					Въведете тук наименованието на регистрираното юридическо лице							
Номер на документа: P18					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**

Съгласувана с приложимите стандарти и регулации

Стандарт/регулация	Клауза/член	Коментар
ISO/IEC 27001:2022	Clause 8	-
ISO/IEC 27002:2022	Контроли 8.24, 8.25, 8	-
NIST SP 800-53 Rev.5	SC-12 до SC-17, SC-28, SC-28(1), SC-12(3)	-
GDPR на ЕС	Член 32, членове 33–34, съображение 83	-
NIS2 на ЕС	Член 21(2)(d)	-
DORA на ЕС	Членове 6(2)(d), 11(1)(c)	-
COBIT 2019	DSS05.01, DSS06.06, MEA	-

1. Цел

1.1 Настоящата политика определя задължителните изисквания за сигурно и съответстващо използване на криптографски контроли в цялата организация с цел гарантиране на поверителността, целостта и автентичността на чувствителна и регулирана информация.

1.2 Използването на криптография е основен елемент за изграждане на доверие в дейностите по защита на данните, подпомага сигурните комуникации, налага контрол на достъпа и осигурява регулаторно съответствие чрез ефективни практики за криптиране и управление на ключове.

1.3 Настоящата политика е съгласувана с ISO/IEC 27001:2022, клауза 8.1 и Приложение A, контрол 8.24, и подпомага изпълнението на правните и оперативните задължения по GDPR, член 32, DORA, член 6(2)(d), и NIS2, член 21. Тя също така подпомага целите на COBIT 2019, свързани с услугите по сигурност и защитата на информационните активи.

2. Обхват

2.1 Настоящата политика се прилага за всички организационни единици, бизнес функции, служители и външни доставчици на услуги, които участват в използването, администрирането или внедряването на криптографски средства и методи.

2.2 Обхванатите среди включват продукционни, развойни и тестови среди, системи за архивиране и среда за аварийно възстановяване, в които чувствителни данни се предават, обработват или съхраняват.

2.3 Обхватът включва всички криптографски компоненти и случаи на използване, включително, но не само:

2.3.1 Симетрично и асиметрично криптиране

2.3.2 Цифрови подписи и сертификати

2.3.3 Хеширащи алгоритми

2.3.4 Сигурно генериране, разпределяне и унищожаване на ключове

2.3.5 Transport Layer Security (TLS), пълнодисково криптиране и криптиране на ниво приложни програмни интерфейси (API)

2.3.6 Защитени елементи, като Hardware Security Modules (HSM), Trusted Platform Modules (TPM) и Key Management Systems (KMS)

2.4 Настоящата политика урежда използването на криптография по отношение на:

2.4.1 Данни, класифицирани като Поверителна, Строго поверителна или Регулирана

2.4.2 Автентикация и проверка на цифровата идентичност

2.4.3 Сигурни комуникации с външни страни

2.4.4 Попечителство върху ключове и механизми за двоен контрол

3. Цели

3.1 Да гарантира, че криптографските технологии се избират, одобряват, внедряват и поддържат в съответствие с бизнес риска, международните стандарти и регулаторните изисквания.

3.2 Да установи стандартизирана структура за управление на криптографските услуги, включително ясна отчетност за внедряването, валидирането и обработването на изключения.

3.3 Да предотвратява неразрешеното използване, неправилната конфигурация или остаряването на криптографски алгоритми и контроли чрез формализиран процес за одобрение и преглед.

3.4 Да гарантира, че криптографските контроли се интегрират още на етапа на проектиране на системите и се валидират регулярно, за да се предотвратят излагане на данни, компрометиране на ключове или отслабване на протоколи.

3.5 Да налага управление на жизнения цикъл на всички криптографски ключове, включително генериране, съхранение, използване, ротация, отнемане и сигурно унищожаване.

3.6 Да осигурява съответствие с международните и регионалните регулации, изискващи криптиране и сигурно обработване на данни, включително GDPR, DORA, NIS2 и COBIT 2019.

4. Роли и отговорности

4.1 Мениджър по информационна сигурност / Главен директор по информационна сигурност

4.1.1 Отговаря за настоящата политика и осигурява нейното съгласуване със Системата за управление на информационната сигурност (СУИС) и ISO/IEC 27001, Приложение A, контрол 8.24.

4.1.2 Одобрява използването на криптографски алгоритми и контроли и осигурява тяхното спазване в цялата организация.

4.2 Ръководител на криптографските операции / Архитект по сигурността

4.2.1 Управлява ежедневните операции и администрирането на криптографските системи.

4.2.2 Поддържа Списъка на одобрените криптографски методи (ACML) и Регистъра за управление на ключове.

4.2.3 Провежда прегледи на криптографския дизайн (CDR) и оценява нови криптографски технологии.

[... 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 Настоящата политика трябва да се преглежда ежегодно от Мениджъра по информационна сигурност и Ръководителя на криптографските операции.

9.2 Основанията за преглед включват:

9.2.1 Установяване на криптографски уязвимости (напр. понижаване на алгоритми, квантови атаки)

9.2.2 Регулаторни промени, изискващи актуализирани стандарти за криптиране

9.2.3 Оперативни или одитни констатации, разкриващи пропуски в политиката

9.2.4 Надграждане на криптографски инструменти или промени в архитектурата

9.3 Актуализациите трябва да се управляват чрез версиониране в Регистъра за контрол на документи на СУИС и да се комуникират до:

9.3.1 Всички администратори с роли за достъп до криптографски средства

9.3.2 Екипите по разработка и ръководителите по DevSecOps

9.3.3 Доставчици от трети страни, обвързани с договорни задължения за криптиране

9.4 Екипът по СУИС трябва да гарантира, че заменените версии се архивират и не се използват повече като референтен източник в оперативните процедури.

10. Свързани политики и връзки

10.1 P1 - Политика за информационна сигурност. Осигурява основната рамка за управление на всички мерки за сигурност, включително прилагането на криптографски контроли, защитата на активите и сигурните комуникации.

10.2 P4 - Политика за контрол на достъпа. Гарантира, че логическият достъп до криптографски материал и системи за управление на криптиране е строго ограничен въз основа на минимални привилегии и разделение на задълженията.

10.3 P6 - Политика за управление на риска. Подпомага оценката на рисковете, свързани с криптографските контроли, и документира стратегията за третиране на риска при изключения, остаряване на алгоритми или сценарии за компрометиране на ключове.

10.4 P12 - Политика за управление на активите. Изисква класификация на чувствителни данни и хардуерни активи, която пряко определя криптографските изисквания и задълженията по попечителство върху ключове.

10.5 P13 - Политика за класификация и етикетиране на данни. Определя нивата на класификация (напр. Поверителна, Регулирана), които задействат конкретни изисквания за криптиране при пренос и при съхранение.

10.6 P14 - Политика за съхранение и унищожаване на данни. Определя процедурите за сигурно унищожаване на криптирани носители за съхранение и криптографски ключов материал при извеждане от употреба.

10.7 P30 - Политика за реагиране при инциденти. Описва стратегията на организацията за реакция при компрометиране на ключове, неправомерно използване на сертификати или предполагаеми алгоритмични уязвимости, включително бързо отнемане и докладване на нарушение на сигурността.

11. Референтни стандарти и рамки

11.1 ISO/IEC 27001

11.1.1 Клауза 8.1 - Оперативно планиране и контрол: Налага технически контроли за сигурност, включително криптографски мерки, като част от оперативните мерки за защита.

11.2 ISO/IEC 27002:2022

11.2.1 Контроли 8.24, 8.25, 8: Предоставя насоки за внедряване по отношение на целите на криптографските контроли, избора на алгоритми, прилагането на протоколи и управлението на жизнения цикъл на сертификатите.

11.3 NIST SP 800-53 Rev.

11.3.1 SC-12 - Установяване на криптографски ключове: Осигурява сигурно генериране и обмен на ключове за криптиране. P18 определя как симетричните и асиметричните ключове трябва да бъдат генерирани и обменяни чрез одобрени алгоритми и протоколи.

11.3.2 SC-13 - Криптографска защита: Изисква използване на криптография за защита на поверителността и целостта на информацията. P18 налага криптиране при съхранение и при

пренос въз основа на класификацията на данните, като стандартите за алгоритми са съгласувани с NIST FIPS 140-3.

11.3.3 SC-17 - Сертификати за инфраструктура с публичен ключ (PKI): Изисква внедряване на PKI в подкрепа на автентикация и цифрови подписи. P18 определя използването на PKI за защита на комуникации, системни идентичности и административен достъп.

11.3.4 SC-28, SC-28(1) - Защита на информацията при съхранение и при пренос: Изисква криптиране на данни при съхранение или предаване през недоверени мрежи. P18 определя прилагането на TLS, VPN тунели, пълнодисково криптиране и методи за сигурно съхранение на чувствителни данни.

11.3.5 SC-12(3) - Генериране на симетрични ключове за сигурно съхранение и разпределение: Фокусира се върху сигурното генериране и обработване на симетрични ключове. P18 изисква използването на силни генератори на случайни числа, политики за ротация на ключове и защитени хранилища за ключове за криптографски операции.

11.4 GDPR на ЕС (2016/679)

11.4.1 Член 32 - Сигурност на обработването: Изрично препоръчва криптиране като мярка за намаляване на риска за личните данни.

11.4.2 Съображение 83: Подчертава криптирането като контрол за предотвратяване на неразрешен достъп до данни.

11.4.3 Членове 33 и 34: Ефективното криптиране може да освободи организациите от задължителни уведомления при нарушение на сигурността.

11.5 Директива NIS2 на ЕС (2022/2555)

11.5.1 Член 21(2)(d): Изисква технически и организационни мерки, включително криптографски защити, за поддържане на наличността и целостта на услугите.

11.6 DORA на ЕС (2022/2554)

11.6.1 Член 6(2)(d): Финансовите институции трябва да защитават данните, включително чрез силно криптиране на критична информация.

11.6.2 Член 11(1)(c): Изисква сигурни контроли за обработване на данни от външни доставчици на ИКТ услуги.

11.7 COBIT 2019

11.7.1 DSS05.01 - Protect Information Assets: Изисква използването на криптиране и управление на ключове за защита на данните срещу неразрешен достъп.

11.7.2 DSS06.06 - Managed Security Testing: Препоръчва валидиране на съответствието на криптографските контроли като част от оценките на уязвимостите.

11.7.3 MEA03 - Monitor, Evaluate and Assess Compliance: Налага непрекъсната увереност в ефективността на контролите по отношение на криптографските контроли.