ОБЕДИНЕНО УЧИЛИЩЕ „ВАСИЛ ЛЕВСКИ“

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

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

ПОЛИТИКА ЗА КОНТРОЛ НА ДОСТЪПА 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:

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. Идентификационни карти, биометрични системи или други подходящи методи за удостоверяване на самоличността са използвани, за да се гарантира, че само упълномощени лица имат достъп 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. Журнали и логове са съхранявани на сигурно място като е осигурен контролиран достъп до тях.
3. Редовни проверки и анализ на журналите се извършват, за да се откриват възможни нарушения и неразрешени действия.

VII. ОБУЧЕНИЕ И ОСВЕДОМЕНОСТ

1. Образователната институция осигурява подходящо обучение на служителите относно политиките и процедурите за контрол на достъпа и защита на информационните активи.
2. Служителите са информирани и осведомени за рисковете от нарушения на контрола на достъпа и да им се предостави информация за докладване на инциденти и нарушения.

VIII. ПРЕГЛЕД И ПОДОБРЕНИЕ

Политиката за контрол на достъпа се преглежда и актуализира периодично, поне веднъж годишно. Резултатите от прегледите се документират и използват за подобряване на процесите на управление на контрола на достъпа.