Спортно училище
„Васил Левски“ гр. Пловдив
ЧРЕЗ СПОРТ КЪМ УСПЕХ

бул .” 6-ти септември” № 1 tel. 032/642 732; e-mail:info-1690347@edu.mon.bg, http://www.suvlevski.com/

УТВЪРЖДАВАМ:
РУЖКА ГЕНОВА
Директор на СУ „Васил Левски“
Пловдив

ПОЛИТИКА ЗА УПРАВЛЕНИЕ НА МОБИЛНИ УСТРОЙСТВА НА Спортно училище „Васил Левски“ - Пловдив

Утвърдена със Заповед РД-06-2495/18.04.2024 г.

Съдържание:

1. Въведение и обхват 3
2. Отговорности 3
3. Определения 3
4. Управление на достъпа 4
5. Конфигурация и актуализации 4
6. Защита на информацията 4
7. Безопасност при използване на обществени мрежи 4
8. Обучение и осведоменост 5
9. Преглед и оценка 5

1. ВЪВЕДЕНИЕ И ОБХВАТ

Настоящата политика за управление на мобилни устройства е разработена в съответствие с изискванията на международни стандарти свързани с мрежовата и информационна сигурност (МИС). Тя има за цел да осигури безопасното и отговорно използване на мобилни устройства в образователната институция и да предотврати рисковете, свързани със загуба, кражба, неоторизиран достъп и злоупотреба с информацията, съхранявана на мобилните устройства.

Тази политика важи за всички мобилни устройства на образователната институция, включително такива на 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 за управление на мобилни устройства.

2.2. Заместник-директрор АСД е отговорен служител за мониторинга и оценката на съответствието с политиката, както и за предоставянето на необходимото обучение на служителите относно тази политика.

2.3. Администратора на ИКТ да осигури при необходимост поддръжка и конфигуриране на мобилните устройства, които се използват в работната среда.

2.4. Служителите спазват настоящата политика и отговарят на задълженията си за сигурно използване на мобилните устройства.

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

3. ОПРЕДЕЛЕНИЯ

3.1. Мобилни устройства - включват, но не се ограничават само до смартфони, таблети, лаптопи и други преносими електронни устройства, които могат да съхраняват, обработват и предават информация.

3.2. BYOD (Bring Your Own Device) - практиката на допускане на служители да

използват личните си мобилни устройства за работни цели.

4. УПРАВЛЕНИЕ НА ДОСТЪПА

4.1. За да се осигури контролиран достъп до информацията, мобилните устройства са защитени с пароли, PIN кодове или други механизми за удостоверяване на потребителя.

4.2. Служителите използват акаунти с ограничени права на мобилните устройства.

4.3. Служителите използват силни пароли и не споделят паролите си с други лица.

4.4. Изгубените или откраднати мобилни устройства се докладват незабавно на директора и на администратора на ИКТ, за да се предприемат мерки за блокиране или изтриване на съхранената информация.

5. КОНФИГУРАЦИЯ И АКТУАЛИЗАЦИИ

5.1. Мобилните устройства са конфигурирани и актуализирани съгласно предварително определени стандарти и политики на образователната институция.

5.2. Служителите актуализират редовно софтуера на своите мобилни устройства, веднага след като са налични нови ъпдейти и пачове свързани със сигурността.

6. ЗАЩИТА НА ИНФОРМАЦИЯТА

6.1. Чувствителната информация, която се съхранява на мобилните устройства, е шифрована, особено в случаите, когато те се използват извън офиса или при BYOD практика.

6.2. Образователната институция извършва редовно резервно копиране и тестване за възстановяване на информацията, съхранявана на мобилните устройства.

7. БЕЗОПАСНОСТ ПРИ ИЗПОЛЗВАНЕ НА ОБЩЕСТВЕНИ МРЕЖИ

Забранява се използването на обществени отворени Wi-Fi мрежи. За осъществяване на комуникация с инфраструктурата на организацията се използват виртуални частни мрежи (VPN) – счетоводен отдел на училището.

8. ОБУЧЕНИЕ И ОСВЕДОМЕНОСТ

Служителите са обучавани редовно относно политиката за управление на мобилни устройства и са осведомени за сигурността и рисковете, свързани с използването на мобилни устройства.

Обучението редовно се актуализира и обхваща актуални заплахи и уязвимост на мобилните устройства.

9. ПРЕГЛЕД И ОЦЕНКА

Политиката за управление на мобилни устройства се преглежда и актуализира периодично, поне веднъж годишно. Резултатите от прегледите и оценките се документират и използват за подобряване на процесите на управление на мобилни устройства.