					Въведете тук наименованието на регистрираното юридическо лице							
Номер на документа: P16					Заглавие на документа: **Политика за маскиране на данни и псевдонимизация**							
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 6.1	Общи изисквания за управление на риска и оперативни контроли за маскиране и псевдонимизация
ISO/IEC 27002:2022	Контроли 8.11, 8	Насоки за прилагане на маскиране и псевдонимизация
NIST SP 800-53 Rev.5	PM-17, PT-2, PT-3, SC-12, SC-28, SC-30	Контроли за защита на поверителността и данните за минимизиране на данните, трансформация и ограничаване на достъпа
EU GDPR	Членове 4(5), 5(1)(c,f), 32	Правно основание и изисквания за псевдонимизация и мерки за защита на данните
EU NIS2	Член 21(2)(c)	Задължение за технически и организационни мерки, включително технологии за повишаване на поверителността (PETs)
EU DORA	Членове 10(1), 10(2)(e)	Управление на ИКТ риска и контроли за поверителност при маскиране на данни и псевдонимизация
COBIT 2019	DSS05.01, DSS06.06, MEA	Управленски контроли за защита на данните чрез маскиране и оценка на съответствието

1. Цел

1.1 Тази политика определя подхода на организацията за прилагане на маскиране на данни и псевдонимизация като технологии за повишаване на поверителността (PETs) с цел намаляване на възможността за идентифициране и ограничаване на експозицията на лични или чувствителни данни.

1.2 Тя подпомага сигурното използване на информацията в дейности по тестване, анализ и експлоатация, като едновременно с това осигурява съответствие с правните и регулаторните изисквания, намалява въздействието при инциденти по сигурността и прилага принципите за минимизиране на данните и защита на поверителността.

1.3 Политиката е съгласувана с ISO/IEC 27001:2022, подкрепя член 4(5) от GDPR относно псевдонимизацията и интегрира прилагане, базирано на риска, в съответствие със стандартите NIST, NIS2, DORA и COBIT 2019.

2. Обхват

2.1 Тази политика се прилага за:

2.1.1 всички служители, външни изпълнители, трети страни и доставчици, които имат достъп до системи, обработващи лична, поверителна или чувствителна информация.

2.1.2 всички среди за данни, включително продукционни, развойни, тестови и среди за осигуряване на качеството.

2.1.3 всички форми на маскиране на данни (напр. статично, динамично, детерминистично, токенизация) и техники за псевдонимизация, използвани за намаляване на рисковете за поверителността.

2.1.4 всички видове данни (структурирани или неструктурирани), системи (локални или хоствани в облачна среда) и приложения, включващи лични или регулирани данни.

2.2 Обхватът включва използване в:

2.2.1 разработка на приложения и среди за осигуряване на качеството/тестване

2.2.2 платформи за анализ или отчетност

2.2.3 обмен на данни с трети страни или външни доставчици на услуги

2.2.4 системи за архивиране, архивно съхранение или възстановяване

3. Цели

3.1 Да се осигури последователно и ефективно прилагане на маскиране и псевдонимизация за намаляване на рисковете от експозиция или неправомерно използване на данни.

3.2 Да се гарантира, че реални данни никога не се използват в среди извън продукционната, освен ако не са трансформирани чрез одобрени PET техники.

3.3 Да се поддържат референтната цялост, използваемостта и трансформациите със запазване на формата, когато това е необходимо за оперативна последователност.

3.4 Да се прилагат строги контроли на достъпа до първични данни, маскирани данни и ключове за повторна идентификация.

3.5 Маскираните или псевдонимизираните набори от данни се третират като чувствителни данни и подлежат на регистриране на достъпа, контроли за сроковете за съхранение и процедури за реагиране при инциденти.

3.6 Да се валидира ефективността на тези контроли чрез непрекъснато тестване, наблюдение и одитни процедури.

4. Роли и отговорности

4.1 Изпълнително ръководство

4.1.1 Одобрява тази политика и осигурява нейното прилагане като част от по-широката рамка за ИТ управление и инициативите за защита на данните.

4.2 Директор по информационна сигурност (CISO) / Мениджър на СУИС

4.2.1 Осъществява надзор върху внедряването и текущото съответствие.

4.2.2 Осигурява съответствие с клауза 6.1.3 от ISO/IEC 27001 (третиране на риска) и клауза 8.1 (оперативен контрол).

4.2.3 Преглежда одитните журнали и валидира ефективността на контролите.

[... 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 Тази политика подлежи на преглед най-малко веднъж годишно или по-рано в случай на:

9.1.1 регулаторни промени, засягащи маскирането или псевдонимизацията

9.1.2 внедряване на нови ИТ системи, обработващи чувствителни данни

9.1.3 съществени промени в схемата за класификация на данните на организацията

9.1.4 одитни констатации, показващи дефицити в контролите

9.1.5 възникване на нови заплахи или технологии за маскиране

9.2 Мениджърът на СУИС трябва да ръководи прегледа в консултация с DPO, собствениците на данни, ИТ сигурност и функцията „Правни въпроси и съответствие“. Актуализациите трябва да бъдат под управление на версиите, одобрени от Висшето ръководство и съобщени на всички засегнати заинтересовани страни.

10. Свързани политики и връзки

10.1 P13 - Политика за класификация и етикетиране на данни. Решенията за маскиране и псевдонимизация зависят пряко от класификацията на полетата с данни и нивата на чувствителност, определени в P13.

10.2 P14 - Политика за съхранение и унищожаване на данни. Трансформираните набори от данни трябва да се съхраняват и унищожават в съответствие с правилата за жизнения цикъл в P14, като се гарантира, че маскираните и псевдонимизираните данни се третират като чувствителни.

10.3 P17 - Политика за защита на данните и поверителност. Осигурява принципите за защита на личните данни и регулаторните основания за прилагане на псевдонимизация като дейност по обработване в съответствие с GDPR и сходни нормативни актове.

10.4 P22 - Политика за регистриране и мониторинг. Осигурява централизирано одитиране и предупреждения за събития, свързани с маскиране и псевдонимизация, в съответствие със структурирани протоколи за мониторинг на сигурността.

11. Референтни стандарти и рамки

11.1 ISO/IEC 27001

11.1.1 Клауза 6.1.3 - План за третиране на риска: Определя маскирането и псевдонимизацията като механизми за третиране на риска с цел намаляване на възможността за идентифициране на чувствителни данни в среди за обработване, които не са съществени за дейността.

11.1.2 Клауза 8.1 - Оперативно планиране и контрол: Изисква технически и процедурни контроли за сигурна трансформация на данни при обработване, съхранение или пренос.

11.2 ISO/IEC 27002:2022

11.2.1 Контроли 8.11, 8: Насоки за маскиране на данни и псевдонимизация с цел минимизиране на рисковете от повторна идентификация и изтичане.

11.3 NIST SP 800-53 Rev.5

11.3.1 PM-17 - Защита на PII: Прилагане на технологии за повишаване на поверителността, като маскиране и псевдонимизация.

11.3.2 PT-2, PT-3: Минимизиране и сигурност при обработването на PII - трансформация за намаляване на възможността за идентифициране и прилагане на контрол на достъпа.

11.3.3 SC-12, SC-28, SC-30: Поверителност и цялост на данните - контроли за поверителност и обфускация при съхранение, пренос и използване.

11.4 EU GDPR (2016/679)

11.4.1 Член 4(5): Официално определение на псевдонимизация.

11.4.2 Член 32: Сигурност на обработването - организационни и технически мерки за псевдонимизация.

11.4.3 Член 5(1)(c,f): Минимизиране на данните и защита на поверителността чрез псевдонимизация/маскиране.

11.5 Директива ЕС NIS2 (2022/2555)

11.5.1 Член 21(2)(c): Изисква технологии PET, като маскиране и псевдонимизация, като мерки за сигурност.

11.6 EU DORA (2022/2554)

11.6.1 Член 10(1): Рамката за управление на ИКТ риска включва контроли за маскиране и псевдонимизация.

11.6.2 Член 10(2)(e): Изисква използване на технологии за трансформация за защита на лични и финансови данни.

11.7 COBIT 2019

11.7.1 DSS05.01: Защита на информационни активи - изисквания за маскиране и псевдонимизация.

11.7.2 DSS06.06: Сигурно тестване и анализ - маскиране в среди извън продукционната среда.

11.7.3 MEA03: Мониторинг на съответствието за ефективността на маскирането и псевдонимизацията.