					Въведете тук наименованието на регистрираното юридическо лице							
Номер на документа: P18S					Заглавие на документа: **Политика за криптографски контроли**							
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**

Съответствие със стандарти и нормативни изисквания

Стандарт/регулация	Клауза/член	Коментар
ISO/IEC 27001:2022	Клауза 8	
ISO/IEC 27002:2022	Контроли 8.24, 8.25	
NIST SP 800-53 Rev. 5	SC-12 до SC-17	
NIS2 на ЕС	Членове 21(2)(d), 21(2)(e)	
DORA на ЕС	Членове 6(2)(d), 9(2)(f)	
COBIT 2019	DSS05.01, APO13	
GDPR на ЕС	Членове 32(1)(a), 34	

1. Цел

1.1 Настоящата политика определя задължителните изисквания за използването на криптиране и криптографски контроли за защита на поверителността, целостта и автентичността на служебни и лични данни.

1.2 Тя гарантира, че криптографските средства се използват по подходящ начин в системи, устройства и облачни услуги в среда на малко предприятие.

1.3 Настоящата политика пряко подпомага сертифицирането по ISO/IEC 27001:2022 и подпомага организацията при изпълнение на правните задължения по Общия регламент относно защитата на данните на ЕС (GDPR), Директивата NIS2 на ЕС и Регламента за цифровата оперативна устойчивост (DORA).

1.4 Обхванатите криптографски контроли включват криптиране на данни, управление на сертификати, сигурно управление на ключове и криптирани резервни копия.

2. Обхват

2.1 Настоящата политика се прилага за:

2.1.1 Всички служители, външни изпълнители и трети страни, които обработват данни на дружеството

2.1.2 Всички бизнес системи, крайни устройства и облачни платформи, използвани за съхранение, предаване или достъп до поверителна информация

2.1.3 Всички лични, финансови, правни или чувствителни записи, класифицирани съгласно политиката на организацията за класификация на данните

2.1.4 Всеки криптографски контрол, включително методи за криптиране, ключове, пароли, сертификати и модули за сигурност

2.2 Политиката обхваща данни в покой, данни при пренос и данни при използване. Тя урежда също използването на криптиране за резервни копия, електронна поща, външни трансфери на данни и публично достъпни уебсайтове.

3. Цели

3.1 Да се гарантира, че чувствителните и регулираните данни са защитени по всяко време чрез подходящи криптографски мерки

3.2 Да се определят отговорностите за избор, конфигуриране и управление на средствата за криптиране и ключовете

3.3 Да се предотвратяват неоторизиран достъп, подправяне или изтичане на данни чрез прилагане на контроли за сигурно предаване и съхранение

3.4 Да се осигури съответствие с правните и регулаторните изисквания, налагащи криптиране на лични и служебни данни

3.5 Да се поддържат оперативната сигурност и наличност чрез ефективно управление на сертификати и криптографски ключове

4. Роли и отговорности

4.1 Управител

4.1.1 Одобрява настоящата политика и гарантира прилагането на криптографските изисквания

4.1.2 Преглежда изключенията, уведомленията за нарушения и съответствието на доставчиците с изискванията за криптиране

4.1.3 Проверява дали възложените на външни изпълнители или предоставяните в облак услуги отговарят на стандартите за криптиране

4.2 Доставчик на ИТ поддръжка / вътрешен ИТ администратор

4.2.1 Внедрява и поддържа решения за криптиране (напр. пълнодисково криптиране, SSL/TLS сертификати, VPN)

4.2.2 Управлява жизнения цикъл на криптографските ключове и средствата за сигурно съхранение

4.2.3 Конфигурира и наблюдава криптирането за защита на резервни копия, уебсайтове и устройства

[... 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 Годишен преглед

9.1.1 Настоящата политика трябва да се преглежда най-малко веднъж годишно от Управителя в координация с доставчика на ИТ поддръжка и Координатора по защита на данните.

9.2 Основания за междинен преглед

9.2.1 Прегледи трябва да се извършват и ако:

9.2.1.1 Криптографските стандарти или протоколи се променят (напр. отпадане на алгоритъм)

9.2.1.2 Се въвеждат нови системи или облачни услуги

9.2.1.3 Нарушение на сигурността или инцидент включва компрометиран ключ или сертификат

9.2.1.4 Правни или регулаторни промени оказват влияние върху изискванията за криптиране

9.3 Управление на версиите и комуникация

9.3.1 Всички промени в политиката трябва да бъдат документирани в регистър на версиите

9.3.2 Персоналът трябва да бъде уведомен за актуализациите, а предишните версии трябва да бъдат архивирани

9.3.3 Последната одобрена версия трябва да се съхранява в централното хранилище за политики

10. Свързани политики и връзки

10.1 Настоящата политика трябва да се прилага съвместно със следните SME политики:

10.1.1 P12S – Политика за управление на активите: Гарантира, че криптиране се прилага към класифицирани активи при съхранение, прехвърляне и унищожаване.

10.1.2 P14S – Политика за съхранение и унищожаване на данни: Определя сроковете за съхранение и изисква криптирано съхранение на данни до сигурното им изтриване.

10.1.3 P17S – Политика за защита на данните и поверителност: Съгласува криптирането с принципите за защита на данните и регулаторните изисквания по член 32 от GDPR.

10.1.4 P22S – Политика за регистриране и мониторинг: Изисква регистриране на използването на ключове, отказите на криптиране и изтичането на сертификати за целите на одита.

10.1.5 P30S – Политика за реагиране при инциденти: Описва процедурите за ескалация, ограничаване и уведомяване, когато криптирането откаже или ключове бъдат компрометирани.

11. Референтни стандарти и рамки

11.1 ISO/IEC 27001

11.1.1 Клауза 8.1 – Изисква внедряване на оперативни контроли, включително криптиране, за управление на рисковете за сигурността.

11.2 ISO/IEC 27002

11.2.1 Контрол 8.24 – Описва изискванията за прилагане на криптиране за поверителност и целост.

11.2.2 Контрол 8.25 – Определя изисквания за сигурно управление на криптографски ключове и сертификати.

11.3 NIST SP 800-53 Rev. 5

11.3.1 SC-12 – Установява изисквания за създаване и валидиране на криптографски ключове.

11.3.2 SC-13 – Определя стандарти за използване на криптографска защита.

11.3.3 SC-17 – Обхваща инфраструктурата с публичен ключ (PKI) и управлението на жизнения цикъл на сертификатите.

11.3.4 SC-28 – Изисква криптиране на данни в покой.

11.3.5 SC-12 до SC-17 (семейство) – Гарантира, че криптографските защити са правилно внедрени във всички системи.

11.4 GDPR на ЕС

11.4.1 Член 32(1)(a) – Изисква организациите да внедрят технически мерки като криптиране, за да осигурят поверителност на данните.

11.4.2 Член 34 – Посочва, че криптирането може да освободи организациите от задължение за уведомяване при нарушение, ако данните са били неразбираеми за неоторизирани лица.

11.5 Директива NIS2 на ЕС

11.5.1 Член 21(2)(d) – Изисква ефективно криптиране за защита на системи и комуникации.

11.5.2 Член 21(2)(e) – Подчертава защитата на данните и смекчаването на киберзаплахи чрез криптиране.

11.6 DORA на ЕС

11.6.1 Член 6(2)(d) – Изисква ИКТ системите да поддържат сигурни комуникационни канали и криптиране.

11.6.2 Член 9(2)(f) – Задължава финансовите субекти да използват силно криптиране за защита на цифровите комуникации и обмена на данни.

11.7 COBIT 2019

11.7.1 DSS05.01 – Изисква защита на чувствителната информация чрез криптиране и криптографски протоколи.

11.7.2 APO13.02 – Изисква ефективно внедряване на контроли за сигурност, включително криптографски мерки, като част от планирането на информационната сигурност.