическата охрана в случай на необходимост

2.1.2. Координаторът уведомява:

- Ръководителя на екипа по оценяване на щетите за настъпилото събитие и разпорежда стартирането на процедура по оценяване на щетите
- Директора на образователната институция
- Ръководителите на екипи от настоящия план

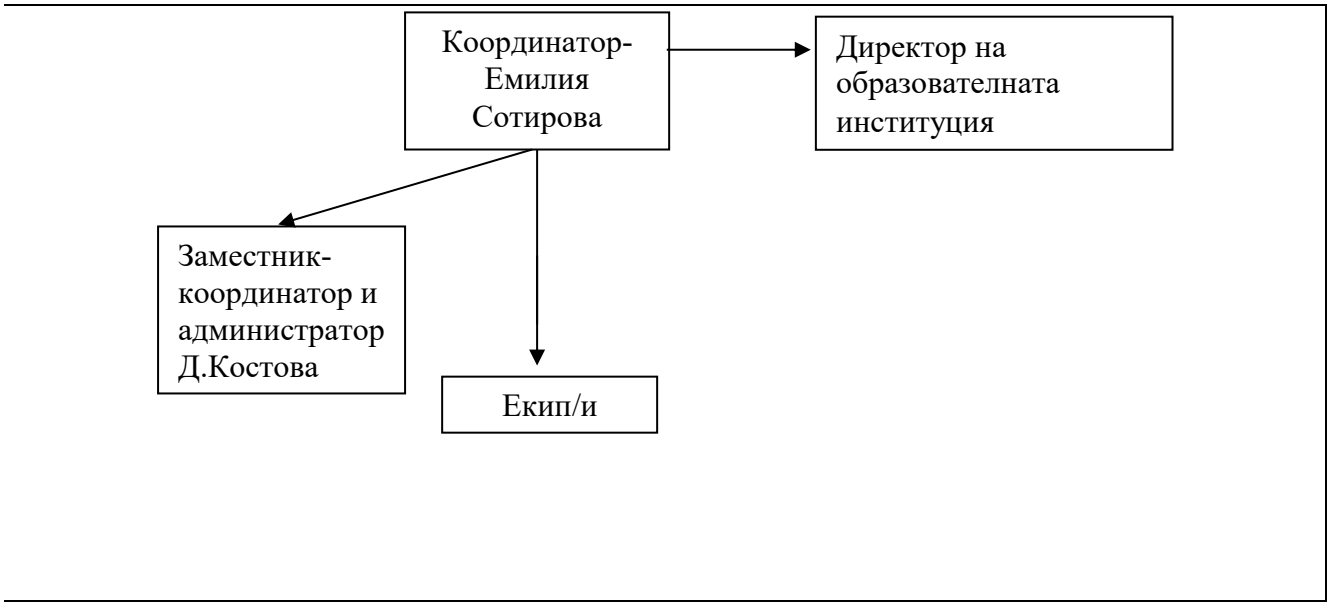
2.1.3. Ръководителят на екипа по оценяване на щетите уведомява членовете на екипа и стартира изпълнението на процедурата по оценяване, описана по-долу, с цел определяне размера на щетите и оценка на необходимото време за възстановяване;

2.1.4. Ръководителите на екипи:

- Уведомяват членовете на екипите
- Организират предприемането на съответните действия, съгласно плана или процедурите за работа
- Координатора за предприетите действия и предстоящите за предприемане мерки

2.1.5. Оповестяването се осъществява по всички възможни канали за комуникация – мобилни телефони, стационарни телефони, електронна поща, лично. Оповестяването се извършва в съответствие с таблицата на отговорностите, в която са определени екипите за всяка фаза и с дървото на повикването (call tree).

Дървото на повикването



Информацията, която трябва да се даде при уведомяването включва по възможност следното:

- вид на събитието;
- пострадали;
- известни щети;
- място на среща за по-нататъшни инструкции;

- инструкции за завършване на повикването (ако е необходимо).

2.2. Процедура по оценка на щетите.

Екипът/ите по оценка на щетите трябва да започнат максимално бързо работа и затова те се уведомяват първи.

След уведомяване от координатора, администратора е длъжен да:

- събере екипа;
- създаде организация на работа на екипа;
- събере необходимата информация за настъпилото събитие, засегнати области;
- извърши оценка и анализ на щетите;
- уведоми директора за резултатите от оценката.

Екипът/ите по оценяване на щетите трябва да отговори на следните въпроси:

- причина на прекъсването;
- потенциал за допълнително разрушаване или щети;
- област засегната от събитието;
- статус на инфраструктурата (състояние на стаите, електрозахранването, телекомуникациите, отопление и т.н.);
- инвентарен и функционален статус на информационната система (напълно, частично или не функционираща);
- тип на повредата на информационното оборудване (от наводнение, пожар, прегряване, електрически удар и т.н.);
- наличие и състояние на документи на хартиен носител;
- ресурси, които трябва да бъдат заменени (хардуер, софтуер, офис-оборудване, други);
- наличие на сервизните услуги;
- приблизителна оценка на времето за възобновяване на работата.

На база на резултатите от оценката, координаторът предприема действия, съобразявайки ситуацията и засегнатите активи според тяхната критичност съгласно Списък на критични ресурси/активи на обучителната организация **– Приложение 3.**

2.3.Активиране на плана

Координаторът на база на извършения анализ от екипа по оценяване на щетите преценява необходимостта от активиране на плана за непрекъснатост на дейността.

Решението за активиране на плана се взима само от Координатора по непрекъснатост на дейността след одобрение от Директора или лицата, които ги заместват в случай на отсъствие. Координаторът уведомява директора по възстановяване за избраната стратегия.

Планът може да бъде активиран, ако е налице прекъсване на дейността **за повече от 24**

часа.

След взимане на решение за активиране на плана, Координаторът уведомява:

- Екипите за възстановяване;
- Ръководителите на засегнатите структури (с цел да бъдат запознати с цялата налична информация);
- Доставчиците, определени да доставят необходимата техника при извънредни събития;
- Резервното сграда за настъпилото извънредното събитие и действията, които следва да се предприемат;
- Всички служители, за общото състояние след инцидента;
- При необходимост се изготвя съобщения до медиите, публикуване на информация.

2.4. Осигуряване на помещения за работа от друга дестинация

Ако аварийната ситуация се очаква да продължи повече от 24 часа всички служители се уведомяват да продължат работа от домовете си или в резервната сграда, съгласно плана за действие при бедствия и аварии.

2.5. Възобновяване на нормалната работата

Възстановяването на нормалната работа се извършва в зависимост от оценката на щетите и предвижда възобновяване на работата в основната сграда или преместване и възобновяване на дейността в избран/определената алтернативна.

Възобновяване на работата се извършва от екипа по възстановяването.

С цел постигане на максимална ефективност при възстановяване на работата, при изпълнението на всяка процедура следва да се спазва последователността, в която същата е представена.

Екипите по възобновяването на работата са посочени ПРИЛОЖЕНИЕ 1.

За документиране на действията при изпълнението на процедурата се използва чек-лист формат.

Процедурата по възстановяването включва следните стъпки (таблицата може да се използва като чек-лист):

Стъпка	Дата/час
Получаване на разрешение за достъп до засегнатия обект (от официалните власти, ако е необходимо)	
Уведомяване вътрешните (съответните ръководители) и външните (засегнати структури, клиенти) страни	
Проверка на офис оборудване и при необходимост доставка на ново	
Проверка на хардуера и при необходимост доставка и инсталиране на нов	

Възстановяване на критичните системи	
Възстановяване на данните на системите	
Тестване функционалността на системите, в т.ч. и мерките за сигурност	
Свързване на системата/те с локалната мрежа или други външни системи	

c. Преминаване в нормален режим на работа.

Цел: Да осигури плавно преминаване на дейностите в основната сграда.

Преминаване в нормален режим на работа се извършва след пълно възстановяване на засегнатите структури и системи. За целта се преминават следните стъпки:

- Проверка за адекватна инфраструктура (електричество, вода, телекомуникации, сигурност, контрол на обкръжението, офис оборудване и др.);
- Инсталиране на системен хардуер, софтуер и фърмуер;
- Установяване на връзки и интерфейси с мрежовите компоненти и външни системи;
- Тестване на системата (от екипа по тестване) за доказване на пълната ѝ функционалност;
- Запис на данните от временната система и прехвърлянето им на възстановената система.

d. Деактивиране на плана.

При деактивирането на плана се преминава към нормална работа, а в случай на използване на алтернативната сграда, оборудването и други материали, се обръща особено внимание на носителите на чувствителна информация.

Материалите, оборудването и носителите на архивни данни медиите с архив /магнитни ленти, дискове CD, DVD, външни хард дискове или масиви от дискове и пр./ трябва да бъдат подходящо опаковани, надписани и изпратени до съответния основен или нов алтернативен офис.

При деактивиране на плана се преминава през следните стъпки посочени в таблицата, която може да се използва и за чеклист.

Стъпка	Дата/час
Изключване на временната система;	
Обезопасяване и преместване на чувствителната информация в съответствие с процедурата за съхраняване на информация.	
Преместване на оборудването.	
Организиране преместването на персонала.	

ПРИЛОЖЕНИЕ 1

Екипи	Име и длъжност	Email	Служебен телефон
1	*2*	*3*	*4*
Екип за управление (включително координатора на Плана)			
Ръководител	Анелия Стоймирова	info-1000060@edu.mon.bg	0882885340
Координатор на Плана	Емилия Сотирова	dg_1juny@abv.bg	0877039505
Зам. координатори на Плана	Десислава Костова	kostova.desislawa@yahoo.com	0885862885
Екип за оценка на щетите/прекъсването – (БФ)			
Ръководител	Анелия Стоймирова	info-1000060@edu.mon.bg	0882885340
Членове:	Емилия Сотирова	dg_1juny@abv.bg	0877039505
	Десислава Костова	kostova.desislawa@yahoo.com	0885862885
	Донка Димитрова	dg_1juny@abv.bg	0882885355
Екип за възстановяване на системна администрация, възстановяване на сървъри, база данни и мрежи			
Ръководител	Анелия Стоймирова	info-1000060@edu.mon.bg	0882885340
Членове:	Емилия Сотирова	dg_1juny@abv.bg	0877039505
	Десислава Костова	kostova.desislawa@yahoo.com	0885862885
	Донка Димитрова	dg_1juny@abv.bg	0882885355
Екип(и) за тестване след възстановяване			
Ръководител	Анелия Стоймирова	info-1000060@edu.mon.bg	0882885340
Членове:	Емилия Сотирова	dg_1juny@abv.bg	0877039505
	Десислава Костова	kostova.desislawa@yahoo.com	0885862885
	Донка Димитрова	dg_1juny@abv.bg	0882885355

ПРИЛОЖЕНИЕ 2

Списък за контакти с организации, доставчици и изпълнители по договори
(Договори за услуги с гарантирано ниво и качество)

Фирма	**Лице за връзка във фирмата**	**Телефони за връзка**	**Отговорен служител за връзка с фирмата** *(Координатор)*
1	*2*	*3*	*4*
НЕИСПУО	Десислава Костова	чрез запитване в платформата	Ален Асенов
EDG.BG	Десислава Костова	0878680579	подръжка

ПРИЛОЖЕНИЕ 3

СПИСЪК НА КРИТИЧНИ РЕСУРСИ/АКТИВИ
На ДГ“Първи юни“

Приложението включва основни критични информационни системи, автоматизиращи дейностите на ключовите функции. Тук се включват всички необходими активи/ресурси (приложни сървъри, сървъри за бази данни, операционни системи, комуникации, инфраструктура и др.), които осигуряват работата на следните информационни системи:

VII. ПРОЦЕДУРИ:

- ПРОЦЕДУРА ЗА УПРАВЛЕНИЕ НА ИНЦИДЕНТИ

I. ВЪВЕДЕНИЕ:

Процедурата за управление на инциденти свързани с информационната сигурност имат за цел да осигурят ефективно разрешаване и управление на инциденти, които засягат информационната сигурност в образователната институция. Тази процедура предоставят рамка за идентификация, оценка, реагиране и документиране на инцидентите, свързани с информационната сигурност.

II. ОПРЕДЕЛЕНИЕ НА ИНЦИДЕНТИ СВЪРЗАНИ С ИНФОРМАЦИОННАТА СИГУРНОСТ

1. Инцидентите свързани с информационната сигурност се определят като нередности или нарушения на политиките, процедурите или мерките за информационна сигурност.

2. Инцидентите могат да включват, но не се ограничават само до, компрометиране на данни, неоторизиран достъп до системи или информация, загуба или повреда на активи, злонамерена програма и други подобни нарушения.

III. ИДЕНТИФИКАЦИЯ И ДОКЛАДВАНЕ НА ИНЦИДЕНТИ

1. Всички служители/доставчици (трети страни, с който образователната институция има отношения), забелязали потенциални или реални инциденти, свързани с информационната сигурност, незабавно ги докладват на определеният служител по информационна сигурност по един от следните канали:
   Имейл : info-1000060@edu.mon.bg / dg1_juny@abv.bg
   Телефон: 0882885340/ 0885862885
   Система: ……...
2. Докладът за инцидент става посредством формата за докладване на инцидент свързан с информационната сигурност **(ПРИЛОЖЕНИЕ 1)**, която съдържа следната информация:

   2.1. Имена и контакти (телефон, имейл) за връзка с подателя на сигнала.

   2.2. Описание на инцидента и неговите последствия.

2.3. Дата и час на забелязване на инцидента.

2.4. Информация за евентуалните причини или източници на инцидента.

2.5. Допълнителни доказателства или информация, свързана с инцидента.

IV. ОЦЕНКА НА ИНЦИДЕНТИТЕ:

1. Идентифицираните инциденти се оценяват възможно най-скоро от определеният служител по информационна сигурност.
2. Оценката на инцидента включва:
   2.1. Категоризация на инцидента според нивото на сериозност и въздействие върху информационната сигурност.

   2.2. Идентифициране на последствията за обучителната организация.

   2.3. Определяне на приоритетите за незабавни действия за управление на инцидента.

V. РЕАГИРАНЕ НА ИНЦИДЕНТИ:

1. След оценка на инцидента се предприемат незабавни мерки за реагиране и справяне с инцидента.

2. Реагирането на инцидента включва следните стъпки:

   2.1. Изолиране на засегнатите активи от инцидента.

   2.2. Възстановяване на информационната система или актив, засегнати от инцидента. При сериозни инциденти по преценка на директора е възможно да се включат различни служители/групи, за по-бързото отстраняване на проблема и възстановяване на нормалната работа.

   2.3. Извършване на изследвания за идентификация на причините и отговорните за инцидента.

   2.4. Анализиране на мерките за превенция и недопускане на повторение на подобни инциденти.

   2.5. При сериозни инциденти, при необходимост се предприемат действия по информирането на компетентните органи.

2.6. Определеният служител по информационна сигурност изготвя доклад до директора с описание на цялата информация свързана с инцидента.

VI. ДОКУМЕНТИРАНЕ И ОТЧЕТНОСТ:

1. Всички инциденти, идентифицирани и управлявани според процедурите, са документирани. За целта определеният служител по информационна сигурност регистрира инцидента, като го записва с регистъра за инциденти свързани с информационната сигурност **(ПРИЛОЖЕНИЕ 2)**.
2. Документацията за инцидентите включва следната информация:

2.1. Дата и час на инцидента.

2.2. Подател на сигнала.

2.3. Описание на инцидента и предприетите действия.

2.4. Имена на отговорните лица за управление на инцидента.

2.5. Идентификация на засегнатите активи и информационни системи.

2.6. Извлечени поуки и препоръки за бъдещи подобни случаи.

VII. ПРЕГЛЕД И ПОДОБРЕНИЕ:

Процедурата за управление на инциденти се преглежда и подобрявани редовно, минимум веднъж в годината от определеният служител по информационна сигурност. Прегледът включва анализ на ефективността на предприетите мерки и идентифициране на възможности за подобрение.

ПРИЛОЖЕНИЕ 1

ФОРМАТА ЗА ДОКЛАДВАНЕ НА ИНЦИДЕНТ СВЪРЗАН С ИНФОРМАЦИОННАТА СИГУРНОСТ

1. Имена и контакти (телефон, имейл) за връзка с подателя на сигнала

……
……
……

2. Дата и час на забелязване на инцидента

……..

3. Описание на инцидента и неговите последствия

……
……
……

4. Информация за евентуалните причини или източници на инцидента

……
……
……

5. Допълнителни доказателства или информация, свързана с инцидента

……
……
……

Приложение № 2

РЕГИСТЪР ЗА ИНЦИДЕНТИ, СВЪРЗАНИ С ИНФОРМАЦИОННАТА СИГУРНОСТ

№	Дата и час на инцидента	Подател на сигнала	Описание на инцидента	Идентификация на засегнатите активи и информационни системи	Въздействие на компонентите на информационната сигурност	Предприети действия	Имена на отговорните лица за управление на инцидента	Извлечени поуки и препоръки
1	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*
1	*11:14 ч. 29.09.2023 г.*	*Иван Иванов*	*Заразен компютър с криптовирус след кликване на потребителя на линк от фишинг имейл.*	*Само една работна станция - на потребителя*	*Загуба на наличност на информацията*	*Премахнат е зловредният софтуер*	*Георги Георгиев*	*Необходими допълнителни обучения на служителите за действия при фишинг имейли. Използване на антивирусна програма с актуални дефиниции*
2								
3								

➢ ПРОЦЕДУРА ЗА СЪОТВЕТСТВИЕ НА СУИС С НОРМАТИВНИТЕ ИЗИСКВАНИЯ

1. ВЪВЕДЕНИЕ И ОБХВАТ

Настоящата процедура за съответствие на СУИС с нормативните изисквания е разработена в съответствие с изискванията на международни стандарти свързани с мрежовата и информационна сигурност (МИС) и има за цел да постигне пълно нормативно, техническо и технологично съответствие на СУИС с изискванията на:

- Закона за Киберсигурност и Наредба за минималните изисквания за мрежова и информационна сигурност;
- Влезли в сила други административни актове в сферата на информационната сигурност, касаещи образователната институция (като Закон за защита на личните данни, Закон за авторското право и сродните му права и други);
- Препоръки и добри практики на колекцията стандарти за системи за управление на сигурността на информацията ISO/IEC 27001;
- Други специфични изисквания – следва да се допълнят от образователната институция.

2. ОТГОВОРНОСТИ

2.1. Директорът на образователната институция е отговорен за утвърждаването и поддръжката на актуална процедура за съответствие на СУИС с нормативните изисквания.
2.2. Определеният служител по информационна сигурност е отговорен за разработването, изпълнението и поддръжката на процедурата и подготвя входните данни необходими за извършване на съответствието.
2.3. Съвета по информационна сигурност разглежда и решава всички казуси, касаещи информационната сигурност.
2.4. Неспазването на политиката може да доведе до дисциплинарни мерки и/или правни последици в зависимост от сериозността на нарушението.

3. ОЦЕНКАТА ЗА СЪОТВЕТСТВИЕ НА СУИС

Оценката се извършва при настъпване на значителни изменения в СУИС, в нормативни актове или взаимоотношенията с трети страни, касаещи информационната сигурност в образователната институция.
Оценката се извършва след взето решение от директора на образователната институция за извършване на оценка за съответствие на СУИС.
Определеният служител по информационна сигурност или фирма-консултант по информационна сигурност подготвя, обобщава и анализира събраната информация, необходима за изпълненото на настоящата процедура и изготвя доклад за извършена оценка за съответствие на СУИС.

Етапи за подготовка за оценка на съответствие:

- Събират и преглеждат документи (източници на информация и данни);
- Детайлно проучване на приложимите изисквания (стандарти, директиви, нормативни актове и добри практики) и целите, които следва да се постигнат;
- Обобщава и анализира документи и информация на принципа „необходима и достатъчна“.
- Идентифициране на приложимите законови и договорни изисквания - процесът по идентифицирането на приложимото законодателство се контролира от директора на образователната институция.

- Защита на записите - важните записи трябва да бъдат защитени от загубване, разрушаване и фалшификация, в съответствие със законовите, регулаторните, договорните и бизнес изисквания.
- Защита на данните и тайната на личната информация – има ли внедрени механизми за контрол, гарантиращи спазването на законодателството за защита на личните данни.
- Независим преглед на мрежовата и информационна сигурност - подходът за управлението и внедряването на информационната сигурност (образователната институция цели по контрол, контроли, политики, процеси и процедури) трябва да се преглеждат независимо, на планирани интервали от време или при настъпили значителни промени
- Съответствие с политиката и стандартите за сигурност - трябва да се гарантира, че всички процедури за сигурност в тяхната област на отговорност се извършват правилно, за да се осигури съответствие с политиките за сигурност и стандартите.
- Права на интелектуална собственост трябва да бъдат изпълнени в съответните процедури, за да се осигури съответствие със законовите, регулаторните и договорните изисквания по използване на активи, по отношение, на които може да има права на интелектуална собственост.
- Оценка на техническото съответствие - информационните системи трябва редовно да се проверяват за съответствие със стандартите за сигурност.
- Добавят се и други при необходимост съобразно попълнената допълнителна информация в т.1 раздел „Други специфични изисквания“

Оценката за съответствие на СУИС се извършва под формата на доклад от отговорният служител по информационна сигурност или фирма-консултант по информационна сигурност, по искане на директора на образователната институция. Той се предоставя за пред Съвета по информационна сигурност на образователната институция;

При установени несъответствия Съвет по информационна сигурност взема решения по казусите свързани с несъответствията с информационната сигурност.
При необходимост се изготвя и заповед за решения и предприемане на действия, по отношение на:
- Отстраняване на евентуални несъответствия на СУИС;
- Изменения на процеси, процедури и механизми за контрол и управление;
- Осигуряване на допълнителни ресурси.

Докладът за извършена оценка за съответствие и решенията на съвета по информационна сигурност, ако има такива се представя за утвърждаване на директора на образователната институция.

4. РЕЗУЛТАТ ОТ ПРОЦЕСА ПО ОЦЕНКА НА СЪОТВЕТСТВИЕТО:
- Утвърден доклад за извършена оценка за съответствие на СУИС;
- Издадена заповед за предприемане на действия – при необходимост

➢ ПРОЦЕДУРА ЗА СИГУРНО РАЗРАБОТВАНЕ, РАЗВИТИЕ И ПОДДЪРЖАНЕ НА СОФТУЕРЕН ПРОДУКТ

1. ВЪВЕДЕНИЕ:

Настоящата процедура за сигурно разработване, развитие и поддържане на софтуерен продукт е в съответствие с изискванията на международни стандарти свързани с мрежовата и информационна сигурност (МИС) и има за цел да осигури ефективното сигурно разработване и поддръжка на софтуерните продукти на образователната институция. Тя гарантира сигурността, наличността и надеждността на системите, които са от съществено значение за образователната институция.

2. ОТГОВОРНОСТИ:

2.1. Директорът на образователната институция е отговорен за утвърждаването на процедура за сигурно разработване, развитие и поддържане на софтуерен продукт.

2.2. Определеният служител по информационна сигурност е отговорен за поддържането в актуално състояние на процедура за сигурно разработване, развитие и поддържане на софтуерен продукт и участва пряко в целият път на разработването на продукта, съгласно компетенцията му.

2.4. Отговорните служители стриктно спазват всички етапи описани в процедура за сигурно разработване, развитие и поддържане на софтуерен продукт

2.5. Неспазването на процедурата може да доведе до дисциплинарни мерки и/или правни последици в зависимост от сериозността на нарушението.

3. ПЛАНИРАНЕ И ДЕФИНИРАНЕ НА ИЗИСКВАНИЯТА:

3.1 Анализ на изискванията

- Процеса стартира с дефинирането на изискването към софтуерният продукт (информационна система, уебсайт и други).
- Следва обобщаване на функционални и нефункционални изисквания.
- Задължително е и идентифицирането и описването на изискванията за сигурност от списъка с изисквания (**ПРИЛОЖЕНИЕ 1**), свързани с поверителност,

автентикация, одит и съответствие на нормативните изисквания и добрите международни стандарти.

3.2. Рисков анализ

- Извършва се оценка на възможните заплахи и уязвимости.
- Създава се план за управление на рисковете.

3.3. Проектиране на сигурност

- Използват се утвърдени модели за сигурност (напр. Zero Trust, OWASP и други).
- Дефинират се сигурностни механизми като криптиране, контрол на достъпа и логване.

4. ДИЗАЙН И АРХИТЕКТУРА:

4.1. Избор на технологии - При избора се предпочитат технологии и библиотеки с активна поддръжка и известна репутация.

4.2. Сигурност по дизайн

- Прилагане на принципа "Least Privilege".
- Сегментиране на системата на модули с минимални точки за достъп.

4.3. Финализиране

- Изготвя се обобщен документ “Технически изисквания към софтуерен продукт“ (**Приложение 3**).
- Провежда се финален преглед от определеният служител по информационна сигурност, за цялостно попълване на документа преди стартиране на разработката на софтуерният продукт.

5. РАЗРАБОТКА:

5.1. Безопасно програмиране

- Следват се утвърдени стандарти за сигурно кодиране (напр. OWASP Secure Coding Practices).

- Избягват се опасни функции и методи.

5.2. Контрол на версията

- Използват се системи за контрол на версиите (напр. Git) с ограничен достъп.
- Редовно се провеждат ревюта на кода.

5.3. Анализ за сигурност на кода

- Провеждат се статичен и динамичен анализ на кода.
- Използват се и автоматизирани инструменти за търсене на уязвимости.

6. ТЕСТВАНЕ И ВЕРИФИКАЦИЯ:

6.1. Функционални тестове – Извършват се тестване на всички функционалности спрямо изискванията.

6.2. Тестове за сигурност

- Извършва се тестване срещу често срещани уязвимости (напр. SQL Injection, XSS).
- Провеждат се пенетрейшън тестове.

6.3. Одит

- При необходимост, наемане на външни специалисти за независим одит.
- След извършване на всички тестове включително и тестове за сигурност, ако са установени критични уязвимости или други функционални проблеми, те следва да се отстранят, след което си извършва повторен тест. Ако не са установени никакви проблеми се попълва протокол за приемане пускане в експлоатация (**ПРИЛОЖЕНИЕ 4**)

7. ДЕПЛОЙМЕНТ:

7.1. Подготовка за пускане

- Осигурява се безопасна продукционна среда (production environment).
- Минимизират се излишни права и достъп до сървърите.

• Реалната и тестовата среда са абсолютно еднакви, за да се избегнат проблеми при деплоймента.

• Средите отговарят на изискванията за киберсигурност съгласно (**ПРИЛОЖЕНИЕ 2)** към процедурата.

7.2. Мониторинг

• Инсталират се инструменти за наблюдение и алармиране.

• Логват се ключови събития за анализ на сигурността.

8. ПОДДРЪЖКА И ОБНОВЛЕНИЯ:

8.1. Постоянен мониторинг

• Следят се уязвимости и се прилагат веднага спешните (критични) пачове.

• Анализират се логовете за подозрителна дейност.

8.2. Обновления и корекции

• Планират се обновления свързани със сигурността.

• Тестват се всички промени преди имплементация.

8.3. Обучение на екипа – Редовно се провеждат обучения за нови заплахи и добри практики при разработването на системите.

9. ПРЕГЛЕД И ПОДОБРЕНИЕ:

Процедурата за сигурно разработване и развитие и поддържане на софтуерните продукти се преглежда и подобрявани редовно, минимум веднъж в годината от определеният служител по информационна сигурност. Прегледът включва анализ на ефективността на предприетите мерки и идентифициране на възможности за подобрение.

ПРИЛОЖЕНИЕ 1

ПРИМЕРЕН СПИСЪК С ИЗИСКВАНИЯ ЗА СИГУРНОСТ ПРИ РАЗРАБОТВАНЕ НА СОФТЕРЕН ПРОДУКТ (ИНФОРМАЦИОННА СИСТЕМА , УЕБСАЙТ И ДРУГИ)

1. Не се допуска съхранението на пароли на администратори, на вътрешни и външни потребители и на акаунти за достъп на системи (ако такива се използват) в явен вид. Всички пароли трябва да бъдат защитени с подходящи сигурни алгоритми (напр. BCrypt, PBKDF2, scrypt (RFC 7914) за съхранение на пароли и където е възможно, да се използва и прозрачно криптиране на данните в СУБД със сертификати (transparent data-at-rest encryption).
2. Да бъде предвидена система за ежедневно създаване на резервни копия на данните, които да се съхраняват извън инфраструктурата на системата.
3. Не се допуска използването на Self-Signed сертификати за публични услуги.
4. Всички уебстраници (вътрешни и публично достъпни в Интернет) трябва да бъдат достъпни единствено и само през протокол HTTPS. Криптирането трябва да се базира на сигурен сертификат с валидирана идентичност (Verified Identity), позволяващ задължително прилагане на TLS 1.2, който е издаден от удостоверителен орган, разпознаван от най-често използваните браузъри (Microsoft Edge, Google Chorme, Mozilla Firefox). Ежегодното преиздаване и подновяване на сертификата трябва да бъде включено като разходи и дейности в гаранционната поддръжка за целия срок на поддръжката.
5. Трябва да бъдат извършени тестове за сигурност на всички уебстраници, като минимум чрез автоматизираните средства на SSL Labs за изпитване на сървърна сигурност (https://www.ssllabs.com/ssltest/).
6. За нуждите на автентикация с КЕП трябва да се предвиди имплементирането на обратен прокси сървър (Reverse Proxy) с балансиране на натоварването, който да препраща клиентските сертификати към вътрешните приложни сървъри с нестандартно поле (дефинирано в процеса на разработка на Системата) в HTTP Header-a. Схемата за проксиране на заявките трябва да бъде защитена от Spoofing.
7. При разгръщането на всички web услуги (Web Services) трябва да се използва единствено протокол HTTPS със задължително прилагане на минимум TLS 1.2.
8. Програмният код трябва да включва методи за автоматична санитизация на въвежданите данни и потребителски действия за защита от злонамерени атаки, като

минимум SQL инжекции, XSS атаки и други познати методи за атаки, и да отговаря, където е необходимо, на Наредбата за минималните изисквания за мрежова и информационна сигурност.

9. При проектирането и разработката на компонентите на Системата и при подготовката и разгръщането на средите трябва да се спазват последните актуални препоръки на OWASP (Open Web Application Security Project).
10. Трябва да бъде изграден модул за проследимост на действия и събития в Системата. Записът за всяко действие (добавяне, изтриване, модификация, четене) трябва да съдържа следните атрибути:
    - Уникален номер;
    - Точно време на възникване на събитието;
    - Вид (номенклатура от идентификатори за вид събитие);
    - Данни за информационна система, където е възникнало събитието;
    - Име или идентификатор на компонент в информационната система, регистрирал събитието;
    - Приоритет;
    - Описание на събитието;
    - Данни за събитието.
11. Астрономическото време за удостоверяване настъпването на факти с правно или техническо значение се отчита с точност до година, дата, час, минута, секунда и при технологична необходимост - милисекунда, изписани в съответствие със стандарта БДС ISO 8601:2006.
12. Астрономическото време за удостоверяване настъпването на факти с правно значение и на такива, за които се изисква противопоставеност, трябва да бъде удостоверявано с електронен времеви печат по смисъла на Глава III, Раздел 6 от Регламент ЕС 910/2014. Трябва да бъде реализирана функционалност за получаване на точно астрономическо време, отговарящо на горните условия от доставчик на доверителни услуги или от държавен орган, осигуряващ такава услуга, отговаряща на изискванията на RFC 3161.
13. Трябва да бъдат проведени тестове за проникване (penetration tests), с които да се идентифицират и коригират слаби места в сигурността на Системата.
14. При идентификация на регистри и бази данни да се използва електронно удостоверение във формат X.509, издаден за съответния регистър. Идентификацията се осъществява двустранно по протокол TLS (Transport Layer Security - Сигурност на

транспортния слой), версия 1.2 или по-висока, дефиниран в Препоръка RFC 5246, приета от IETF

15. Информационните системи на административните органи да се идентифицират пред регистрите чрез цифров сертификат, двустранно по протокол TLS (Transport Layer Security - Сигурност на транспортния слой), версия 1.2 или по-висока.

ПРИЛОЖЕНИЕ 2

ПРИМЕРНИ ИЗИСКВАНИЯ ПО ОТНОШЕНИЕ НА КИБЕРСИГУРНОСТ С ЦЕЛ ДОСТИГАНЕ НА ИЗИСКВАНОТО НИВО НА СИГУРНОСТ НА ИНФОРМАЦИЯТА, В МРЕЖИТЕ И ИНФОРМАЦИОННИТЕ СИСТЕМИ

1. Да бъдат включени адекватни и комплексни изисквания за мрежова и информационна сигурност, основани на анализ и оценка на риска, с цел да се гарантира, че изискваното ниво на сигурност на информацията, мрежите и информационните системи е заложено още в етапа на разработка и внедряване;
2. Да се представят анализ и оценка на риска, които да послужат като основа за включването на адекватни и комплексни изисквания за мрежова и информационна сигурност?
3. Ненужните портове по протоколи TCP и User Datagram Protocol (UDP) да бъдат забранени чрез адекватно конфигуриране на използваните софтуерни решения, хардуерни устройства и оборудване за защита и контрол на трафика;
4. Да се използва отделна, изолирана от другите информационни и комуникационни системи и от интернет, подходящо защитена среда (мрежа, система, софтуер и др.) за целите на администриране на информационните и комуникационните системи и техните компоненти. Тази среда трябва да не се използва за други цели;
5. Да се валидират всички входни данни, постъпващи от клиента, включително съдържанието, предоставено от потребителя и съдържанието на браузъра, като headers на препращащия и потребителски агент;
6. Всички данни да бъдат кодирани с HTML, изпращани от клиента и показвани в уеб страница;
7. Да се ограничават заявките и по-специално по максимална дължина на съдържанието, максимална дължина на заявката и максимална дължина на заявката по URL;
8. Да се конфигурира типът и размерът на headers, които уеб сървърът ще приеме;

9. Да се ограничава времетраенето на връзката (connection Timeout) - времето, за което сървърът изчаква всички headers на заявката, преди да я прекъсне, както и минималният брой байтове в секунда при изпращане на отговор на заявка:

   ✓ Да се въведе ограничение на броя неуспешни опити за влизане в системата;

   ✓ Да не се допуска извеждането на списък на уеб директориите;

10. Бисквитките (cookies) задължително да имат:

   ✓ флаг за защита (security flag), който инструктира браузъра, че „бисквитката“ може да бъде достъпна само чрез защитени SSL канали;

   ✓ флаг HTTP only, който инструктира браузъра, че „бисквитката“ може да бъде достъпна само от сървъра, а не от скриптовете, от страна на клиента;

11. Да се предвидят и предприемат мерки за защита на DNS за публичните системи, като задължително се прилага DNSSEC (Domain Name System Security Extensions);

12. По отношение на системните записи (Logs) да бъдат предвидени следните възможности:

   ✓ в сървъри за приложения, които поддържат критични дейности, сървъри от системната инфраструктура, сървъри от мрежовата инфраструктура, охранителни съоръжения, станции за инженеринг и поддръжка на индустриални системи, мрежово оборудване и работни места на администратори се регистрират автоматично всички събития, които са свързани най-малко с автентикация на потребителите, управление на профилите, правата на достъп, промени в правилата за сигурност и функциониране на информационните и комуникационните системи;

   ✓ за всяко от тези събития в записите се отбелязва с астрономическото време, когато е настъпило събитието;

13. Да бъде предвидена възможност за синхронизиране на часовниците на компоненти на информационните и комуникационните системи, като се използва протокол NTP V4 (Network Time Protocol, версия 4.0 и следващи), основан на RFC 5905 на IETF от 2010 г., като се осигурява хронометрична детерминация с времевата скала на UTC (Coordinated Universal Time), или аналогичен;

14. Да се предвиди информацията ще бъде архивирана за срок не по-кратък от дванадесет месеца.

ПРИЛОЖЕНИЕ 3

ТЕХНИЧЕСКИ ИЗИСКВАНИЯ ПРИ РАЗРАБОТВАНЕ НА СОФТУЕРЕН ПРОДУКТ

1. *Описание*

Настоящия документ има за цел да документира изискванията в софтуерният продукт. ……Описва се накратко какво представлява той. …….

2. *Изисквания към изпълнението – техническа спецификация*

Описват се подробно всички функционални изпикавания, които следва да притежава новият софтуерен продукт

3. *Изисквания за опазване на информацията*

*В описаната ИС ……. се/не се обработва информация, съдържаща лични данни. *Всички описани дейности в изискванията от документа следва да се изпълняват съгласно и при спазване на нормативните разпоредби, свързани с обработване на лични данни и обработване и критичната за образователната институция.*

4. *Изискванията за мрежова и информационна сигурност*

Тук се описват съотнесените изисквания свързани с МИС и киберсигурността. Пълните изисквания са описани в ПРИЛОЖЕНИЕ 1 и ПРИЛОЖЕНИЕ 2. От тях се избират само тези, които са относими.

5. *Изискванията за тестване*

Тестването следва да се извърши, както от гледна точка на функционалност, така и за спазване на изискванията за сигурност, за да се минимизира риска от уязвимости в приложението още на етапа на разработка.

6. *Оценка на риска*

В хода на анализа са/не са идентифицирани неприемливи рискове. Ако са идентифицирани рискове, те се описват, за да може в изискванията при разработка да се заложат конкретни стъпки, които да смекчат риска.

Екип по изготвяне на техническите изисквания:

Служител: ....., ..., ...

(име и фамилия) *(длъжност)* *(подпис)*

Служител: ....., ..., ...

(име и фамилия) *(длъжност)* *(подпис)*

Служител: ....., ..., ...

(име и фамилия) *(длъжност)* *(подпис)*

ПРИЛОЖЕНИЕ 4

ПРОТОКОЛ ЗА ТЕСТВАНЕ И ПУСКАНЕ В ЕКСПЛОАТАЦИЯ НА СОФТУЕРЕН ПРОДУКТ

Днес, ... 20..... г. *(дата),* екипа по тестване подписа настоящият протокол, като потвърждение на резултатите от теста, както следва:

1. **Функционални тестове**

Извършени са функционални тестове на софтуерният продукт и се установи, че всичко е реализирани , съгласно дефинираните изисквания.

2. **Тест за сигурност**

Не са открити критични проблеми със сигурността.

Ако са открити незначителни проблеми, те могат да се опишат тук или да се препоръчат мерки за смекчаване на установените проблеми.

ЗАКЛЮЧЕНИЕ:

Въз основа на извършените тестове за приемане и резултати от тях, считаме, че софтуерният продукт може да бъде пуснат в реална среда.

Екип по тестване:

Служител: ....., ..., ...
(име и фамилия) (длъжност) (подпис)

Служител: ....., ..., ...
(име и фамилия) (длъжност) (подпис)

Служител: ....., ..., ...
(име и фамилия) (длъжност) (подпис)

ОДОБРЕНИЕ ЗА ПУСКАНЕ В ЕКСПЛОАТАЦИЯ НА СОФТУЕРЕН ПРОДУКТ:

ОДОБРЕН ОТ:

Директор: ....., ...
(име и фамилия) (подпис)

ДЕТСКА ГРАДИНА „ПЪРВИ ЮНИ”, ГР. КЮСТЕНДИЛ,
КВ. ЗАПАД, ТЕЛ.: 078/ 55 20 73, e-mail: info-100060@edu.mon.bg

ДЕКЛАРАЦИЯ ЗА ПРИЛОЖИМОСТ
НА

ДГ“Първи юни“, град Кюстндил

Идентификатор на механизма за контрол	Име на механизма за контрола	Описание на механизма за контрола	Приложимост	Забележка
1	*2*	*3*	*4*	*5*
5	**Организационни механизми за контрол**			
5.1	**Политики за сигурността на информацията**	Политиката за сигурност на информацията и политики по конкретни теми би трябвало да бъдат определени, одобрени от ръководството, публикувани, съобщени на, и потвърдени от съответния персонал и съответните заинтересовани страни и преглеждани на планирани интервали, и ако настъпят значителни промени.	**проложимо**	
5.2	**Роли и отговорности за сигурността на информацията**	Ролите и отговорностите за сигурността на информацията би трябвало да бъдат определени и разпределени според нуждите на организацията.	**проложимо**	
5.3	**Разделяне на задълженията**	Противоречивите задължения и конфликтните зони на отговорност би трябвало да бъдат разделени.	**няма подобен тип зони.Задълженията са определени със заповед.**	

5.4	**Отговорности на ръководството**	Ръководството би трябвало да изисква от целия персонал да прилага сигурността на информацията в съответствие с установената политика за сигурност на информацията, политики по конкретни теми и процедури на организацията.	**проложимо**	
5.5	**Контакт с овластените органи**	Организацията би трябвало да установи и да поддържа контакт със съответните овластени органи.	**проложимо**	
5.6	**Контакт с групи със специални интереси**	Организацията би трябвало да установи и поддържа контакт с групи със специални интереси или други специализирани форуми по сигурността и професионални асоциации.	**не проложимо**	
5.7	**Събиране на сведения за заплахите**	Информацията, свързана със заплахите за сигурността на информацията, би трябвало да бъде **събирана и анализирана**, за да се получат сведения на заплахите	**проложимо**	
5.8	**Сигурност на информацията при управление на проекти**	Сигурността на информацията би трябвало да бъде интегрирана в управлението на проекти.	**проложимо**	
5.9	**Опис на информацията и други свързани активи**	Би трябвало да се разработи и поддържа опис на информацията и другите свързани активи, включително собствениците им.	**проложимо**	
5.1	**Допустимо използване на информация и**	Правилата за допустима употреба и процедурите за работа	**проложимо**	

	други свързани активи	с информация и другите свързани активи би трябвало да бъдат идентифицирани, документирани и внедрени.		
5.11	**Връщане на активи**	Персоналът и другите заинтересовани страни, според случая, при промяна или прекратяване на техния трудов договор, договор или споразумение би трябвало да върнат на организацията всички активи, които са в тяхно владение.	**проложимо**	
5.12	**Класификация на информацията**	Информацията би трябвало да бъде класифицирана в съответствие с нуждите на организацията от сигурност на информацията въз основа на поверителността, цялостност, наличността и приложимите изисквания на заинтересованите страни.	**проложимо**	
5.13	**Етикетиране на информацията**	Би трябвало да се разработи и внедри подходящ набор от процедури за етикетиране на информацията в съответствие със схемата за класификация на информацията, приета от организацията	**проложимо**	
5.14	**Пренос на информация**	Правилата, процедурите или споразуменията за трансфер на информация би трябвало да бъдат	**проложимо**	

		въведени за всички видове съоръжения за пренос в рамките на организацията и между организацията и други страни.		
5.15	**Механизъм за контрол на достъпа**	За контрол на физическия и логическия достъп до информацията и другите свързани активи би трябвало да се създадат и приложат правила, въз основа на изискванията за сигурност на бизнеса и информацията.	**проложимо**	
5.16	**Управление на идентичност**	Би трябвало да се управлява пълният жизнен цикъл на идентичностите.	**Управление от НЕИСПУО**	
5,17	**Информация за автентификация**	Разделението и управлението на информацията за автентификация би трябвало да бъде контролирано чрез процес на управление, включващ инструктиране на персонала относно подходящото боравене с информация за автентификация	**проложимо**	
5.18	**Права на достъп**	Правата на достъп до информацията и другите свързани активи би трябвало да бъдат предоставяни, преглеждани, променяни и премахвани в съответствие със политики по конкретни теми на организацията и правилата за контрол на достъпа.	**проложимо ЧРЕЗ ЗАПОВЕДИ**	
5.19	**Сигурност на информацията при взаимоотношенията**	Би трябвало да се определят и внедрят процеси и процедури за	**проложимо**	

	с доставчици	управление на рисковете за сигурността на информацията, асоциирани с използването на продукти или услуги на доставчика.		
5.20	**Поддържане на сигурността на информацията в рамките на споразуменията с доставчици**	С всеки доставчик би трябвало да бъдат въведени и съгласувани съответните изисквания за сигурност на информацията, въз основа на вида на взаимоотношенията с доставчика.	**проложимо**	
5,21	**Управление на сигурността на информацията във веригата за ИКТ доставки**	Би трябвало да се определят и прилагат процеси и процедури за управление на рисковете за сигурността на информацията, свързани с веригата за доставка на ИКТ продукти и услуги.	**проложимо**	
5.22	**Мониторинг, преглед и управление на промените в услугите на доставчиците**	Организацията би трябвало редовно да осъществява мониторинг, да преглежда, да оценява и да управлява промените в практиките за сигурност на информацията на доставчиците и в предоставянето на услугите.	**НЕ проложимо**	
5.23	**Сигурност на информацията при използване на услуги в облак**	Би трябвало да се въведат процеси за придобиване, използване, управление и излизане от облачни услуги в съответствие с изискванията на организацията за сигурност на	**проложимо използва се само от гл.счетоводител**	

		информацията		
5.24	**Планиране и подготовка за управлението на инциденти, свързани със сигурността на информацията**	Организацията би трябвало да планира и да се подготви за управлението на инциденти, свързани със сигурността на информацията, посредством определяне, създаване и съобщаване на процесите по управление на инциденти, свързани със сигурността на информацията, на ролите и на отговорностите.	**проложимо**	
5.25	**Оценяване и вземане на решение относно събития, свързани със сигурността на информацията**	Организацията би трябвало да оцени събитията, свързани със сигурността на информацията и да реши дали те да бъдат категоризирани като инциденти със сигурността на информацията.	**проложимо**	
5.26	**Реагиране на инциденти, свързани със сигурността на информацията**	На инцидентите, свързани със сигурността на информацията би трябвало да се реагира в съответствие с документираните процедури.	**проложимо**	
5.27	**Извличане на поуки от инцидентите, свързани със сигурността на информацията**	Знанията, придобити от инцидентите, свързани със сигурността на информацията, би трябвало да се използват за укрепване и усъвършенстване на механизмите за контрол на сигурността на информацията.	**проложимо**	

5.28	**Събиране на доказателства**	Организацията би трябвало да създаде и внедри процедури за идентифициране, събиране, придобиване и опазване на доказателствата, отнасящи се до събития, свързани със сигурността на информацията.	**проложимо**	
5.29	**Сигурност на информацията по време на прекъсване**	Организацията би трябвало да планира как да поддържа сигурността на информацията на подходящо ниво по време на прекъсване.	**проложимо**	
5.30	**Готовност на ИКТ за непрекъснатост на бизнеса**	Готовността на ИКТ би трябвало да се планира, прилага, поддържа и тества въз основа на целите за непрекъснатост на бизнеса и изискванията за непрекъснатост на ИКТ.	**проложимо**	
5.31	**Правни, законови, регулаторни и договорни изисквания**	Правните, законовите, регулаторните и договорните изисквания, свързани със сигурността на информацията и подходът на организацията за изпълнение на тези изисквания, би трябвало да бъдат идентифицирани, документирани и актуализирани	**проложимо**	
5.32	**Права върху интелектуална собственост**	Организацията би трябвало да въведе подходящи процедури за защита на правата върху интелектуалната собственост		
5.33	**Защита на записи**	Записите трябва да бъдат защитени от загуба, унищожаване,	**проложимо в архив**	

		фалшифициране, неоторизиран достъп и неоторизирано изтичане		
5.34	**Право на неприкосновеност на личния живот и защита на ЛИИ**	Организацията би трябвало да идентифицира и отговори на изискванията по отношение на опазването на правото на неприкосновеност на личния живот и защита на личната информация за идентифициране (ЛИИ) съгласно приложимите закони и разпоредби и договорните изисквания.	**проложимо**	
5.35	**Независим преглед на сигурността на информацията**	Подходът на организацията към управлението на сигурността на информацията и неговото въвеждане, включващо хора, процеси и технологии, би трябвало да се подлага на независим преглед през планирани интервали или когато настъпят значителни промени.	**проложимо**	
5.36	**Съответствие с политики, правила и стандарти за сигурност на информацията**	Съответствието с политиката за сигурност на информацията на организацията, политиките по конкретни теми, правилата и стандартите би трябвало да се подлагат на редовни прегледи.	**проложимо**	
5.37	**Документирани оперативни процедури**	Оперативните процедури за съоръженията за обработване на информация би	**проложимо**	

		трябвало да са документирани и предоставени на персонала, който се нуждае от тях.		
6	**Механизми за контрол на хората**			
6.1	**Скрининг**	Проверките на биографичните данни/компетентността на всички кандидати, за да бъдат назначени като персонал, би трябвало да се извършват преди постъпването им в организацията и на постоянна основа, като се отчитат приложимите закони, нормативни актове и етични норми и би трябвало да бъдат пропорционални на бизнес изискванията и класификацията на информацията, до която ще се осъществява достъп и предполагаемите рискове	**проложимо**	
6.2	**Условия за наемане на работа**	Трудовите договори би трябвало да посочват отговорностите на персонала и организацията за сигурността на информацията.	**проложимо**	
6.3	**Осъзнаване, образование и обучение в областта на сигурността на информацията**	Персоналът на организацията и съответните заинтересовани страни би трябвало да получат подходящо осъзнаване, образование и обучение в областта на сигурността на информацията, а също така и редовните	**проложимо**	

		актуализации на политиката за сигурност на информацията на организацията и политики по конкретна тема и процедури, съответстващи на заеманата от лицата длъжност.		
6.4	**Дисциплинарен процес**	Дисциплинарният процес би трябвало да бъде официализиран и съобщен, за да се предприемат действия срещу персонала и другите заинтересовани страни, които са извършили нарушение на политиката за сигурност на информацията.	**проложимо**	
6.5	**Отговорности след прекратяване или промяна на трудовото правоотношение**	Отговорностите и задълженията в областта на сигурността на информацията, които остават валидни след прекратяване или промяна на трудово правоотношение, би трябвало да бъдат определени, наложени и съобщени на съответния персонал и на другите заинтересовани страни.	**проложимо**	
6.5	**Споразумения за поверителност или не разкриване на информация**	Споразуменията за поверителност или неразкриване на информация, отразяващи нуждите на организацията за защита на информацията, би трябвало да бъдат определени, документирани, редовно преглеждани и подписани от	**проложимо**	

		персонала и съответно от другите заинтересовани страни.		
6.7	**Дистанционна работа**	Когато персоналът работи от разстояние би трябвало да се прилагат мерки за сигурност, за да се защити информацията, която е достъпна, обработвана или съхранявана извън помещенията на организацията.	**не проложимо/ не се извършва дистанционна работа**	
6.8	**Докладване на събития, свързани със сигурността на информацията**	Организацията би трябвало да осигури на персонала механизъм за своевременно докладване чрез подходящи канали за наблюдавани или подозрителни събития, свързани със сигурността на информацията.	**проложимо**	
7	**Механизми за контрол за физическа сигурност**			
7.1	**Периметри на физическата сигурност**	Би трябвало да бъдат определени и използвани периметри за сигурност за защита на зони, които съдържат информация и други свързани активи.	**проложимо**	
7.2	**Физическо влизане**	Сигурните зони трябва да бъдат защитени с подходящи механизми за контрол на влизането и точки за достъп.	**проложимо**	
7.3	**Обезопасяване на офиси, стаи и съоръжения**	Физическата сигурност на офисите, стаите и съоръженията би трябвало да бъде проектирана и изпълнена.	**проложимо**	
7.4	**Мониторинг на физическата сигурност**	В помещенията би трябвало да се извършва непрекъснат	**проложимо**	

		мониторинг за неоторизиран физически достъп.		
7.5	**Защита срещу физически заплахи и заплахи от обкръжаващата среда**	Би трябвало да бъде проектирана и внедрена защита срещу физическите заплахи и заплахите от обкръжаващата среда, като например природни бедствия и други умишлени или непреднамерени физически заплахи за инфраструктурата.	**проложимо**	
7.6	**Работа в защитени зони**	Би трябвало да бъдат проектирани и приложени мерки за сигурност при работа в защитени зони.	**Няма защитени зони**	
7.7	**Чисто бюро и чист екран**	Би трябвало да се определят и да се прилагат по подходящ начин правила за чисто бюро по отношение на документи и сменяеми носители за съхранение и правилата за чист екран по отношение на съоръженията за обработване на информация.	**проложимо**	
7.8	**Разположение и защита на оборудването**	Оборудването би трябвало да бъде разположено по сигурен и защитен начин.	**проложимо**	
7.9	**Защита на активи извън организацията**	Активите извън организацията би трябвало да са защитени.		
7.10	**Носители за съхранение на информация**	Носителите за съхранение би трябва да се управляват през жизнения им цикъл на придобиване, използване, транспортиране и унищожаване, в съответствие със	**проложимо**	

		схемата за класификация на организацията и изискванията за манипулиране.		
7.11	**Поддържащи комунални услуги**	Съоръженията за обработване на информация би трябвало да са защитени от прекъсване на електрозахранването и други смущения, причинени от аварии в поддържащите комунални услуги.	**проложимо**	
7.12	**Защита на окабеляването**	Кабелите за захранване, за данни или поддържащите кабели за информационни услуги би трябвало да са защитени от прихващане, смущения или повреди.	**проложимо**	
7.13	**Поддръжка на оборудването**	Оборудването би трябвало да се поддържа правилно, за да се осигури наличността, цялостност и поверителността на информацията.	**проложимо**	
7.14	**Сигурно ликвидиране или повторна употреба на оборудването**	Компонентите на оборудване, съдържащо носители за съхранение, би трябвало да бъдат проверени, за да се гарантира, че всички чувствителни данни и лицензиран софтуер са премахнати или надеждно презаписани преди унищожаването или повторната им употреба.	**проложимо**	
8	**Технологични механизми за контрол**			

8.1	**Потребителски крайни устройства**	Информацията, съхранявана, обработвана от или достъпна чрез потребителски крайни устройства, би трябвало да бъде защитена.	**проложимо**	
8.2	**Права за привилегирован достъп**	Разделението и използването на правата за привилегирован достъп би трябвало да се ограничава и управлява.	**проложимо**	
8.3	**Ограничаване на достъпа до информация**	Достъпът до информацията и другите свързани активи би трябвало да бъде ограничен в съответствие с установената политика по конкретна тема за контрол на достъпа.	**проложимо**	
8.4	**Достъп до изходния код**	Достъпът за четене и запис до изходен код, инструменти за разработване и софтуерни библиотеки би трябвало да се управлява по подходящ начин.	**не проложимо**	
8.5	**Сигурна автентификация**	Технологиите и процедурите за сигурна автентификация би трябвало да се прилагат въз основа на ограниченията за достъп до информацията и политика по конкретна тема за контрол на достъпа.	**чрез НЕИСПУО**	
8.6	**Управление на капацитета**	Използването на ресурсите би трябвало да се контролират и коригират в съответствие с текущите и очакваните изисквания за	**проложимо**	

		капацитет.		
8.7	**Защита срещу злонамерен софтуер**	Защитата срещу злонамерен софтуер би трябвало да бъде въведена и поддържана чрез подходящо осъзнаване на потребителите.	**проложимо**	
8.8	**Управление на технически уязвимости**	Би трябвало да се получи информация за техническите уязвимости на информационните системи, които се използват, за да се оцени как е подложена организацията на такива уязвимости и да се вземат подходящите мерки.	**проложимо**	
8.9	**Управление на конфигурация**	Конфигурациите, включително конфигурации за сигурност, на хардуер, софтуер, услуги и мрежи би трябвало да бъдат установени, документирани, внедрени, контролирани и подлагани на преглед.	**не проложимо**	
8.10	**Изтриване на информация**	Информацията, съхранявана в информационни системи, устройства или в други носители за съхранение, би трябвало да се изтрива, когато вече не е необходима.	**проложимо**	
8.11	**Маскиране на данни**	Маскирането на данни би трябвало да се използва в съответствие с политиката по конкретни теми на организацията за контрол на достъпа и	**не проложимо**	

		другите свързани политики по конкретна тема и с изискванията на бизнеса, като се вземе предвид приложимото законодателство.		
8.12	**Предотвратяване на изтичането на данни**	Мерките за предотвратяване на изтичане на данни би трябвало да се прилагат към системи, мрежи и всякакви други устройства, които обработват, съхраняват или предават чувствителна информация.	**проложимо**	
8.13	**Резервиране на информацията**	Резервните копия на информацията, софтуерът и системите би трябвало да се поддържат и редовно да се тестват в съответствие със съгласуваната политика по конкретна тема за резервиране на информацията.	**проложимо**	
8.14	**Резервиране на средства за обработване на информация**	Средствата за обработване на информация би трябвало да бъдат внедрявани с резерв, достатъчен, за да отговори на изискванията за наличност.	**проложимо**	
8.15	**Регистриране (Влизане в системата)**	Би трябвало да се създадат, съхраняват, защитават и анализират регистрационни дневници, които записват дейности, изключения, неизправности и други съответни събития.	**проложимо**	
8.16	**Дейности по мониторинг**	Мрежите, системите и приложенията би трябвало да бъдат	**проложимо**	

		подложени на мониторинг за аномално поведение и да се предприемат подходящи действия за оценяване на потенциалните инциденти, свързани със сигурността на информацията.		
8.17	**Синхронизация на часовниците**	Часовниците на системите за обработване на информация, използвани от организацията, би трябвало да се синхронизират с одобрени източници на време.	**проложимо**	
8.18	**Използване на привилегировани спомагателни програми**	Използването на помощни програми, които може да заменят механизмите за контрол на системата и приложенията, би трябвало да бъде ограничено и строго контролирано.	**проложимо**	
8.19	**Инсталиране на софтуер върху операционни системи**	Би трябвало да се въведат процедури и мерки за сигурно управление на инсталирането на софтуер в работещи системи.	**проложимо**	
8.20	**Сигурност на мрежите**	Мрежите и мрежовите устройства би трябвало да бъдат защитени, управлявани и контролирани, за да се защити информацията в системите и приложенията.	**проложимо**	
8.21	**Сигурност на мрежовите услуги**	Механизмите за сигурност, нивата на услуги и изискванията за обслужване на мрежовите услуги би трябвало да бъдат	**проложимо**	

		идентифицирани, внедрени и подложени на мониторинг.		
8.22	**Разделяне на мрежите**	Групите информационни услуги, потребители и информационни системи би трябвало да бъдат разделени в мрежите на организацията.	**проложимо**	
8.23	**Уеб филтриране**	Достъпът до външни уебсайтове би трябвало да се управлява, за да се намали излагането на злонамерено съдържание.		
8.24	**Използване на криптография**	Правилата за ефективното използване на криптографията, включително управлението на криптографски ключове, би трябвало да бъдат определени и приложени.	**не се включва в дейността на институцията**	
8.25	**Жизнен цикъл на сигурно разработване**	Би трябвало да се създадат и прилагат правила за сигурно разработване на софтуер и системи.	**не се включва в дейността на институцията**	
8.26	**Изисквания за сигурност на приложението**	При разработване или придобиване на приложения би трябвало да бъдат идентифицирани, специфицирани и одобрени изискванията за сигурност на информацията.	**не се включва в дейността на институцията**	
8.27	**Архитектура на сигурни системи и принципи на инженеринга**	Принципите за инженеринг на сигурни системи би трябвало да бъдат установени, документирани, поддържани и приложени към всякакви дейности по	**не се включва в дейността на институцията**	

		разработване на информационните системи.		
8.28	**Сигурно кодиране**	При разработването на софтуер би трябвало да се прилагат принципите на сигурно кодиране.	**не се включва в дейността на институцията**	
8.29	**Тестване на сигурността при разработване и приемане**	Процесите на тестване на сигурността би трябвало да се определят и внедрят в жизнения цикъл на разработването.	**не се включва в дейността на институцията**	
8.30	**Разработване от външни изпълнители**	Организацията би трябвало да посочва, контролира и подлага на прегледи дейностите, свързани с външното разработване на системи.	**проложимо**	
8.31	**Разделяне на средата за разработване, тестване и производство**	Обкръжаващите среди за разработване, тестване и производство би трябвало да са разделени и защитени.	**не се включва в дейността на институцията**	
8.32	**Управление на промените**	Промените в съоръженията за обработване на информация и информационните системи би трябвало да бъдат предмет на процедурите за управление на промените.	**проложимо**	
8.33	**Информация за тестването**	Информация за тестването би трябвало да бъде подходящо подбрана, защитена и управлявана.	**проложимо**	
8.34	**Защита на информационните системи при одитно тестването**	Одитните тестове и другите дейности за осигуряване на увереност, включващи оценяване на операционните системи, би трябвало да се планират и	**проложимо**	

		съгласуват между лицето, провеждащо теста и съответното ръководство.		

ДЕТСКА ГРАДИНА „ПЪРВИ ЮНИ”, ГР. КЮСТЕНДИЛ,
КВ. ЗАПАД, ТЕЛ.: 078/ 55 20 73,
e-mail: info-100060@edu.mon.bg /dg_1juny@abv.bg

ЗАПОВЕД

№ ...../..... ..... 20..... г.

На чл. 259, ал. 1 от Закона за предучилищното и училищното образование, във връзка с чл. 4, ал. 1 от Наредба за минималните изисквания за мрежова и информационна сигурност, с цел обезпечаване на дейността по мрежова и информационна сигурност в ДГ “Първи юни“, град Кюстендил

I. У Т В Ъ Р Ж Д А В А М:

Политика за мрежова и информационна сигурност, ведно с всички допълнителни документи документите за системата за управление на сигурност на информацията както следва:

- Политика управление на атхивирането
  - Политика за регистриране на наблюдение
  - Политика за управление на уязвимост и корекции
  - Политика за управление на промени
  - Политика за управление на инциденти
  - Политика за използване на облачни услуги
  - Политика за преглед от ръководството за ефикасността на системата за управление на информационната сигурност

  - План за непрекъсваемост на дейността

VII. ПРОЦЕДУРИ:

- Процедура за управление на инциденти
  Приложение 1- Формата за докладване на инцидент свързан с информационната сигурност .
  Приложение № 2- Регистър за инциденти, свързан с информационната сигурност

- Процедура за съответствие на СУИС с нормативните изисквания
- Процедура за сигурно разработване,развитиеи поддържане на софтуерен продукт

II. Н А Р Е Ж Д А М:

1. Копие от Политиката за мрежова и информационна сигурност и всички документи свързани със Системата за управление на информационната сигурност (СУИС) да бъдат оставени в *дирекцията* и домакинската стая, за да са общодостъпни за всички служители.

2. Ефикасността на системата ще бъде проверявана редовно, чрез извършването на одити в ДГ “Първи юни“, град Кюстендил

В срок до .... 20..... г. Емилия Сотирова-ЗАС/домакин да сведе настоящата заповед до знанието на отговорните длъжностни лица срещу подпис за сведение и изпълнение.

Контрол по изпълнение на заповедта упражнявам лично.

ДИРЕКТОР:
Анелия Стоймирова

Запознати със съдържанието на заповедта:

№ по ред	Име и фамилия	Заемана длъжност	Дата	Подпис на лицето
1	Антоанета Мишева			
2	Силвия Николова-Атова			
3	Илиана Георгиева			
4	Теодора Тимова-Рублева			
5	Елена Миленска			
6	Снежана Сахатчийска			
7	Аглика Бончева			

8	Бориславa Борисова-Радославова			
9	Александра Костова			
10	Галина Дюлгерова			
11	Десислава Костова			
12	Гергана Крумова			
13	Румяна Матуска			
14	Надя Помпулуска			
15	Даниела Грозданова			
16	Екатерина Иванова			
17	Теодора Янчева			
18	Силвия Петкова			
19	Мая Найденова			
20	Донка Димитрова			
21	Антоанета Василиева			
22	Емилия Сотирова			
23	Павлета Анева			
24	Ивета Димитрова			

ДЕТСКА ГРАДИНА „ПЪРВИ ЮНИ”, ГР. КЮСТЕНДИЛ,
КВ. ЗАПАД, ТЕЛ.: 078/ 55 20 73, e-mail: info-100060@edu.mon.bg

ЗАПОВЕД

№ ...../..... ..... 20..... г.

На чл. 259, ал. 1 от Закона за предучилищното и училищното образование, във връзка с чл. 3, ал. 1, т. 3 и т. 5 от Наредба за минималните изисквания за мрежова и информационна сигурност, с цел обезпечаване на дейността по мрежова и информационна сигурност в ДГ“Първи юни“,град Кюстендил.

I . С Ъ З Д А В А М :

I. Съвет по информационна сигурност в ДГ“Първи юни“,град Кюстендил като постоянно действащ орган по информационната сигурност в ДГ“Първи юни“,град Кюстендил, в състав:

1. **Председател:**

Анелия Стоймирова – директор

2. **Членове**:

2.1. Десислава Костова – заместник-директор

2.3. Емилия Сотирова – отговорен служител по информационна сигурност

и Администратора на ИКС

2.4. Донка Димитрова– гл.счетоводител

II. Н А Р Е Ж Д А М:

1. Във връзка с прилагането на Политиката по мрежова и информационна сигурност на ДГ“Първи юни“,град Кюстендил, Съвета по информационна сигурност да обсъжда стратегическите въпроси по информационната сигурност и да взема решения по обсъдените въпроси.
2. Съвета по информационна сигурност се свиква на заседание от председателя, или по искане на всеки от членовете му, след предварително съгласуване с председателя, минимум веднъж в годината или при необходимост

3. Заседанията на Съвета по информационна сигурност се ръководят от председателя на съвета, а при отсъствието му, от друг член на Съвета, предварително определен от председателя.

4. Дневният ред и материалите за заседанията се изпращат на членовете на Съвета най-малко 5 работни дни преди датата на заседанието. Мотивирани предложения за промени в дневния ред може да внася всеки член на Съвета по информационна сигурност най-късно до началото на заседанието.

5. За всяко заседание на Съвета по информационна сигурност се съставя протокол, който се подписва от всички членове. В протокола се вписват дата на провеждане, час на откриване на заседанието, приетия дневен ред, изказванията на членовете на Съвета, решенията, които са взети и час на закриване на заседанието.

В срок до .... 2025 г. Емилия Сотирова, на длъжност ЗАС/домакин да сведе настоящата заповед до знанието на отговорните длъжностни лица срещу подпис за сведение и изпълнение.

Контрол по изпълнение на заповедта упражнявам лично.

ДИРЕКТОР: …….
Анелия Стоймирова

Запознати със съдържанието на заповедта:

№ по ред	Име и фамилия	Заемана длъжност	Дата	Подпис на лицето

ДЕТСКА ГРАДИНА „ПЪРВИ ЮНИ”, ГР.КЮСТЕНДИЛ,
КВ. „ЗАПАД”, ТЕЛ: 078/55 20 73, e-mail: info-1000060@edu.mon.bg

УТВЪРЖДАВАМ:
АНЕЛИЯ СТОЙМИРОВА
Директор на ДГ „Първи юни”
Заповед № /……..2025г.

ДОКЛАД
ЗА СЪСТОЯНИЕТО НА
ИНФОРМАЦИОННАТА СИГУРНОСТ
НА

ДГ“Първи юни“, град Кюстендил

1. ВЪВЕДЕНИЕ

.....
.....
.....

Докладът представя текущото състояние на информационната сигурност в образователната институция в съответствие с изискванията на ISO 27001. Обхватът на доклада включва оценка на системата за управление на информационната сигурност (СУИС), идентифициране на рисковете и предложения за подобрения.

2. ОРГАНИЗАЦИОННА РАМКА

.....

.....

.....

Описва се организационната структура и отговорностите във връзка с информационната сигурност. Включва се информация за определените роли и отговорности, както и за комуникационните и координационни механизми.

3. ОЦЕНКА НА СЪОТВЕТСТВИЕТО

.....

.....

.....

Процесът на оценка включва проверка на съответствието на текущата информационна сигурност с изискванията на ISO 27001. В този раздел се описват резултатите от оценката, включително идентифицираните отклонения от стандарта.

4. ИДЕНТИФИКАЦИЯ НА РИСКОВЕТЕ

.....

.....

.....

Извършва се анализ на риска, като се идентифицират потенциалните заплахи и уязвимости в информационната сигурност. Определят се нивото на риск и възможните последици. Резултатите от анализа на риска се използват за приоритизиране на мерките за сигурност.

5. ПОЛИТИКА И ПРОЦЕДУРИ ЗА ИНФОРМАЦИОННА СИГУРНОСТ

.....

.....

.....

Докладът описва текущата политика и процедури за информационна сигурност, включително подходите за управление на достъпа, криптирането, защитата на данните и др. Оценява се съответствието на политиката и процедурите с изискванията на ISO 27001.

6. ФИЗИЧЕСКА И ОКОЛНА СИГУРНОСТ

.....

.....

.....

Разглежда се състоянието на физическата и околната сигурност в образователната институция. Включва оценка на мерките за контрол на достъпа до физическите обекти и оборудването, системите за наблюдение, защитата от пожар и други рискове.

7. УПРАВЛЕНИЕ НА РИСКА

.....

.....

.....

Описва се текущият подход към управлението на риска в образователната институция. Включва се оценка на ефективността на съществуващите мерки за управление на риска и предложения за подобрения.

8. ОБУЧЕНИЕ И ОСВЕДОМЕНОСТ

.....

.....

.....

Процесът на обучение и осведомяване на персонала относно информационната сигурност се оценява в този раздел. Включват се информация за проведените обучения и насочени мерки за повишаване на осведомеността на персонала.

9. ИЗПЪЛНЕНИЕ НА МЕРКИ ЗА СИГУРНОСТ

.....

.....

.....

Оценява се изпълнението на конкретните мерки за сигурност, определени в СУИС. Включва се информация за проведените проверки и аудити, както и резултатите от тях.

10. ПОДОБРЕНИЯ И НАБЛЮДЕНИЕ

.....

.....

.....

Последният раздел отразява предложенията за подобрения на информационната сигурност и мерките, които трябва да бъдат предприети. Описва се текущата практика за наблюдение и преглед на системата за управление на информационната сигурност.

Изготвил:

....

(име и фамилия) *(длъжност)* *(подпис)*

Съгласувал:

....

(име и фамилия) *(длъжност)* *(подпис)*

ИНСТРУКЦИЯ № 1 от 21 декември 2016 г.

за обстоятелствата, при които предприятията, предоставящи обществени електронни съобщителни услуги, уведомяват потребителите за нарушения на сигурността на личните данни, формата и начина на уведомяването

Издадена от Комисията за защита на личните данни, обн., ДВ, бр. 1 от 3.01.2017 г., в сила от 7.01.2017 г., изм., бр. 9 от 30.01.2024 г., в сила от 30.01.2024 г.

Глава първа

ОБЩИ ПОЛОЖЕНИЯ

Чл. 1. С тази инструкция се определят обстоятелствата, при които предприятията, предоставящи обществени електронни съобщителни услуги, уведомяват потребителите за нарушения на сигурността на личните им данни, формата и начина на уведомяването.

Чл. 2. Инструкцията се отнася до всички предприятия, които са вписани в публичния регистър на предприятията по чл. 33, ал. 1, т. 1 от Закона за електронните съобщения (ЗЕС), поддържан от Комисията за регулиране на съобщенията.

Глава втора

ОБСТОЯТЕЛСТВА, ПРИ КОИТО ПРЕДПРИЯТИЯТА, ПРЕДОСТАВЯЩИ ОБЩЕСТВЕНИ ЕЛЕКТРОННИ СЪОБЩИТЕЛНИ УСЛУГИ, УВЕДОМЯВАТ ПОТРЕБИТЕЛИТЕ ЗА НАРУШЕНИЯ НА СИГУРНОСТТА НА ЛИЧНИТЕ ДАННИ

Чл. 3. (1) В случай на нарушение на сигурността на личните данни по смисъла на § 1, т. 34а от допълнителните разпоредби на ЗЕС, което може да повлияе неблагоприятно на лични данни или на неприкосновеността на личния живот на абонат или на друго физическо лице, предприятието, при което е настъпило нарушението на сигурността, уведомява своевременно съответното лице за нарушението, но не по-късно от три дни от установяването му.

(2) Предприятието не уведомява абоната или друго физическо лице, в случай че Комисията за защита на личните данни (КЗЛД) е приела, че предприятието е предприело предхождащи подходящи технологични мерки за защита на сигурността на личните данни – обект на нарушението, при условията на чл. 261в, ал. 3 ЗЕС.

(3) В случаите по ал. 1 след разглеждане на възможните неблагоприятни последици от нарушението КЗЛД може да възложи на предприятието да уведоми съответните неуведомени засегнати лица по ал. 1.

Чл. 4. Извън случаите по чл. 3, ал. 2 предприятието не извършва уведомяване и когато са налице обстоятелствата по чл. 3, параграф 5 от Регламент (ЕС) № 611/2013 на Комисията от 24 юни 2013 г. относно мерките, приложими за съобщаването на нарушения на сигурността на личните данни съгласно Директива 2002/58/ЕО на Европейския парламент и на Съвета за правото на

неприкосновеност на личния живот и електронни комуникации.

Чл. 5. (Изм. – ДВ, бр. 9 от 2024 г., в сила от 30.01.2024 г.) При определянето, че дадено нарушение на сигурността на личните данни може да повлияе неблагоприятно на лични данни или на неприкосновеността на личния живот на абонат или на друго физическо лице, предприятието отчита следните обстоятелства:

1. категориите лични данни – обект на нарушение на сигурността, като данни по чл. 9, параграф 1 от Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 г. относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни и за отмяна на Директива 95/46/ЕО (Общ регламент относно защитата на данните); данни по чл. 248, ал. 2 ЗЕС; данни по чл. 3, параграф 2, буква "а" от Регламент (ЕС) № 611/2013;

2. характера на нарушението на сигурността на личните данни и вероятните последици от него за засегнатия абонат или друго физическо лице, като някоя от последиците, посочени в чл. 3, параграф 2, буква "б" от Регламент (ЕС) № 611/2013; загуба или промяна на данни; незаконно унищожаване; нерегламентиран достъп.

Глава трета

ФОРМА И НАЧИН НА УВЕДОМЯВАНЕ

Чл. 6. Предприятието уведомява абоната или друго физическо лице за настъпилото нарушение на сигурността на личните данни в разбираема форма. Уведомлението задължително съдържа информацията по Приложение II от Регламент (ЕС) № 611/2013.

Чл. 7. При спазване на изискванията на чл. 3, параграф 6 от Регламент (ЕС) № 611/2013 предприятието уведомява абоната или друго физическо лице чрез средства за комуникация, гарантиращи незабавното получаване на информацията по чл. 6.

Чл. 8. (1) В случаите по чл. 3, параграф 7 от Регламент (ЕС) № 611/2013 предприятието прави обявление в две или повече национални и/или регионални медии. Обявлението в този случай е в срока по чл. 3.

(2) След идентифициране на всички засегнати от нарушението лица предприятието незабавно уведомява всяко от тях, като им предоставя информацията по чл. 6, с изключение на случаите, когато това е невъзможно или е свързано с прекомерни усилия.

ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

§ 1. Тази инструкция е приета на основание чл. 261г, ал. 1 ЗЕС с решение на КЗЛД от 21.12.2016 г.