



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 ФИЗИЧЕСКА СИГУРНОСТ

НА

.НУ “СТАНИСЛАВ ДОСПЕВСКИ”, ГР. САМОКОВ

Съдържание:

1. Въведение и обхват.....	3
2. Отговорности.....	4
3. Физически достъп и контрол.....	5
4. Видеонаблюдение и мониторинг.....	5
5. Управление на бедствия и аварийни ситуации.....	5
6. Обучение и осведоменост.....	Error! Bookmark not defined.
7. Преглед и подобрене.....	4

III. ФИЗИЧЕСКИ ДОСТЪП И КОНТРОЛ

1. Образователната институция е предприела подходящи мерки за контрол и ограничаване на физическия достъп до информационните активи и физическата инфраструктура.
2. Използването на идентификационни карти или други механизми за удостоверяване на самоличността е въведено и поддържано, за да се сигурно, че само упълномощени лица имат достъп до физическите обекти и активи.
3. Извършват се редовни прегледи на физическата инфраструктура и контролните мерки, за да се гарантира, че те са ефективни и отговарят на изискванията за сигурност.

IV ВИДЕОНАБЛЮДЕНИЕ И МОНИТОРИНГ

1. Където е необходимо, се използва видеонаблюдение за защита на физическата инфраструктура и активите на образователната институция.
2. Видеозаписите са съхранявани на сигурно място и е осигурен контролиран достъп до тях.
3. Мониторингът на системите за видеонаблюдение се извършва редовно, за да се засекат възможни нарушения и нередности.

V. УПРАВЛЕНИЕ НА БЕДСТВИЯ И АВАРИЙНИ СИТУАЦИИ

1. Планове за управление на бедствия и аварийни ситуации са разработени и изпълнени, за да се минимизират потенциалните щети и прекъсвания на работата в случай на физически инциденти.
2. Редовни проверки и прегледи на плановете се извършват, за да се гарантира, че те са актуални и действащи.

VI. ОБУЧЕНИЕ И ОСВЕДОМЕНОСТ

Образователната институция осигурява подходящо обучение на служителите относно политиките и процедурите за физическа сигурност и защита на физическата инфраструктура и активите.

Служителите са информирани и осведомени за рисковете от нарушения на физическата сигурност и да им се предостави информация за докладване на инциденти и нарушения.

I. ВЪВЕДЕНИЕ И ОБХВАТ

Настоящата политика за физическа сигурност е разработена в съответствие с изискванията на международни стандарти свързани с мрежовата и информационна сигурност (МИС) и има за цел да осигури опазването и защитата на физическата инфраструктура и активи на образователната институция.

Тази политика важи за всички физически обекти, инфраструктура и активи, свързани с информационните активи на образователната институция, както и за всички служители, външни изпълнители и други заинтересовани страни, които имат достъп до тези обекти и активи.

II. ОТГОВОРНОСТИ

1. Директорът на образователната институция е отговорен за създаването на политики и процедури, които се отнасят до физическата сигурност.
2. Заместник-директорът по административно стопанската дейност е отговорен за разработването, изпълнението и поддържането на политики, процедури и системи, и Регистър на събития, свързани с физическата сигурност.
3. Определеният служител по информационна сигурност е отговорен за мониторинга и оценката на съответствието с политиките и процедурите за физическа сигурност, както и за предлагане на теми за обучения на служителите, относно тези политика.
4. Служителите спазват всички приложими политики и процедури, свързани с физическата сигурност, и съдействат в осъществяването на защитата на физическата инфраструктура и активите.
5. Неспазването на политиката може да доведе до дисциплинарни мерки и/или правни последици в зависимост от сериозността на нарушението.

4. Образователната институция осигурява подходящо обучение на служителите относно политиките и процедурите за физическа сигурност и защита на физическата инфраструктура и активите.
5. Служителите са информирани и осведомени за рисковете от нарушения на физическата сигурност и да им се предостави информация за докладване на инциденти и нарушения.

VII. ПРЕГЛЕД И ПОДОБРЕНИЕ

Политиката за физическа сигурност се преглежда и актуализира периодично, поне веднъж годишно. Резултатите от прегледите се документират и използват за подобряване на процесите на управление на физическата сигурност.