ОБЕДИНЕНО УЧИЛИЩЕ „ВАСИЛ ЛЕВСКИ“

с. Михалич, общ. Вълчи дол, обл. Варна

УТВЪРЖДАВАМ:……

Антония Пенчева

Директор на ОбУ „Васил Левски“

с. Михалич

ПОЛИТИКА ЗА СИГУРНОСТ НА КОМУНИКАЦИИТЕ НА ОБЕДИНЕНО УЧИЛИЩЕ „ВАСИЛ ЛЕВСКИ“

Настоящата политика е приета на Педагогически съвет с протокол № 2/04.10.2023 г., утвърдена със Заповед №РД-08-61/05.10.2023 г. на Директора

Версия: 1.0

2023 год.

Съдържание:

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.

6. ОБУЧЕНИЕ И ОСВЕДОМЕНОСТ

6.1. Обучителната институция осигурява подходящо обучение на служителите относно политиките за сигурност на комуникациите, както и за потенциалните рискове и мерки за сигурност.

6.2. Служителите са информирани и осведомени за важността на сигурността на комуникации и за докладване на инциденти и нарушения.

7. ПРЕГЛЕД И ПОДОБРЕНИЕ

Политиката за сигурност на комуникациите се преглежда и актуализира периодично, поне веднъж годишно. Резултатите от прегледите се документират и използват за подобряване на сигурността на комуникациите.