

МИНИСТЕРСТВО НА ОБРАЗОВАНИЕТО И НАУКАТА
11 ОУ“СВЕТИ ПИМЕН ЗОГРАФСКИ“

София, район Изгрев, ул. Никола Габровски 22, тел. 02/8627248,

e-mail: info-2205011@edu.mon.bg

ПОЛИТИКА ПО МРЕЖОВА И ИНФОРМАЦИОННА СИГУРНОСТ НА
11.ОУ „СВЕТИ ПИМЕН ЗОГРАФСКИ“

1. ОБХВАТ И ПРИЛОЖИМОСТ

Политиката обхваща всички аспекти на дейността на училищната администрация, свързани с информационната сигурност. Тя се отнася до всички служители, независимо от длъжност и ниво в йерархията. В нейния обхват попадат всички информационни системи и бази данни, използвани от училището, както и всички устройства, свързани с информационната инфраструктура. Важен аспект на приложимостта е включването на процесите по предоставяне на електронни образователни услуги, които представляват съществена част от взаимодействието с учениците и родителите. Политиката обхваща също външните доставчици на ИТ услуги и поддръжка, както и всички партньори, които имат достъп до информационни ресурси на училището.

2. ОСНОВНИ ПРИНЦИПИ И ЦЕЛИ

2.1. Принципи

Училищната политика по киберсигурност се основава на следните принципи:

1. Поверителността осигурява защита на информацията от неоторизиран достъп, гарантирайки че само упълномощени лица могат да получат достъп до чувствителни данни.
2. Целостта като принцип защитава точността и непроменяемостта на данните, предотвратявайки неоторизирани модификации.
3. Наличността гарантира, че информацията и системите са достъпни за оторизираните потребители в момента, когато имат нужда от тях, което е от съществено значение за непрекъснатостта на административните процеси.
4. Принципът на отчетност позволява проследяване на действията на всички потребители, създавайки ясна следа за отговорност.
5. Допълвайки общата рамка, принципът на неотричане гарантира, че извършените действия в системите не могат да бъдат отречени от лицата, които са ги предприели.

2.2. Цели

Политиката по киберсигурност има следните цели:

1. Защитата на информационните активи от външни и вътрешни заплахи, което включва предотвратяване на неоторизиран достъп, промяна или унищожаване на информацията.
2. Спазването на законовите и регулаторни изисквания.
3. Минимизирането на риска от инциденти, свързани с киберсигурността, цели ограничаване на потенциалните щети и разходи в случай на нарушение на сигурността.
4. Осигуряването на непрекъснатост на услугите при възникване на инциденти позволява училището да продължи да функционира ефективно дори при проблеми със сигурността.
5. Повишаването на осведомеността на служителите е особено важно, тъй като човешкият фактор е най-уязвимото звено в защитата на информацията.
6. Ефективното управление на взаимоотношенията с външни доставчици на ИТ услуги.

3. ОРГАНИЗАЦИОННА СТРУКТУРА И ОТГОВОРНОСТИ

3.1. Ръководство

Директорът на училището носи крайната отговорност за цялостното състояние на киберсигурността в организацията. Неговата роля е от стратегическо значение, тъй като осигурява необходимите ресурси в рамките на бюджетните възможности на училището.

3.2. Отговорно лице за мрежова и информационна сигурност

В съответствие със Закона за киберсигурност в училището се определя Отговорно лице за мрежова и информационна сигурност (ОЛМИС). Съгласно чл. 16 от ЗКС, ОЛМИС отговаря за мрежовата и информационната сигурност в училищната администрация. Това лице координира всички дейности по киберсигурността, включително разработване и актуализиране на вътрешните политики и процедури. ОЛМИС отговаря за своевременното докладване на инциденти съгласно законовите изисквания. Важна част от неговите отговорности е координирането на обученията на служителите относно киберзаплахите и добрите практики. За осигуряване на бързо вземане на решения, ОЛМИС докладва директно на директора на училището по всички въпроси, свързани с киберсигурността, без междинни нива на управление.

3.3. Външни доставчици на ИТ услуги

Тези доставчици осигуряват необходимата техническа експертиза и поддръжка, която не би могла да бъде осигурена с вътрешни ресурси. Те са отговорни за внедряването и управлението на технически мерки за сигурност, като антивирусна защита, защитни стени, системи за откриване на проникване и други. При възникване на инциденти, външни ИТ специалисти оказват съдействие за ограничаване на щетите и възстановяване на нормалната работа. Те също така предоставят редовни консултации и препоръки за подобряване на цялостната сигурност на информационната инфраструктура.

3.4. Отговорности на служителите в училището

Всички служители на училището имат съществена роля в поддържането на ефективна система за киберсигурност. Те са длъжни да се запознаят и стриктно да спазват всички правила за киберсигурност, приложими за тяхната дейност. Отговорността на служителите включва своевременно докладване на подозрителни дейности или инциденти на ОЛМИС, като предоставят цялата налична информация, която би помогнала за бърза реакция. Активното участие в организираните обучения по киберсигурност е задължение на всички служители, тъй като повишаването на информираността е ключов елемент от общата защита. В ежедневната си работа, служителите трябва да използват информационните системи отговорно и в съответствие с установените изисквания, като избягват рисково поведение, което би могло да застраши сигурността на училищните информационни активи.

4. УПРАВЛЕНИЕ НА РИСКА

4.1. Базова оценка на риска

Управлението на риска започва с процес на оценка на риска. Отговорно лице за мрежова и информационна сигурност, с помощта на преподаватели по КМ/КМИТ от училището или външния ИТ доставчик, извършва оценка на риска веднъж годишно, за да идентифицира основните заплахи и уязвимости. Първата стъпка е идентифицирането на най-критичните информационни активи – системи, данни и процеси, чието компрометиране би имало сериозно въздействие върху дейността на училището. След определяне на критичните активи, се извършва анализ на основните заплахи, специфични за училището, като например фишинг атаки, зловреден софтуер и социално инженерство. Оценката включва и анализ на потенциалното въздействие върху административните услуги в случай на успешна реализация на заплахите, като се фокусира върху най-вероятните сценарии (**Приложение №3** към настоящия документ).

4.2. Третиране на риска

След идентифициране и оценка на рисковете, училището предприема конкретни действия за тяхното третиране. Мерките за защита се избират така, че да съответстват на наличните ресурси и капацитет на училището. Фокусът се поставя върху най-критичните заплахи, които представляват най-голям риск, като се прилага принципът "максимална защита с минимални ресурси". Всички внедрени мерки подлежат на периодично преразглеждане, за да се гарантира тяхната продължаваща ефективност в променящата се среда на заплахи.

5. БАЗОВО УПРАВЛЕНИЕ НА ДОСТЪПА

5.1. Управление на потребителските акаунти

Ефективното управление на потребителските акаунти е основополагащ елемент от цялостната стратегия за киберсигурност. В основата на този процес стои принципът на "минимални привилегии", при който всеки потребител получава само тези права за достъп, които са абсолютно необходими за изпълнение на служебните му задължения. Това значително ограничава потенциалните щети в случай на компрометиране на акаунт. От особена важност е своевременното премахване на потребителските акаунти при напускане на служители, което предотвратява възможността за неоторизиран достъп чрез стари, неактивни акаунти. За предотвратяване на натрупването на излишни права с течение на времето, училището провежда годишен преглед на правата за достъп. При този преглед се проверява дали съществуващите права съответстват на текущите длъжности и отговорности на служителите, като неизползваните или ненужни права се премахват.

5.2. Автентикация

Надеждната автентикация на потребителите е критичен компонент за защита на информационните системи. Училището изисква използването на сложни пароли, които включват минимален брой символи. За повишаване на сигурността, особено за достъп

до критични системи, се прилага двуфакторна автентикация, комбинираща паролите с допълнителен фактор, като например еднократен код, изпратен чрез SMS или генериран от специално приложение. За защита от неоторизиран достъп до незащитени работни компютри, всички системи са конфигурирани да извършват автоматично заключване на потребителските сесии след определен период на неактивност. За отключване отново се изисква пълна автентикация, което осигурява допълнително ниво на защита.

5.3. Контрол на достъпа до мрежата

Контролът на достъпа до мрежата включва няколко ключови мерки, внедрени с помощта на учители по Компютърно моделиране/Компютърно моделиране и информационни технологии от училището или външния ИТ доставчик. Базовото сегментиране на мрежата разделя различните типове системи и данни, ограничавайки възможностите за неоторизиран достъп между сегментите. Допълнителна мярка е ограничаването на достъпа на посетители до отделна гостуваща мрежа, която е изолирана от вътрешната мрежа на училището, предотвратявайки потенциални рискове от външни устройства.

6. ОСНОВНИ МЕРКИ ЗА ЗАЩИТА ОТ ЗЛОВРЕДЕН СОФТУЕР

6.1. Антивирусна защита

Защитата от вредоносен софтуер е една от най-важните мерки за киберсигурност в училището. Основата на тази защита е инсталирането и поддържането на актуален антивирусен софтуер на абсолютно всички устройства, свързани към информационната инфраструктура – компютри, лаптопи и мобилни устройства. За максимална ефективност, антивирусните решения са конфигурирани да извършват автоматично актуализиране на дефинициите веднага след публикуването им от производителя. Това гарантира защита срещу новооткрити заплахи без необходимост от ръчна намеса. Допълнителна мярка е периодичното сканиране на всички системи за наличие на зловреден код, което позволява откриване на потенциални заплахи, които може да са били пропуснати при първоначалната проверка.

6.2. Защита от зловреден код

Освен традиционните антивирусни решения, училището прилага и други мерки за защита от зловреден код. Съществува строга политика, забраняваща инсталирането на неоторизиран софтуер на работните компютри и лаптопи. Това предотвратява въвеждането на потенциално опасни програми в мрежата и намалява повърхността за атака. Специално внимание се отделя на защитата на електронната поща от фишинг атаки, тъй като това е един от най-често използваните вектори за доставяне на зловреден код. Филтрирането на електронната поща блокира съобщения със съмнително съдържание преди те да достигнат до потребителите.

7. УПРАВЛЕНИЕ НА АКТУАЛИЗАЦИИТЕ

Своевременното инсталиране на актуализации за операционните системи и приложенията е критично за отстраняване на известни уязвимости, които могат да бъдат използвани от злонамерени лица. За улесняване на този процес и намаляване на административната тежест, системите са конфигурирани за автоматично изтегляне и

инсталиране на актуализации, където това е технически възможно и безопасно. Този подход гарантира, че защитата се поддържа актуална без необходимост от постоянна ръчна намеса. За системи, при които автоматичното актуализиране не е препоръчително поради специфични изисквания или риск от несъвместимост, учителите по КМИТ/КМ, ОЛМИС или външният ИТ доставчик извършват месечна проверка за налични актуализации и ги прилага контролирано след тестване в непродуктивна среда.

8. БАЗОВА СИГУРНОСТ НА КОМУНИКАЦИИТЕ

8.1. Мрежова сигурност

Защитата на комуникационните канали в мрежовата инфраструктура на училището е от ключово значение за осигуряване на поверителността и интегритета на предаваната информация. Особено внимание се отделя на безжичните мрежи, които поради своя характер са потенциално по-уязвими. За тяхната защита се прилага протокола WPA, който осигурява високо ниво на сигурност. За откриване на потенциални проблеми или аномалии, експерти от училището или външният ИТ доставчик извършват периодичен преглед на журналните файлове от мрежовите устройства, търсейки модели, които могат да индикират опити за неоторизиран достъп.

8.2. Електронна поща

Електронната поща като основен комуникационен канал изисква специално внимание поради високата експозиция към външни заплахи. Училището внедрява система за филтриране на електронната поща, която ефективно защитава от спам и фишинг съобщения, предотвратявайки достигането на потенциално опасни съобщения до крайните потребители. Всички прикачени файлове, получени по електронната поща, автоматично се сканират за зловреден код преди да бъдат доставени до пощенските кутии на служителите. Това позволява откриване и блокиране на скрити заплахи, преди те да причинят щети. Допълнителна мярка е блокирането на известни опасни типове файлове, като например изпълними файлове (.exe, .bat, .cmd), които често се използват за разпространение на зловреден софтуер. Тези файлове се задържат от системата и се освобождават само след допълнителна проверка от ОЛМИС.

9. УПРАВЛЕНИЕ НА ИНЦИДЕНТИ

9.1. Базови процедури за управление на инциденти

Ефективното управление на инциденти със сигурността е критично за минимизиране на негативното въздействие върху операциите на училището. В основата на този процес стои определянето на ясни стъпки за реакция при възникване на различни типове инциденти. Училището разработва и документира опростени, но ефективни процедури, които описват необходимите действия при различни сценарии – от загуба на данни и заразяване със зловреден софтуер до физически нарушения на сигурността. За улесняване на координацията при инциденти, се създава и поддържа актуален списък с контакти на всички отговорни лица и експерти, които трябва да бъдат уведомени в

зависимост от естеството и сериозността на инцидента. За справяне с по-сложни инциденти, които надхвърлят вътрешния капацитет, училището разчита на подкрепата на външния ИТ доставчик, който предоставя специализирана експертиза и ресурси за бързо ограничаване и отстраняване на последствията (**Приложение №2**).

9.2. Докладване на инциденти

Своевременното и точно докладване на инциденти със сигурността е от ключово значение за ефективната реакция. Училището определя ясна верига за докладване, при която всички служители незабавно уведомяват ОЛМИС при забелязване на потенциални проблеми или инциденти. ОЛМИС оценява ситуацията и уведомява външния ИТ доставчик за техническа подкрепа, както и ръководството на училището при по-сериозни инциденти. В изпълнение на законовите изисквания, ОЛМИС отговаря за докладването на значимите инциденти към компетентните органи, спазвайки сроковете и форматите, определени в Закона за киберсигурност.

9.3. Анализ и извличане на поуки

След приключване на инцидент, училището извършва опростен, но систематичен анализ на случилото се, за да идентифицира първопричините и да извлече ценни поуки за бъдещето. Този анализ включва преглед на хронологията на инцидента, предприетите действия и тяхната ефективност. На база на извлечените поуки, се актуализират мерките за защита, за да се предотврати повторното възникване на подобни инциденти. Това може да включва промени в техническите контроли, актуализиране на процедурите или допълнително обучение на служителите.

10. БАЗОВА НЕПРЕКЪСНАТОСТ НА ДЕЙНОСТТА

10.1. План за непрекъснатост

Осигуряването на непрекъснатост на дейността при инциденти със сигурността или други извънредни ситуации е от критично значение за функционирането на училищната администрация. Училището разработва опростен, но ефективен план за непрекъснатост, който започва с идентифициране на критичните административни услуги, чието функциониране трябва да бъде осигурено с приоритет. За всяка критична услуга се определят минимално необходимите ресурси – хардуер, софтуер, данни и персонал, необходими за нейното функциониране. Планът включва конкретни действия при основните типове инциденти, като например компрометиране на данни, отказ на хардуер или софтуер, прекъсване на електрозахранването или интернет връзката, физически заплахи като пожар или наводнение. За всеки сценарий се определят отговорните лица, последователността от действия и каналите за комуникация.

10.2. Създаване на резервни копия

Надеждната система за създаване на резервни копия е фундаментален елемент от стратегията за непрекъснатост на дейността. Училището внедрява система за регулярно създаване на резервни копия на всички критични данни и документи, като графикът и обхватът на архивирането се определят според важността на информацията. От изключителна важност за надеждността на процеса на възстановяване е периодичният мониторинг на създаването на резервните копия.

11. УПРАВЛЕНИЕ НА ВЗАИМООТНОШЕНИЯТА С ВЪНШНИ ИТ ДОСТАВЧИЦИ

11.1. Изисквания към външните ИТ доставчици

Всички договори с доставчици включват конкретни клаузи за сигурност, които детайлно описват изискванията за защита на информацията, процедурите за докладване на инциденти и последствията при нарушаване на тези изисквания. Тези клаузи са правно обвързващи и гарантират, че доставчиците са задължени да спазват същото ниво на защита, което се изисква от училището. От особена важност е изискването за стриктно спазване на националното законодателство в областта на киберсигурността и защитата на личните данни, включително Закона за киберсигурност и Общия регламент за защита на данните (GDPR). Договорите също така определят ясни процедури за докладване на инциденти, които осигуряват своевременно уведомяване на училището при установяване на потенциални проблеми или нарушения на сигурността.

11.2. Мониторинг на доставчиците

Непрекъснатият мониторинг на дейностите на външните ИТ доставчици е от ключово значение за своевременно идентифициране и адресиране на потенциални рискове. Училището следи за състоянието на системите, които включват информация за извършените дейности по поддръжка, приложените актуализации, идентифицираните инциденти и предприетите мерки за тяхното ограничаване. Проследяването на състоянието на системите позволява на ОЛМИС да следи ефективността на защитните мерки и да идентифицира области, нуждаещи се от подобрене.

12. ОБУЧЕНИЯ И ПОВИШАВАНЕ НА ОСВЕДОМЕНОСТТА

12.1. Програма за базово обучение

Човешкият фактор играе ключова роля в цялостната стратегия за киберсигурност, поради което училището осигурява ефективна програма за обучение на служителите. За всички новопостъпили служители се провежда задължително въвеждащо обучение, което обхваща основните принципи на киберсигурността, специфичните политики на училището и личните отговорности за поддържане на сигурността на информационните активи (**Приложение №1 и Приложение №4**).

12.2. Повишаване на осведомеността

Освен формалните обучения, училището провежда дейности за повишаване на осведомеността на служителите относно киберзаплахите и важноста на сигурното поведение. Редовното разпространение на информация за актуални заплахи помага на служителите да бъдат бдителни и да разпознават потенциалните рискове в ежедневната си работа. Тази информация се споделя чрез вътрешни канали за комуникация, като електронна поща или кратки съобщения на информационните табла. Периодичните напомняния за добри практики в областта на киберсигурността поддържат високо ниво на внимание и предотвратяват формирането на рисково поведение поради рутинна или комфорт.

13. ОСНОВНИ МЕРКИ ЗА ФИЗИЧЕСКА СИГУРНОСТ

13.1. Физически контрол на достъпа

Физическата сигурност е неразделна част от цялостната стратегия за киберсигурност, тъй като неоторизираният физически достъп до информационните системи може да компрометира и най-добре защитената мрежа. Училището прилага базови, но ефективни мерки за ограничаване на физическия достъп до компютрите, имащи администраторски достъп да НЕИСПУО и Админплюс. Достъпът до тези компютри е разрешен само на оторизирани лица, чиито служебни задължения изискват пряк достъп до тези компютри. За посетители и външни изпълнители, които имат нужда от временен достъп до защитените зони, се прилагат специални процедури, включващи постоянно придружаване от оторизиран служител и водене на регистър на посетителите, съдържащ информация за целта на посещението и времето на влизане и излизане.

14. БАЗОВО СЪОТВЕТСТВИЕ И ОДИТ

14.1. Законова рамка

Настоящата политика по киберсигурност е разработена съобразно Закона за киберсигурност (ЗКС), Наредбата за минималните изисквания за мрежова и информационна сигурност (НМИМИС) и Актуализираната национална стратегия за киберсигурност "КИБЕРУСТОЙЧИВА БЪЛГАРИЯ 2023.

14.2. Спазване на законовите изисквания

Стриктното спазване на приложимото законодателство в областта на киберсигурността е основен приоритет и отговорност на училището. За постигане на това съответствие, училището провежда годишен преглед на приложимите изисквания и внедрените мерки за защита. Този преглед позволява идентифициране на потенциални пропуски и планиране на необходимите подобрения. ОЛМИС отговаря за документирането на предприетите мерки, като поддържа опростен, но достатъчно подробен регистър на контролите за сигурност. Тази документация служи не само за доказване на съответствие при евентуални проверки от регулаторните органи, но и като основа за непрекъснато подобрение.

14.3. Вътрешни проверки

Вътрешните проверки са важен механизъм за гарантиране на ефективното прилагане на политиките за киберсигурност. Тази самооценка се координира от ОЛМИС и включва преглед на въведените контроли, както и оценка на тяхната ефективност. Резултатите от тези проверки се документират и се използват за идентифициране на области, нуждаещи се от подобрение.

15. ПОДДЪРЖАНЕ НА АКТУАЛНА ПОЛИТИКА

15.1. Годишен преглед

Поддържането на актуална и ефективна политика по киберсигурност изисква систематичен процес на периодичен преглед и актуализация. Училището извършва цялостен преглед на политиката по киберсигурност веднъж годишно, за да гарантира нейната адекватност спрямо променящата се среда на заплахи, технологичното развитие и актуалните нормативни изисквания. Този преглед се координира от ОЛМИС, но включва принос от всички служители, имащи администраторски достъп до платформи за административно управление на училището, както и учители по КМ/КМИТ. Ключов аспект на прегледа е оценката на ефективността на прилаганите мерки за сигурност, която се базира на анализ на възникналите инциденти, резултатите от проверките и обратната връзка от служителите. Особено внимание се отделя на новите и нововъзникващите заплахи, които може да не са били адекватно адресирани в съществуващата политика. За тази цел, ОЛМИС следи информацията за тенденциите в киберзаплахите от публично достъпни източници и участва в информационни сесии, организирани от националните компетентни органи.

15.2. Управление на промените

Управлението на промените в политиката по киберсигурност е структуриран процес, който гарантира, че всички изменения са документирани, валидирани и ефективно комуникирани. Всяка предложена промяна, независимо дали е резултат от периодичния преглед, установен инцидент или промяна в нормативните изисквания, се документира с ясно описание и обосновка. Предложенията за промени се одобряват от директора на училището, който носи крайната отговорност за киберсигурността. След одобрение, промените се внедряват според предварително определен график, който позволява адекватна подготовка и минимизира потенциалното въздействие върху оперативните дейности. От особена важност е ефективното информирание на всички служители за промените в политиката. Това се осъществява чрез различни канали за комуникация, включително електронна поща, вътрешни съобщения или работни срещи, в зависимост от естеството и обхвата на промените.

ПРИЛОЖЕНИЯ

Приложение №1: Основни термини и дефиниции

Приложение №2: Процедура за докладване на инциденти

Приложение №3: Формуляр за оценка на риска

Приложение №4: Програма за въвеждащо обучение за новоназначени служители

Основни термини и дефиниции

Киберсигурност - съвкупност от организационни и технически мерки и дейности за защита на мрежовите и информационните системи от заплахи за тяхната сигурност и от инциденти.

Мрежова и информационна сигурност (МИС) - способност на мрежовите и информационните системи да се противопоставят (с определено ниво на доверие) на действия, които компрометират наличността, автентичността, целостта или поверителността на съхранявани, пренасяни или обработвани данни или на свързаните с тях услуги, предлагани от тези мрежови и информационни системи или достъпни чрез тях.

Риск за мрежовата и информационната сигурност - възможността инцидент да причини вреда, като се отчита вероятността от настъпването му и тежестта на въздействието му.

Инцидент - събитие, което има действително неблагоприятно въздействие върху мрежовите и информационните системи.

Значителен инцидент - инцидент, който предизвиква или може да предизвика значително нарушаване на функционирането на органите на държавното управление или на предоставянето на услуги за обществото.

Зловреден код/софтуер - програма или част от програма, която е създадена с цел да навреди, да наруши нормалното функциониране на системите или да осигури неототоризиран достъп до информация.

Фишинг - техника за придобиване на поверителна информация чрез измама, като извършителят се представя за надеждно лице или организация.

Уязвимост - слабост в информационна система, системни процедури за сигурност, вътрешни контроли или начин на прилагане, която може да бъде използвана за компрометиране на сигурността.

Заплаха - потенциална причина за нежелан инцидент, който може да доведе до вреда за система или организация.

Криптиране - процес на трансформиране на информация по начин, който я прави нечетлива за неототоризирани лица.

Автентикация - процес на проверка на идентичността на потребител или устройство.

Авторизация - процес на предоставяне на права за достъп до ресурси на автентикирани потребители.

Двуфакторна автентикация - метод за идентификация на потребител, който изисква представяне на два отделни компонента за автентикация.

Защитна стена (Firewall) - система за мрежова сигурност, която наблюдава и контролира входящия и изходящия мрежов трафик.

Резервно копие (Backup) - копие на данни, което може да бъде използвано за възстановяване в случай на загуба на оригиналните данни.

CERT/CSIRT - Computer Emergency Response Team/Computer Security Incident Response Team - екип от експерти, отговорни за реагиране при инциденти с компютърната сигурност.

ISO/IEC 27001 - международен стандарт за управление на информационната сигурност.

VPN (Virtual Private Network) - технология, която създава защитена връзка през публична мрежа, като интернет.

Процедура за докладване на инциденти

1. Цел

Настоящата процедура определя стъпките, които трябва да бъдат следвани при установяване, докладване и управление на инциденти, свързани с киберсигурността.

2. Обхват

Процедурата се прилага при всички инциденти, които могат да повлияят на поверителността, цялостността или наличността на информационните активи на училището.

3. Отговорности

- **Всички служители** са отговорни за докладване на подозрителни дейности или инциденти.
- **ОЛИМС** отговаря за оценка, класификация и управление на инцидентите.
- **Директорът на училището** отговаря за вземане на стратегически решения при значителни инциденти.

4. Етапи на процедурата

4.1. Установяване и докладване на инцидент

- Служител, който установи или подозира инцидент със сигурността, незабавно уведомява ОЛИМС чрез определените канали за комуникация.
- Докладването трябва да съдържа:
 - Име и контакти на докладващия
 - Дата и час на установяване на инцидента
 - Описание на инцидента
 - Потенциално засегнати системи или данни
 - Предприети действия (ако има такива)

4.2. Регистриране и класификация на инцидента

- ОЛИМС регистрира инцидента в система за управление на инциденти.
- Инцидентът се класифицира според:
 - Тип на инцидента (напр. зловреден код, неоторизиран достъп, DDoS атака)
 - Ниво на въздействие (ниско, средно, високо, критично)
 - Обхват на засегнатите системи или данни

4.3. Реагиране на инцидента

- За всеки инцидент се определя отговорник, който да координира реакцията.
- Предприемат се незабавни действия за ограничаване на въздействието:

- Изолиране на засегнатите системи
 - Блокиране на компрометирани акаунти
 - Прекъсване на подозрителен мрежов трафик
- Събират се и се съхраняват доказателства за инцидента.

4.4. Възстановяване

- Разработва се и се изпълнява план за възстановяване.
- Проверява се цялостта на данните и системите.
- Системите се връщат в експлоатация след потвърждение, че са защитени.

4.5. Последващи действия

- Провежда се анализ на причините за инцидента.
- Извличат се поуки и се предлагат мерки за предотвратяване на подобни инциденти.
- Актуализират се политиките и процедурите за сигурност при необходимост.
- Провежда се допълнително обучение на служителите, ако е необходимо.

5. Документиране

- За всеки инцидент се поддържа пълна документация, включваща:
 - Формуляр за докладване на инцидента
 - Записи от предприетите действия
 - Комуникация със заинтересованите страни
 - Доклад от анализа на инцидента
 - План за корективни действия

6. Периодичен преглед

- Процедурата за докладване на инциденти се преглежда и актуализира поне веднъж годишно или след значителни инциденти.

Формуляр за оценка на риска за информационната сигурност

Дата на оценката:

Извършил оценката:

Одобрил оценката:

Част 1: Идентификация на актива

Наименование на актива	Описание	Собственик	Местоположение	Класификация

Част 2: Идентификация на заплахите

№	Заплаха	Източник на заплахата	Потенциално въздействие	Вероятност (1-5)
1				
2				
3				

Част 3: Идентификация на уязвимостите

№	Уязвимост	Свързана заплаха	Съществуващи контроли	Ефективност на контролите (1-5)
1				
2				
3				

Част 4: Оценка на риска

№	Заплаха/Уязвимост	Вероятност (1-5)	Въздействие (1-5)	Ниво на риска (В×В)	Приемливост
1					
2					
3					

Скала за вероятност: 1 - Много малка: Събитието е изключително малко вероятно да се случи 2 - Малка: Събитието може да се случи, но рядко 3 - Средна: Събитието вероятно ще се случи в някакъв момент 4 - Висока: Събитието вероятно ще се случи в близко бъдеще 5 - Много висока: Събитието почти сигурно ще се случи в близко бъдеще

Скала за въздействие: 1 - Незначително: Минимално въздействие, без нарушаване на услугите 2 - Ограничено: Ограничено въздействие, краткосрочно нарушаване на услугите 3 - Умерено: Значително въздействие, временно нарушаване на ключови услуги 4 - Сериозно: Сериозно въздействие, продължително нарушаване на ключови услуги 5 - Критично: Критично въздействие, пълно спиране на ключови услуги, загуба на данни

Матрица на риска:

- Нисък риск (1-6): Приемлив риск, не се изискват допълнителни мерки
- Среден риск (7-14): Умерен риск, изискват се мерки в разумен срок
- Висок риск (15-25): Неприемлив риск, изискват се незабавни мерки

Част 5: Третиране на риска

№	Риск	Избран подход	Предложени мерки	Отговорник	Срок	Ресурси	Очаквано ниво на риска след прилагане на мерките
1							
2							
3							

Подходи за третиране на риска:

- Намаляване: Прилагане на контроли за намаляване на риска
- Прехвърляне: Прехвърляне на риска към трета страна (застраховка)
- Избягване: Прекратяване на дейността, която поражда риска
- Приемане: Приемане на риска без допълнителни действия

Част 6: Одобрение

Изготвил:

Име:

Длъжност:

Дата:

Подпис:

Одобрил:

Име:

Длъжност:

Дата:

Подпис:

Приложение №4

Програма за въвеждащо обучение на новоназначени служители

1.1. Цел и обхват

Въвеждащото обучение има за цел да запознае новите служители с основните принципи на киберсигурността, политиките и процедурите, действащи в училището, както и с личните им отговорности за поддържане на сигурността на информационните активи. Обучението е задължително за всички новопостъпили служители и се провежда в рамките на първите две седмици от постъпването им на работа.

1.2. Продължителност и формат

Обучението се провежда в рамките на 2 учебни часа и включва теоретична част. Теоретичната част се представя под формата на презентация, придружена с конкретни примери и дискусии.

1.3. Съдържание на обучението

1.3.1. Основни принципи на киберсигурността

- **Въведение в киберсигурността**
 - Какво представлява киберсигурността и защо е важна
 - Основни понятия и терминология
 - Типове киберзаплахи и атаки (фишинг, социално инженерство, злонамерен софтуер и др.)
 - Статистика за инциденти в публичния сектор в България
- **Основни принципи на защитата на информацията**
 - Поверителност, цялостност и наличност
 - Отчетност и неотричане
 - Управление на риска - основни концепции
 - Многопластов подход към сигурността
- **Законова и регулаторна рамка**
 - Основни изисквания на Закона за киберсигурност
 - Наредба за минималните изисквания за мрежова и информационна сигурност
 - Общ регламент за защита на данните (GDPR) - основни аспекти, свързани с киберсигурността

1.3.2. Политики по киберсигурност в 11.ОУ „Свети Пимен Зографски“

- **Преглед на училищната политика по киберсигурност**
 - Обхват и приложимост
 - Роли и отговорности (ръководство, ОЛМИС, външни доставчици, служители)
 - Процедури за докладване на инциденти

- **Управление на достъпа**
 - Политика за пароли - изисквания за сложност и периодична промяна
 - Правила за управление на потребителски акаунти
 - Двухфакторна автентикация - какво представлява и как се използва
 - Правила за отдалечен достъп до системите

- **Защита от зловреден софтуер**
 - Антивирусна защита - как работи и защо е важна
 - Правила за ползване на преносими носители (USB устройства и др.)
 - Правила за инсталиране на софтуер

- **Сигурност на комуникациите**
 - Безопасно използване на електронна поща
 - Безопасно сърфиране в интернет
 - Политика за използване на социални медии
 - Правила за споделяне на информация по телефон и други канали

1.3.3. Лични отговорности и практически мерки

- **Практически мерки за ежедневна защита**
 - Как да разпознаваме фишинг съобщения
 - Безопасно съхранение и управление на пароли
 - Как да защитим работната станция и мобилните устройства
 - Физическа сигурност на работното място (политика на "чисто бюро", заключване на екрана)

- **Докладване на инциденти**
 - Как да разпознаем потенциален инцидент със сигурността
 - Процедура за докладване - към кого и как
 - Каква информация да предоставим при докладване на инцидент
 - Практически упражнения за докладване на различни типове инциденти

- **Непрекъснатост на работата**
 - Основни принципи за непрекъснатост на работата
 - Индивидуални отговорности при извънредни ситуации
 - Как да работим сигурно извън офиса