					Въведете тук наименованието на регистрираното юридическо лице							
Номер на документа: P12S					Заглавие на документа: **Политика за управление на активите**							
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**

Съгласувано с приложими стандарти и регулации

Стандарт/регулация	Клауза/член	Коментар
ISO/IEC 27001:2022	Clause 8	Изисквания за управление на активите
ISO/IEC 27002:2022	Control 5	Контроли за управление на активите
NIST SP 800-53 Rev.5	CM-8	Инвентар на системните компоненти
EU NIS2	Article 21(2)(a)	Проследяване на активите за защита на мрежовите и информационните системи
EU DORA	Article 5(8)	Изисквания за инвентаризация на ИКТ активите
COBIT 2019	BAI	Управление на жизнения цикъл на ИТ активите
EU GDPR	Article 30	Инвентар на дейностите по обработване на данни

1. Цел

1.1 Настоящата политика определя как организацията идентифицира, проследява, защитава и извежда от употреба своите информационни активи, включително физически и цифрови компоненти.

1.2 Целта е да се намалят оперативните рискове и рисковете за сигурността чрез осигуряване на видимост, отчетност и сигурно боравене с всички бизнес активи през целия им жизнен цикъл.

1.3 Надеждният инвентар на активите подпомага регулаторното съответствие, реагирането при инциденти, планирането на непрекъсваемостта на дейността и управлението на риска.

1.4 Настоящата политика подпомага и сертифицирането по ISO/IEC 27001 и демонстрира съответствие с правните, финансовите и киберсигурностните задължения по рамки като GDPR, NIS2 и DORA.

1.5 За малките и средните предприятия (SMEs) опростеният, но систематичен подход към управлението на активите е съществен за избягване на неуправлявани устройства, изтичане на данни или несъответствия при одит, особено при ограничен технически персонал.

2. Обхват

2.1 Настоящата политика се прилага за всички активи, притежавани, наети или по друг начин управлявани от организацията, включително активи, използвани при:

2.1.1 работа в офис

2.1.2 дистанционна или хибридна работа

2.1.3 работа на терен или мобилни операции

2.1.4 облачни среди и външно възложени услуги

2.2 Обхванатите видове активи включват, но не се ограничават до:

2.2.1 Хардуер: лаптопи, настолни компютри, монитори, телефони, таблети, USB носители, рутери, принтери, носители за резервни копия

2.2.2 Софтуер: инсталирани приложения, SaaS решения, операционни системи, антивирусен софтуер, лицензи

2.2.3 Информационни активи: хранилища на бизнес данни, електронни таблици, клиентски записи, изходен код

2.2.4 Цифрови идентификационни данни и услуги: имена на домейни, цифрови сертификати, API ключове, акаунти за електронна поща, облачни акаунти

2.2.5 Средства за достъп: ключове, смарт карти, пропуски за достъп, биометрични токени

2.3 Всички служители, външни изпълнители и доставчици от трети страни, които боравят с организационни активи, попадат в обхвата на тази политика.

2.4 Политиката урежда както краткосрочни активи (напр. лаптопи за конкретен проект), така и дългосрочни активи, както и споделени активи, използвани от повече от едно лице.

3. Цели

3.1 Да се създаде и поддържа пълен и точен инвентар на активите за всички релевантни активи, който да се актуализира текущо.

3.2 Да се гарантира, че за всеки актив е определен собственик, който носи отговорност за използването, съхранението и връщането му.

3.3 Да се класифицират активите въз основа на чувствителност, въздействие върху бизнеса или регулаторна значимост, така че да се прилагат съответни нива на защита.

3.4 Да се определят ясни процедури за предоставяне на оборудване, преназначаване, поддръжка, докладване на загуба и извеждане от употреба на активи.

3.5 Да се гарантира сигурно боравене с активите през целия им жизнен цикъл, а информацията, която съхраняват, да бъде защитена или сигурно изтрита при унищожаване.

3.6 Да се намали вероятността от инциденти по сигурността, причинени от непроследени, невърнати или неправомерно използвани организационни ресурси.

3.7 Да се подпомогне съответствието с приложимите закони (напр. принципа на отчетност по GDPR) и стандартите за сертификация в областта на киберсигурността.

4. Роли и отговорности

4.1 Управител

4.1.1 Отговаря за настоящата политика и осигурява внедряването и спазването на практиките за управление на активите в цялата организация.

4.1.2 Преглежда и одобрява актуализациите на инвентара на активите и разрешава извеждането от употреба или прехвърлянето на активи, когато е необходимо.

4.1.3 Трябва да бъде уведомяван за всяка значителна загуба, кражба или неправомерна употреба на активи.

4.2 ИТ ръководител или определен отговорник по активите

4.2.1 Поддържа инвентара на активите (напр. в електронна таблица, система за заявки или лек инструмент за проследяване на активи).

4.2.2 Определя собственик на актив и проследява промените в статуса (напр. нов, в употреба, в ремонт, изведен от употреба).

4.2.3 Проверява, че всички предоставени активи са документирани и свързани с конкретно лице или бизнес звено.

4.2.4 Осигурява прилагането и спазването на етикетите за класификация (напр. „Вътрешна употреба“, „Поверително“).

4.2.5 Координира връщането, сигурното изтриване и деактивирането на активи при освобождаване на служител или извеждане от употреба.

4.2.6 Докладва на Управителя всички неразрешени несъответствия, свързани с активи.

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

9. Изисквания за преглед и актуализация

9.1 Настоящата политика трябва да се преглежда най-малко веднъж годишно и винаги когато:

9.1.1 се въвеждат нови видове технологии или активи

9.1.2 се променят процедурите за проследяване на активи (напр. при внедряване на нови инструменти или платформи)

9.1.3 нови регулаторни задължения засягат проследимостта или унищожаването на активи

9.1.4 инцидент или одит установи пропуск в текущите практики за управление на активите

9.2 Прегледите трябва да включват Управителя и ИТ ръководителя и да обхващат актуализации на процедурите за боравене с активи, шаблоните за инвентар и указанията за класификация.

9.3 Всички актуализации трябва да бъдат документирани и съобщени на засегнатия персонал. Трябва да се поддържа журнал на промените под управление на версиите.

10. Свързани политики и връзки

10.1 P2S – Политика за роли и отговорности в управлението: определя отчетността за собствеността върху политиките и ИТ операциите.

10.2 P4S – Политика за контрол на достъпа: свързва използването на активи (напр. лаптопи, мобилни устройства) с правата за достъп и управлението на идентичности.

10.3 P7S – Политика за въвеждане в работата и прекратяване на правоотношенията: гарантира, че предоставянето и връщането на активи са включени в процесите по жизнения цикъл на персонала.

10.4 P13S – Политика за класификация и етикетиране на данни: предоставя правила за определяне дали даден актив следва да бъде класифициран като „Вътрешна употреба“ или „Поверително“.

10.5 P30S – Политика за реагиране при инциденти: определя процедурите за реакция, ако събитие, свързано с актив, доведе до нарушение на сигурността или поверителността.

11. Референтни стандарти и рамки

11.1 ISO/IEC 27001

11.1.1 Clause 8.1: Изисква оперативни контроли за управление на активите и защитата им по време на използване.

11.2 ISO/IEC 27002

11.2.1 Control 5.9: Описва как активите да бъдат идентифицирани, с определен собственик, класифицирани и управлявани по сигурен начин.

11.3 NIST SP 800-53 Rev.5

11.3.1 CM-8: Изисква организациите да разработят и поддържат инвентар на системните компоненти, включително хардуер, софтуер и виртуални активи.

11.4 EU GDPR

11.4.1 Article 30: Изисква документиране на дейностите по обработване на данни, което зависи от това да е известно къде се съхраняват данните и върху кои активи.

11.5 EU NIS2

11.5.1 Article 21(2)(a): Изисква технически и организационни мерки, включително проследяване на активите, за защита на мрежовите и информационните системи.

11.6 EU DORA

11.6.1 Article 5(8): Финансовите субекти трябва да поддържат подробни инвентари на ИКТ активите като част от управлението на ИКТ риска.

11.7 COBIT 2019

11.7.1 BAI09: Определя, че ИТ активите трябва да бъдат управлявани през целия им жизнен цикъл – от придобиването до извеждането от употреба – при ясно определена собственост и контроли.