					Въведете тук наименованието на регистрираното юридическо лице							
Номер на документа: P12					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**

1. Цел

1.1 Настоящата политика определя задължителните организационни изисквания за идентифициране, класифициране, управление и защита на информационните активи през целия им жизнен цикъл. Тя подпомага управлението в цялата организация на хардуерни, софтуерни, информационни, облачни и нематериални активи, включително в мобилни, отдалечени и управлявани от трети страни среди.

1.2 Целта на тази политика е да осигури пълна видимост върху средата от информационни активи на организацията, като създава условия за ефективни контроли за сигурност, ясно определяне на собствеността, съответствие с приложимите изисквания и сигурно извеждане от употреба или унищожаване.

1.3 Политиката е съгласувана с ISO/IEC 27001:2022, Приложение A, контрол 5.9, като изисква поддържането на централизиран инвентар на информацията и свързаните с нея активи. Тя осигурява отчетност чрез определяне на собственик за всеки актив и прилагане на защита, съобразена с класификацията, чувствителността за бизнеса и регулаторните изисквания.

2. Обхват

2.1 Настоящата политика се прилага за всички служители, външни изпълнители, доставчици от трети страни и доставчици на услуги, които управляват, използват, достъпват, съхраняват или обработват информационни активи, притежавани или контролирани от организацията.

2.2 Обхватът включва всички категории активи, включително:

2.2.1 Физически активи: преносими компютри, настолни компютри, мобилни устройства, преносими носители, принтери, мрежово оборудване

2.2.2 Цифрови активи: софтуер, приложения, системни образи, бази данни, резервни копия на данни, криптографски ключове

2.2.3 Информационни активи: структурирани и неструктурирани данни, отчети, електронна поща, интелектуална собственост

2.2.4 Облачни и виртуални активи: IaaS, SaaS и PaaS среди, виртуални машини, контейнери

2.2.5 Логически активи: имена на домейни, лицензи, потребителски акаунти, базови конфигурации

2.3 Политиката урежда и активите, използвани в условия на дистанционна работа, хибридна работа или във външно възложени среди, като осигурява защита и видимост, дори когато активите не се намират физически в обектите на организацията.

3. Цели

3.1 Да се поддържа пълен, точен и актуален инвентар на активите за всички информационни активи на организацията с определени атрибути за собственост, класификация и местоположение.

3.2 Да се определят собственици на активи, които отговарят за класифицирането, обработването и защитата на активите под техен контрол в съответствие с политиките за управление на данните и сигурността.

3.3 Да се прилагат подходяща класификация и етикетиране на всички активи въз основа на чувствителност, критичност и регулаторни изисквания.

3.4 Да се защитават активите според тяхната класификация и свързаната с нея рискова експозиция, включително при съхранение, достъп, предаване и унищожаване.

3.5 Да се прилагат процедури за връщане на активи и сигурно извеждане от употреба при освобождаване, прекратяване на договор или приключване на жизнения цикъл на актива.

3.6 Да се подпомага регулаторното съответствие с рамки като ISO/IEC 27001, GDPR, NIS2, DORA и COBIT 2019 чрез структурирано управление на активите и осигуряване на възможност за одит.

4. Роли и отговорности

4.1 Изпълнително ръководство

4.1.1 Одобрява Политиката за управление на активите и осигурява необходимите ресурси за пълното ѝ прилагане.

4.1.2 Носи крайната отговорност за защитата и управлението на организационните активи в съответствие с регулаторните и договорните задължения.

4.2 Директор по информационна сигурност (CISO)

4.2.1 Отговаря за Политиката за управление на активите и осигурява интегрирането ѝ в по-широката Система за управление на информационната сигурност (СУИС) на организацията.

4.2.2 Преглежда изключенията и отклоненията от настоящата политика и изисква стратегии за смекчаване, базирани на риска.

4.2.3 Осъществява надзор върху периодичните одити на класификацията на активите, целостта на инвентара и съответствието по жизнения цикъл на активите.

[... 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 или при настъпване на:

9.1.1 Промени в правните или регулаторните задължения, засягащи класификацията на активите или изискванията за инвентаризация

9.1.2 Въвеждане на нови категории активи или платформи за управление (напр. cloud-native CMDB)

9.1.3 Одитни констатации от вътрешен одит или инциденти по сигурността, свързани с неправилно управление на активите

9.1.4 Организационно преструктуриране, което засяга собствеността или контролите по жизнения цикъл

9.2 Процесът по преглед трябва да бъде иницииран от Мениджъра на ИТ активи и координиран с Директора по информационна сигурност (CISO), Закупуване, Правни въпроси и засегнатите ръководители на отдели.

9.3 Междинни прегледи могат също да бъдат задействани от:

9.3.1 Придобиване или отделяне на бизнес звена

9.3.2 Промени в доставчиците, засягащи активи, управлявани от трети страни

9.3.3 Технологични обновявания, включващи масово извеждане от употреба или предоставяне

9.4 Всички ревизии на тази политика трябва:

9.4.1 Да бъдат под версионен контрол и съхранявани в хранилището на СУИС

9.4.2 Да бъдат одобрени от Изпълнителното ръководство

9.4.3 Да включват обобщение на промените и основанието за тях

9.4.4 Да бъдат съобщени на всички засегнати заинтересовани страни, включително чрез актуализирани процедури или системни обучения, когато е приложимо

10. Свързани политики и връзки

10.1 Настоящата политика се прилага съвместно със следните свързани политики и подпомага тяхното прилагане:

10.1.1 P4 - Политика за контрол на достъпа: Осигурява съгласуваност между видимостта на активите, предоставените права за достъп и контролните механизми в системите и средите за данни.

10.1.2 P7 - Политика за въвеждане в работата и прекратяване на правоотношенията: Регламентира своевременното предоставяне и връщане на физически и логически активи при промени в персонала.

10.1.3 P13 - Политика за класификация и етикетиране на данните: Определя задължителните правила за класификация на активите, които определят процедурите по етикетиране, обработване и унищожаване.

10.1.4 P14 - Политика за съхранение и унищожаване на данни: Определя сроковете и методите за сигурно унищожаване на цифрови и физически активи, съдържащи информация.

10.1.5 P22 - Политика за регистриране и мониторинг: Осигурява проследимост на достъпа до активи и тяхното използване чрез системно журнализиране, видимост на крайните точки и поведенчески анализ.

10.1.6 P30 - Политика за реагиране при инциденти: Подпомага бързото ограничаване и разследване на нарушения, свързани с активи, като загубени преносими компютри или непроследени носители за съхранение.

10.2 Тези политики формират съгласувана рамка за управление, която осигурява активите да бъдат сигурно управлявани, точно инвентаризирани и обработвани по подходящ начин през целия им жизнен цикъл.

11. Референтни стандарти и рамки

11.1 Настоящата политика е съгласувана с международно признати стандарти за информационна сигурност и регулаторни рамки, които изискват устойчиво управление на активите през целия им жизнен цикъл.

11.2 ISO/IEC 27001:

11.2.1 Клауза 8.1 - Изисква организациите да планират, прилагат и контролират процесите, необходими за изпълнение на изискванията за информационна сигурност, включително тези за управление на жизнения цикъл на активите.

11.3 ISO/IEC 27002:2022 - Контроли 5.9 до 5.11

11.3.1 Контрол 5.9 - Инвентар на информацията и други свързани активи: Изисква актуален и пълен инвентар на всички активи, свързани с обработването на информация.

11.3.2 Контрол 5.10 - Допустимо използване на корпоративни активи: Подкрепя се чрез правила за използване, собственост и процеси по връщане.

11.3.3 Контрол 5.11 - Връщане на активи: Прилага се чрез формални процедури за предаване и извеждане от употреба.

11.3.4 Тези контроли установяват структурирани изисквания за идентифициране, етикетиране, поддържане и проследяване на организационните активи, със съответни отговорности за собствениците и лицата, които ги съхраняват или управляват през целия жизнен цикъл.

11.4 NIST SP 800-53 Rev.5:

11.4.1 CM-8 - Инвентар на системните компоненти: Отразява се чрез централизирано управление на активите, видимост в реално време и обвързване с оперативните конфигурации.

11.4.2 RA-3 - Оценка на риска: Инвентарът на активите служи като основен елемент за моделиране на заплахи и оценка на риска.

11.4.3 MP-6 - Почистване на носители: Прилага се чрез сигурни методи за унищожаване, определени в контролите по жизнения цикъл на активите и Политиката за унищожаване на данни.

11.5 EU GDPR (2016/679):

11.5.1 Член 30 - Записи на дейностите по обработване: Изисква организациите да документират системите, устройствата и хранилищата, които съхраняват или обработват лични данни.

11.5.2 Член 32 - Сигурност на обработването: Съгласува се с оценка на риска, базирана на активите, и мерки за защита, съобразени с класифицираните активи и критичната инфраструктура.

11.6 Директива NIS2 на ЕС (2022/2555):

11.6.1 Член 21(2)(a, b): Изисква видимост и инвентаризация на активите като основа за анализ на риска, защита и реагиране при инциденти по киберсигурност.

11.6.2 Член 21(3): Подчертава необходимостта от структурирано управление на активите като част от културата на сигурност в организацията.

11.7 EU DORA (2022/2554):

11.7.1 Член 5 - Управление на ИКТ и вътрешен контрол: Изисква финансовите субекти да контролират ИКТ активите чрез ясен инвентар, собственост и изисквания за защита.

11.7.2 Член 9 - Рамка за управление на ИКТ риска: Установява, че процесите по управление на активите трябва да подпомагат смекчаването на заплахите, планирането на непрекъсваемостта и устойчивостта на услугите.

11.8 COBIT 2019:

11.8.1 BAI09 - Управление на активите: Пряко съответства на структурираното идентифициране, класифициране, използване и унищожаване на организационните активи.

11.8.2 DSS01 - Управлявани операции: Подпомага внедряването на контроли, които осигуряват защита на активите и непрекъснато оперативно управление.

11.8.3 MEA03 - Мониторинг, оценяване и преценка на съответствието: Осигурява редовно одитиране на контролите за управление на активите и тяхната ефективност по отношение на регулаторното съответствие.