бул .” 6-ти септември” № 1 tel. 032/642 732; e-mail:info-1690347@edu.mon.bg, http://www.suvlevski.com/

УТВЪРЖДАВАМ:
РУЖКА ГЕНОВА
Директор на СУ „Васил Левски“
Пловдив

ПОЛИТИКА ЗА МРЕЖОВА И ИНФОРМАЦИОННА СИГУРНОСТ

НА

Спортно училище „Васил Левски“ - Пловдив

Утвърдена със заповед РД-06-2462/16.04.2024 г.

2024 год.

Съдържание:

1. ВЪВЕДЕНИЕ 1.1. Цел и обхват 3
2. ОБЩИ ПРИНЦИПИ 3
3. ЧОВЕШКИ РЕСУРСИ 4
4. УПРАВЛЕНИЕ НА АКТИВИТЕ 4
5. ФИЗИЧЕСКА ЗАЩИТА И ОКОЛНА СИГУРНОСТ 5.1. Физическа защита 5
6. УПРАВЛЕНИЕ НА ЛОГИЧЕСКИЯ ДОСТЪП 5
7. КОМУНИКАЦИОННА И ОПЕРАТИВНА СИГУРНОСТ 5
8. УПРАВЛЕНИЕ НА ИНЦИДЕНТИ 6
9. НЕПРЕКЪСНАТОСТ НА ДЕЙНОСТТА 6
10. УПРАВЛЕНИЕ НА СИГУРНОСТТА НА ИНФОРМАЦИЯТА 6
11. НАРУШЕНИЯ И НАКАЗАНИЯ 7
12. ВЗАИМООТНОШЕНИЯ С ТРЕТИ СТРАНИ 7
13. УПРАВЛЕНИЕ НА РИСКА 8
14. ОРГАНИЗАЦИЯ И УПРАВЛЕНИЕТО НА МИС 8
15. УПРАВЛЕНИЕ НА ИНФОРМАЦИОННИТЕ СИСТЕМИ 9
16. ПРИДОБИВАНЕ УПРАВЛЕНИЕ И УСЪВЪРШЕНСТВАНЕ НА ИНФОРМАЦИОННИ АКТИВИ 9

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. 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 ѝ. 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.
2. Служителят отговорен за МИС – лицето отговорно за МИС в образователната институция.
3. Администратор на ИКС в образователната институция.
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 и ученик има право на достъп до Интернети носи отгорност за посещаваниете от него сайтове. За учениците 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.

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.