НУ „Станислав Доспевски“

гр. Самоков, ул. „ Иван Вазов“ № 80,

e – mail: info-2308899@edu.mon.bg, Тел.: 0722/6 63 92

УТВЪРДИЛ:

ДИРЕКТОР:

КАМЕЛИЯ АСЕНОВА

ПОЛИТИКА ЗА ОТДАЛЕЧЕН ДОСТЪП

НА НУ „СТАНИСЛАВ ДОСПЕВСКИ“,

ГР. САМОКОВ

Съдържание

1. Въведение и обхват..... 3

2. Отговорности..... 3

3. Условия за отдалечен достъп..... 3

4. Защита на отдалечените достъпни системи..... 4

5. Мониторинг и регистрация..... 4

6. Обучение и осведоменост..... 5

7. Преглед и подобрение..... 5

1. ВЪВЕДЕНИЕ И ОБХВАТ

Настоящата политика за отдалечен достъп е разработена в съответствие с 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 хората, които имат достъп до тези активи.

Тази политика важи за всички отдалечени достъпи до информационните активи на образователната институция, включително за служители, външни изпълнители и други заинтересовани страни, които имат разрешение за отдалечен достъп.

2. ОТГОВОРНОСТИ

2.1. Директорът на образователната институция е отговорен за създаването и поддръжката на политики и процедури, свързани с отдалечения достъп.

2.2. Определеният служител по информационна сигурност е отговорен за разработването, изпълнението и поддръжката на политиката за отдалечения достъп, както и за предоставянето на необходимото обучение на служителите относно тази политика.

2.3. Администратора на ИКС е отговорен за предоставянето на сигурни технически решения за отдалечен достъп, включително за конфигуриране, мониторинг и поддръжка на отдалечени достъпни системи.

2.4. Служителите, които използват отдалечен достъп, спазват всички приложими политики и процедури и съдействат за осигуряването на безопасността на информационните активи.

2.5. Неспазването на политиката може да доведе до дисциплинарни мерки и/или правни последици в зависимост от сериозността на нарушението.

3. УСЛОВИЯ ЗА ОТДАЛЕЧЕН ДОСТЪП

3.1. Потребителите преминат през идентификация и удостоверяване преди да им бъде предоставен отдалечен достъп до информационните активи.

3.2. Използването на сигурни протоколи и криптиране на данните се прилагат при отдалечен достъп, за да се гарантира сигурността на комуникациите и защитата на информацията от неоторизиран достъп.

3.3. Ограничаването на правата и привилегиите на потребителите при отдалечен достъп се основава на принципа на най-малките привилегии (principle of least privilege), като потребителите получават само необходимите права за изпълнение на техните служебни задължения.

4. ЗАЩИТА НА ОТДАЛЕЧЕНИТЕ ДОСТЪПНИ СИСТЕМИ

4.1. Администратора на ИКС предоставя сигурни технически мерки за защита на отдалечените достъпни системи, включително:

- защита от зловреден софтуер, уязвимости и неоторизиран достъп;
- най-малко двуфакторна автентикация при работа от разстояние;
- предоставя само канали с висока степен на защита като Virtual Private Network (VPN) ;
- проверява да не се използват File Transfer Protocol (FTP) и Remote Desktop Connection.

4.2. Редовни актуализации на софтуера и пачове свързани със сигурността се прилагат за отдалечените достъпни системи, за да се предотвратят потенциални уязвимости и за да се осигури актуална защита.

5. МОНИТОРИНГ И РЕГИСТРАЦИЯ

5.1. Всички активности при отдалечения достъп са регистрирани и мониторирани, включително успешни и неуспешни опити за достъп, промени в привилегиите и други съществени събития.

5.2. Журнали и логове от отдалечените достъпни системи се съхраняват на сигурно място, като е осигурен и контролиран достъп до тях.

5.3. Редовни проверки и анализ на журналите от отдалечените достъпни системи се извършват, за да се открият възможни нарушения и несанкционирани действия.

6. ОБУЧЕНИЕ И ОСВЕДОМЕНОСТ

6.1. Образователната институция осигурява подходящо обучение на служителите относно политиките и процедурите за отдалечен достъп, както и за потенциалните рискове и мерки за сигурност.

6.2. Служителите са информирани и осведомени за важността на сигурния отдалечен достъп и начина за докладване на инциденти и нарушения.

7. ПРЕГЛЕД И ПОДОБРЕНИЕ

Политиката за отдалечен достъп се преглежда и актуализира периодично, поне веднъж годишно. Резултатите от прегледите се документират и използват за подобряване на процесите на управление на отдалеченият достъп.