| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | Въведете тук наименованието на регистрираното юридическо лице | | | | | | | |
| Номер на документа:<br>P34S | | | | | Заглавие на документа:<br>**Политика за мобилни устройства и BYOD** | | | | | | | |
| Версия:<br>1.0 | | Дата на влизане в сила:<br>01.01.2025 | | | Собственик на документа: | | | | | | | |
| X | Политика | | Стандарт | | Процедура | | Формуляр | | Регистър | | Друго | |

| **История на редакциите** | | | | |
|---|---|---|---|---|
| **Номер на редакцията** | **Дата на редакцията** | **Промени** | **Прегледано от** | **Собственик на процеса** |
| | | | | |
| | | | | |

| **Одобрения** | | | |
|---|---|---|---|
| **Име** | **Длъжност** | **Дата** | **Подпис** |
| | | | |
| | | | |

Съгласуване със стандарти и регулации

| Стандарт/регулация | Клауза/член | Коментар |
|---|---|---|
| ISO/IEC 27001:2022 | Клаузи 5.1, 5.2, 6.1, 6.2, 8 | Общи изисквания към СУИС и контролите за мобилни устройства/BYOD |
| ISO/IEC 27002:2022 | Контроли 5.10–5.13 | Подробни контроли за мобилни устройства/BYOD и отдалечен достъп |
| NIST SP 800-53 Rev.5 | AC-19, AC-20, CM-6, MP-7 | Контроли за устройства, носители и конфигурации |
| GDPR на ЕС | Член 5(1)(f) | Защита на личните данни и мобилните крайни точки |
| NIS2 на ЕС | Член 21(2)(d) | Защита на устройства, критични за дейността, включително BYOD |
| DORA на ЕС | Членове 9, 10 | Управление на ИКТ риска/непрекъсваемост за мобилни крайни точки |
| COBIT 2019 | APO13, DSS01, DSS05 | Контроли за ИТ управление, операции и услуги по сигурност |

**1. Цел**

1.1. Настоящата политика определя задължителните изисквания за сигурност при използване на мобилни устройства, включително смартфони, таблети и лаптопи, при достъп до фирмена информация, системи или услуги.

1.2. Политиката урежда и използването на лични устройства (BYOD), за да гарантира защитата на клиентските данни и служебната информация независимо от собствеността върху устройството.

1.3. Политиката въвежда последователни мерки за защита при мобилен достъп, подпомага постигането на целите за сертифициране по ISO/IEC 27001 и предотвратява загуба или компрометиране на данни вследствие на загубени, откраднати или неправомерно използвани мобилни крайни точки.

1.4. Политиката гарантира прилагането на технически и процедурни мерки за защита при използването на мобилни устройства в МСП без собствен ИТ екип, включително в условия на дистанционна работа и при използване на облачни услуги.

**2. Обхват**

**2.1. Настоящата политика се прилага за всички служители, външни изпълнители, стажанти и доставчици на услуги, които:**

2.1.1. използват мобилно устройство за достъп, обработване или съхранение на фирмени данни или системи;

2.1.2. се свързват с фирмени услуги, включително електронна поща, споделени папки, облачни приложения или вътрешни системи чрез корпоративен VPN.

**2.2. Политиката обхваща:**

2.2.1. всички мобилни устройства: смартфони, таблети, лаптопи (предоставени от организацията или лични устройства по BYOD);

2.2.2. всички операционни системи (напр. iOS, Android, Windows, macOS);

2.2.3. всички местоположения (офис, дом, дистанционна работа, обществени места).

2.3. Политиката се прилага във всички работни среди и трябва да се спазва независимо от собствеността върху устройството.

**3. Цели**

3.1. Предотвратяване на загуба на данни: да се гарантира, че използването на мобилни устройства не излага чувствителни фирмени или клиентски данни на неоторизиран достъп, кражба или неправомерна употреба.

3.2. Определяне на ясни правила за BYOD: да се въведат задължителни условия за използване на лични устройства за служебни цели, включително правни и технически мерки за защита.

3.3. Подпомагане на регулаторното съответствие: да се изпълнят изискванията на ISO/IEC 27001, GDPR, NIS2 и други правни задължения чрез задължителни практики за сигурност на мобилните устройства.

3.4. Минимизиране на оперативния риск: да се намали вероятността от оперативно прекъсване, причинено от неправомерно използване, компрометиране или отказ на мобилни устройства.

3.5. Поддържане на доверието на клиентите: да се демонстрира пред клиенти и партньори, че техните данни остават защитени дори когато до тях се осъществява достъп чрез мобилни или лични устройства.

**4. Роли и отговорности**

**4.1. Управител:**

4.1.1. носи отговорност за настоящата политика;

4.1.2. одобрява всяко използване на мобилен достъп и BYOD за достъп до фирмени системи;

4.1.3. гарантира, че споразуменията за BYOD са подписани, съхранявани и проследявани;

4.1.4. проверява, че външните доставчици на ИТ услуги прилагат изискваните мерки за защита на мобилните устройства.

**4.2. Определен служител или доставчик на ИТ поддръжка:**

4.2.1. подпомага настройването, регистрирането и конфигурирането на мобилни устройства, използвани за работа;

4.2.2. прилага контролите за достъп, ограниченията за приложения и правилата за мониторинг, свързани с мобилните устройства;

4.2.3. подпомага реагирането при инциденти, свързани с мобилни устройства (загубени, откраднати или компрометирани устройства).

[ ... Раздели 4.3–8 не са включени в тази предварителна версия. Закупете пълния документ за достъп до пълното съдържание. ... ]

**9. Преглед и актуализация на изискванията**

**9.1. Годишен преглед**

9.1.1. Управителят трябва да преглежда настоящата политика най-малко веднъж на всеки 12 месеца.

9.1.2. Прегледът трябва да потвърждава продължаващото съответствие с изискванията на ISO/IEC 27001, развитието на мобилните технологии и промените в бизнес дейността.

9.1.3. При актуализациите трябва да се отчитат и скорошни инциденти, резултати от одити или регулаторни промени (напр. GDPR, NIS2, DORA).

**9.2. Събития, които налагат междинен преглед**

**9.2.1. Настоящата политика трябва да бъде актуализирана незабавно, ако настъпи някое от следните обстоятелства:**

9.2.1.1. съществен инцидент по сигурността на мобилни устройства (напр. нарушение вследствие на загубено или компрометирано устройство);

9.2.1.2. промяна в поддържаните платформи или инструментите за управление на мобилни устройства;

9.2.1.3. правна или регулаторна промяна, засягаща използването на лични устройства или защитата на данните;

9.2.1.4. внедряване на нови приложения, услуги или инструменти на трети страни, използвани на мобилни устройства.

**9.3. Документиране на промените**

9.3.1. Всички прегледи и актуализации трябва да бъдат документирани, включително датата на преглед, направените промени и одобрението на Управителя.

9.3.2. За целите на одита трябва да се съхранява история на версиите.

**9.4. Комуникация и достъп**

9.4.1. Управителят трябва да гарантира, че всички потребители (служители, външни изпълнители, трети страни) са информирани за промените.

9.4.2. Актуализираните версии трябва да бъдат лесно достъпни, например в споделени папки или вътрешни платформи.

**10. Свързани политики и връзки**

**10.1. Настоящата политика е част от общия набор от политики по информационна сигурност за МСП и трябва да се прилага съвместно със следните документи:**

10.1.1. P4S – Политика за контрол на достъпа: определя изискванията за управление на сигурния достъп до системи, включително системи, до които се осъществява достъп чрез мобилни устройства. Налага добра практика при използването на пароли и контроли върху сесиите.

10.1.2. P8S – Политика за информираност и обучение по информационна сигурност: гарантира, че потребителите са обучени относно сигурното използване на мобилни устройства, докладването на инциденти и условията за BYOD.

10.1.3. P17S – Политика за защита на данните и поверителност: определя обработването на лични данни и фирмени данни на мобилни платформи в съответствие с GDPR, особено когато за работа се използват лични устройства.

10.1.4. P9S – Политика за дистанционна работа: съгласува очакванията за използване на мобилни устройства при работа извън обекта или от дома, включително мерки за защита при работа с устройства и достъп до мрежата.

10.1.5. P30S – Политика за реагиране при инциденти: предоставя рамката за реагиране при инциденти, свързани с мобилни устройства, включително компрометирани или загубени устройства.

10.2. Тези свързани политики формират заедно цялостен набор от контроли за сигурност на мобилните устройства в МСП без собствен ИТ персонал, като осигуряват приложимост, прозрачност и готовност за сертификация.

**11. Референтни стандарти и рамки**

11.1. Настоящата политика подпомага пълното съответствие със следните стандарти за сигурност и изисквания за съответствие:

**11.2. ISO/IEC 27001:**

11.2.1. Клауза 5.1 – Лидерство и ангажираност: осигурява надзор от ръководството и отговорност за мобилния достъп и BYOD;

11.2.2. Клауза 6.1 – Действия за адресиране на рисковете: изисква рисковете за сигурността на мобилните устройства да бъдат оценявани и третирани;

11.2.3. Клауза 8.1 – Оперативно планиране и контрол: изисква последователни процедури за мобилен достъп за защита на служебната информация.

**11.3. ISO/IEC 27002:**

11.3.1. Контроли 5.10 (Използване на мобилни устройства), 5.11 (Дистанционна работа), 5.12 (Отдалечен достъп) и 5.13 (BYOD): предоставят насоки за прилагане на управление на рисковете, свързани с устройствата, в контекста на малкия бизнес.

**11.4. NIST SP 800-53 Rev.5:**

11.4.1. AC-19 – Контрол на достъпа за мобилни устройства: изисква настройки за сигурност при разрешено използване на мобилни устройства;

11.4.2. AC-20 – Използване на външни системи: урежда рисковете, свързани с BYOD и отдалечения достъп;

11.4.3. CM-6 – Настройки на конфигурацията: налага сигурни настройки по подразбиране и персонализирани настройки на мобилни платформи;

11.4.4. MP-7 – Използване на носители: разглежда правилното използване и ограниченията при мобилно съхранение и достъп до данни.

**11.5. GDPR на ЕС (2016/679):**

11.5.1. Член 5(1)(f) – Цялостност и поверителност: изисква защита на данните чрез подходяща сигурност на личните данни, особено на мобилни платформи;

11.5.2. Член 32 – Сигурност на обработването: изисква използване на подходящи технически и организационни мерки за защита на данни, до които се осъществява достъп или които се съхраняват на мобилни устройства.

**11.6. Директива NIS2 на ЕС (2022/2555):**

11.6.1. Член 21(2)(d) – Мерки за сигурност на устройствата: изисква контроли за сигурност за хардуера и софтуера, използвани за достъп до критични бизнес системи, включително лични устройства.

**11.7. DORA на ЕС (2022/2554):**

11.7.1. Член 9 – Рамка за управление на ИКТ риска: изисква защита на мобилните крайни точки, използвани за критични бизнес комуникации и облачни услуги;

11.7.2. Член 10 – Непрекъсваемост на ИКТ дейността: налага поддържане на сигурен достъп до бизнес системи дори при прекъсвания или дистанционна работа.

**11.8. COBIT 2019:**

11.8.1. APO13 – Управление на сигурността: изисква организацията да прилага политики за мобилни устройства и BYOD, съгласувани с корпоративния риск;

11.8.2. DSS01 – Управление на операциите: осигурява техническото прилагане на механизми за сигурен достъп;

11.8.3. DSS05 – Управление на услугите по сигурност: урежда участието на трети страни в поддържането на сигурни мобилни среди и координацията при реагиране на инциденти.