					Въведете тук наименованието на регистрираното юридическо лице							
Номер на документа: P34					Заглавие на документа: **Политика за мобилни устройства и BYOD**							
Версия: 1.0		Дата на влизане в сила: 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**

Съгласуваност със стандарти и регулаторни изисквания

Стандарт/регулация	Клауза/член	Коментар
ISO/IEC 27001:2022	5.2, 6.1, 7.5, 8	Прилагат се контроли за сигурност и изисквания за съответствие
ISO/IEC 27002:2022	5.10, 8.1, 8.5, 8	Предоставя подробни контроли за управление на мобилни устройства
NIST SP 800-53 Rev.5	AC-19, AC-17, CM-7, MP-5, SC-12	Контрол на достъпа, отдалечен достъп, конфигурация и изисквания за сигурност за мобилни устройства
GDPR на ЕС	5(1)(f), 25, 32	Задължителни изисквания за поверителност, криптиране на данни и сигурност на обработването
NIS2 на ЕС	21(2)(d)	Технически и организационни мерки за защита при мобилен достъп
DORA на ЕС	9, 10	Изисквания за управление на ИКТ риска и сигурност на мобилни устройства
COBIT 2019	APO13.02, DSS01.04, BAI09	Планове за информационна сигурност, конфигурация на активи и контроли за мобилни среди

1. Цел

1.1 Настоящата политика определя изискванията за сигурност, съответствие и експлоатация при използването на мобилни устройства и лични технологии (BYOD – използване на лични устройства) за достъп до организационни системи, приложения или данни.

1.2 Политиката има за цел да гарантира поверителността, целостта и наличността на фирмената информация, до която се осъществява достъп или която се обработва чрез мобилни крайни устройства, включително смартфони, таблети, лаптопи и хибридни устройства.

1.3 Политиката установява също техническите и процедурните контроли, необходими за ограничаване на рискове като изтичане на данни, неоторизиран достъп, загуба или кражба на устройство и компрометиране на мобилни приложения.

1.4 Настоящата политика подпомага съответствието с регулаторните и договорните изисквания, като същевременно осигурява сигурна мобилна работа за служители, външни изпълнители и упълномощени трети страни.

2. Обхват

2.1 Настоящата политика се прилага за целия персонал, включително служители, външни изпълнители, стажанти и външни доставчици на услуги, които използват мобилни устройства за достъп до фирмени данни, системи, приложения или комуникационни платформи.

2.2 Политиката обхваща всички мобилни изчислителни устройства, включително, но не само:

2.2.1 смартфони и таблети (iOS, Android и др.)

2.2.2 лаптопи и ултрабуци (Windows, macOS, Linux)

2.2.3 носими и хибридни интелигентни устройства, способни на синхронизация на данни

2.3 Политиката се прилага независимо дали устройството е собственост на организацията или е лично устройство, използвано по силата на BYOD споразумение.

2.4 Политиката обхваща всички канали за достъп, включително VPN, виртуални работни плотове, облачни приложения, електронна поща, платформи за сътрудничество (напр. SharePoint, Teams) и инструменти за синхронизация на файлове (напр. OneDrive, Dropbox, ако са разрешени).

2.5 Политиката се прилага при дистанционна работа, в локална среда, по време на пътуване или при хибридни модели на работа.

3. Цели

3.1 Да се намали рискът от компрометиране, изтичане или загуба на данни вследствие на незащитено използване на мобилни устройства.

3.2 Да се прилагат последователни и изпълними контроли за сигурност за всички мобилни крайни устройства, независимо от модела на собственост (корпоративно устройство или BYOD).

3.3 Да се гарантира, че използването на мобилни устройства е в съответствие с ISO/IEC 27001 и други регулаторни рамки, приложими към поверителността, защитата на данните и киберсигурността.

3.4 Да се улесни сигурната интеграция на мобилните устройства в оперативните, комуникационните и съвместните работни процеси на организацията.

3.5 Да се осигурят ясно определени отговорности и процеси за управление на мобилни устройства (MDM), включително въвеждане, отдалечено изтриване, криптиране, удостоверяване и мониторинг.

3.6 Да се защитят правата на поверителност на лицата, използващи собствени устройства, като същевременно се защитава чувствителната информация на организацията.

4. Роли и отговорности

4.1 Директор по информационна сигурност (CISO) / Ръководител по ИТ сигурност

4.1.1 Определя политиката и техническите стандарти за използване на мобилни устройства и BYOD.

4.1.2 Осъществява надзор върху съответствието, реагирането при инциденти и управлението на изключенията от контролите за мобилни устройства.

4.1.3 Координира действията с отделите „Правни въпроси и съответствие“ и „Човешки ресурси“ (ЧР), за да гарантира, че прилагането е правно издържано и съгласувано с организационните изисквания.

4.2 ИТ администратор / MDM администратор

4.2.1 Управлява предоставянето, въвеждането и конфигурирането на мобилни устройства чрез MDM решения.

4.2.2 Прилага контроли на ниво устройство (напр. криптиране, ПИН кодове, контроли върху приложенията).

4.2.3 Изпълнява отдалечено изтриване, блокиране на устройството и отнемане на достъп при необходимост.

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

9. Преглед и актуализиране

9.1 Настоящата политика подлежи на преглед най-малко веднъж годишно от директора по информационна сигурност (CISO) или определения мениджър по информационна сигурност, за да се гарантира съгласуваност с:

9.1.1 промени в платформите за мобилни операционни системи, MDM технологиите или стандартите за удостоверяване;

9.1.2 регулаторни или договорни промени, засягащи защитата на мобилни данни (напр. GDPR, DORA, NIS2);

9.1.3 изменения в наборите от контроли на ISO/IEC 27001:2022, ISO/IEC 27002:2022 или NIST SP 800-53 Rev.5;

9.1.4 обратна връзка от одити, прегледи след инциденти или сигнали от служители.

9.2 Извънредни прегледи могат да бъдат задействани от:

9.2.1 инциденти по сигурността, свързани с мобилни устройства или BYOD платформи;

9.2.2 уведомление от доставчик за високорискови уязвимости в поддържаните платформи;

9.2.3 внедряване на нови мобилни приложения или платформи за сътрудничество, използвани за бизнес операции.

9.3 Актуализациите на политиката трябва да бъдат:

9.3.1 документирани в историята на версиите на политиката;

9.3.2 комуникирани до целия персонал и засегнатите външни изпълнители;

9.3.3 потвърдени повторно чрез актуализирано потвърждение за запознаване за всички BYOD потребители.

9.4 Всички прегледи и изменения трябва да бъдат формално одобрени от изпълнителното ръководство и регистрирани в регистъра на промените по политиките.

10. Свързани политики и връзки

10.1 Настоящата политика е взаимосвързана с няколко ключови политики в рамката на СУИС на организацията. Основните връзки включват:

10.1.1 P1 – Политика по информационна сигурност: Определя общите принципи на управление за всички контроли по информационна сигурност, включително тези, уреждащи използването на мобилни устройства.

10.1.2 P3 – Политика за допустима употреба: Определя допустимото поведение и ограниченията, свързани с използването на технологии, които се прилагат пряко към мобилния и BYOD достъп.

10.1.3 P9 – Политика за дистанционна работа: Определя допълнителни задължения по сигурността за мобилни работни среди и допълва специфичните за мобилните устройства контроли, определени в настоящата политика.

10.1.4 P13 – Политика за класификация и етикетиране на данни: Регламентира как трябва да се обработват данните на мобилни устройства според нивото на класификация, което влияе върху съхранението, прехвърлянето и прилагането на криптиране.

10.1.5 P22 – Политика за регистриране и мониторинг: Подпомага събирането и прегледа на журнали за мобилен достъп с цел откриване на аномалии или нарушения.

10.1.6 P30 – Политика за реагиране при инциденти: Регламентира как се обработват и ескалират инциденти, свързани с мобилни устройства (напр. загуба на устройство, неоторизиран достъп).

10.1.7 P33 – Политика за мониторинг на одита и съответствието: Осигурява основата за периодични проверки на съответствието на мобилната сигурност, включително спазването на BYOD политиката.

11. Референтни стандарти и рамки

11.1 Настоящата политика е съгласувана с международно признати рамки за киберсигурност и правни задължения, за да гарантира сигурното използване на мобилни устройства и лични технологии (BYOD) в корпоративна среда.

11.2 ISO/IEC 27001:

11.2.1 Клауза 5.10 – Допустимо използване на информация и активи: Изисква контроли за отговорно използване на корпоративни активи, включително мобилни устройства.

11.2.2 Клауза 5.11 – Дистанционна работа: Регламентира сигурни практики при достъп до системи извън помещенията на организацията.

11.2.3 Клауза 5.12 – Използване на мобилни устройства: Налага контроли, базирани на риска, за мобилни крайни устройства и BYOD конфигурации.

11.2.4 Клауза 5.13 – Прехвърляне на информация: Налага защита на информацията, прехвърляна чрез мобилни канали.

11.3 ISO/IEC 27002:2022 – Контроли 5.10 до 5.13:

11.3.1 Контроли от Приложение A 5.10 до 5.13: Определят как мобилният достъп, криптирането, мониторингът и ограничаването на загуби трябва да се прилагат в рамките на Система за управление на информационната сигурност (СУИС). Тези контроли предоставят подробни указания за внедряване за защита на мобилни крайни устройства, налагане на контейнеризация, мониторинг на целостта на устройствата и осигуряване на конфигурации, съобразени с поверителността, при използване на BYOD.

11.4 NIST SP 800-53 Rev.5:

11.4.1 AC-19 – Контрол на достъпа за мобилни устройства: Определя базови защити, включително криптиране, удостоверяване и прилагане на MDM.

11.4.2 AC-17 – Отдалечен достъп: Изисква сигурно удостоверяване и защита на сесиите за отдалечени мобилни потребители.

11.4.3 CM-7 – Минимална функционалност: Подпомага премахването на ненужни приложения и функции от мобилните крайни устройства за намаляване на риска.

11.4.4 MP-5 – Защита при пренос на носители: Регламентира сигурното предаване на данни от мобилни системи към външни или облачни местоназначения.

11.4.5 SC-12 – Установяване на криптографски ключове: Налага използването на сигурни криптографски протоколи за мобилна комуникация и съхранение.

11.5 GDPR на ЕС (2016/679):

11.5.1 Член 5(1)(f) – Цялостност и поверителност: Изисква организациите да защитават личните данни на мобилни устройства срещу неоторизиран или незаконосъобразен достъп.

11.5.2 Член 25 – Защита на данните още при проектиране и по подразбиране: Изисква поверителността да бъде вградена в BYOD и MDM процесите.

11.5.3 Член 32 – Сигурност на обработването: Налага контроли, базирани на риска (напр. криптиране, удостоверяване, контрол на достъпа), за личните данни в мобилни платформи.

11.6 Директива NIS2 на ЕС (2022/2555):

11.6.1 Член 21(2)(d): Изисква мобилният достъп до критични системи и информация да бъде защитен чрез подходящи технически и организационни мерки, като контрол на крайните точки, криптиране и мониторинг.

11.7 DORA на ЕС (2022/2554):

11.7.1 Член 9 – Рамка за управление на ИКТ риска: Изисква субектите от финансовия сектор да ограничават рисковете при мобилен и отдалечен достъп като част от оперативната устойчивост.

11.7.2 Член 10 – Изисквания за сигурност на ИКТ системите: Изисква сигурна мобилна архитектура, мониторинг и механизми за реагиране при киберзаплахи, произтичащи от мобилни устройства.

11.8 COBIT 2019:

11.8.1 APO13.02 – Създаване и поддържане на план за информационна сигурност: Изисква използването на мобилни устройства, включително BYOD, да бъде интегрирано в организационните стратегии за сигурност.

11.8.2 DSS01.04 – Управление на конфигурацията и целостта на активите: Прилага се за контрол на конфигурацията и сигурно внедряване на мобилни устройства.

11.8.3 BAI09.01 – Създаване и поддържане на контроли: Подпомага внедряването на технически и процедурни предпазни мерки за сигурни мобилни и отдалечени операции.