ОБЕДИНЕНО УЧИЛИЩЕ „ВАСИЛ ЛЕВСКИ“

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

УТВЪРЖДАВАМ:.....
Антония Пенчева
Директор на ОбУ „Васил Левски“
с. Михалич

ПОЛИТИКА СРЕЩУ ЗЛОВРЕДЕН СОФТУЕР 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 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.

7. ОБУЧЕНИЕ И ОСВЕДОМЕНОСТ

7.1. Образователната институция е осигурила подходящо обучение на служителите относно зловредния софтуер и техниките за предотвратяване на атаки.

7.2. Служителите са информирани и осведомени за рисковете от зловредния софтуер, защитните мерки и процедури за сигурност.

8. ПРЕГЛЕД И ПОДОБРЕНИЕ

Политиката срещу зловреден софтуер се преглежда и актуализира периодично, поне веднъж годишно. Резултатите от прегледите се документират и използват за подобряване на процесите на управление на действията срещу зловреден софтуер.