					Въведете тук наименованието на регистрираното юридическо лице							
Номер на документа: P16S					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 регулаторни изисквания

Стандарт/регулация	Клауза/член	Коментар
ISO/IEC 27001:2022	Клауза 6.1.3, Клауза 8	Рискове за информационната сигурност и необходимите контроли, включително маскиране и псевдонимизация
ISO/IEC 27002:2022	Контроли 8.11, 8.12	Насоки относно маскирането и предотвратяването на изтичане на данни
NIST SP 800-53 Rev.5	SC-12, SC-28, PT-2, PT-3	Обфускация на данни, технологии за повишаване на поверителността
EU NIS2	Член 21(2)(c)	Пропорционални технически мерки, включително псевдонимизация като контрол
EU DORA	Член 10(1)	Контроли за ИКТ риска, включително защитни мерки при трансформиране на данни
COBIT 2019	DSS05.01, DSS06	Защита на данните, техники за обфускация и псевдонимизация
EU GDPR	Членове 4(5), 5(1)(c), 32	Минимизиране на данните, псевдонимизация като технически контрол

1. Цел

1.1. Настоящата политика определя задължителните изисквания за използване на маскиране на данни и псевдонимизация с цел защита на чувствителни, лични и поверителни данни в малки и средни предприятия (МСП).

1.2. Тези техники са задължителни, когато използването на реални данни не е необходимо, например при разработка, анализи или в сценарии с външни доставчици на услуги, като допринасят за намаляване на риска от разкриване, неправомерно използване или инцидент по сигурността.

1.3. Настоящата политика пряко подпомага съответствието с ISO/IEC 27001:2022, както и с европейски регулаторни изисквания като GDPR, Директива NIS2 и Регламент DORA.

1.4. Чрез трансформиране на данните преди използването им извън първоначалния им бизнес контекст организацията ограничава отговорността и повишава способността си да докаже надлежно спазване на изискванията за поверителност и сигурност.

2. Обхват

2.1. Настоящата политика се прилага за всички структурирани и неструктурирани данни, класифицирани като лични, поверителни или чувствителни, независимо дали се съхраняват или обработват:

2.1.1. В продукционни, тестови или развойни среди

2.1.2. На локални устройства, сървъри или облачни платформи

2.1.3. От вътрешен персонал, външни изпълнители или външни доставчици

2.2. Политиката обхваща също всички инструменти за трансформиране на данни (маскиране, токенизация, псевдонимизация), независимо дали са с отворен код, търговски или разработени вътрешно.

2.3. Случаите на приложение по тази политика включват:

2.3.1. Подготовка на тестови или развойни набори от данни

2.3.2. Експортиране на данни към системи за анализ

2.3.3. Достъп на доставчици или консултанти до оперативни системи

2.3.4. Минимизиране на данните за субектите на данни с цел намаляване на риска при обработването

3. Цели

3.1. Да се гарантира, че реални лични или чувствителни данни никога не се разкриват в среди с по-ниско ниво на сигурност, когато това не е строго необходимо.

3.2. Да се изисква използването на техники за маскиране или псевдонимизация, когато реалните идентификатори не са строго необходими за изпълнение на задачата.

3.3. Да се предотвратява неоторизиран достъп или неправомерно използване на данни чрез прилагане на контроли за трансформиране преди прехвърляне или обработване на данни.

3.4. Да се гарантира, че всички процеси по маскиране и псевдонимизация са проследими, одитируеми и се изпълняват чрез одобрени инструменти.

3.5. Да се осигури съответствие с приложимите правни и регулаторни изисквания относно минимизирането на данните, поверителността и защитните мерки при трансформиране на данни.

4. Роли и отговорности

4.1. Управител (GM)

4.1.1. Носи отговорност за тази политика и я одобрява

4.1.2. Осигурява, че всички отдели и доставчици спазват изискванията за трансформиране на данни

4.1.3. Преглежда изключенията, оценките на риска и журналите за трансформиране

4.1.4. Координира правни, оперативни и действия спрямо доставчици при нарушения

4.2. Доставчик на ИТ поддръжка / вътрешен ИТ екип

4.2.1. Избира и управлява инструменти за маскиране или псевдонимизация

4.2.2. Осигурява прилагането на подходящи методи за трансформиране според вида на данните

4.2.3. Поддържа журнали за трансформираните набори от данни и процедурите за управление на ключове

4.2.4. Осигурява маскирането да се извършва преди използване за тестове, от доставчици или за анализи

[... 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 бъде преглеждана най-малко веднъж годишно от Управителя (GM), за да се гарантира, че отразява:

9.1.1.1. Актуализации в приложимите регулации (напр. GDPR, DORA)

9.1.1.2. Нови бизнес системи или обмен на данни с трети страни

9.1.1.3. Обратна връзка от одити или инциденти, свързани с използването на немаскирани данни

9.2. Междинни прегледи

9.2.1. Прегледи трябва да се извършват също когато:

9.2.1.1. Се въвеждат нови приложения или платформи, които обработват чувствителни данни

9.2.1.2. Съществен инцидент разкрие пропуски в текущите контроли за трансформиране

9.2.1.3. Промени в нивата на класификация засягат процедурите за обработване на данни

9.3. Управление на версиите и промените

9.3.1. Всички промени по политиката трябва да бъдат:

9.3.1.1. Одобрени от Управителя (GM) и документирани в журнал на промените

9.3.1.2. Ясно комуникирани на засегнатите служители и доставчици на услуги

9.3.1.3. Архивирани по сигурен начин с ограничен достъп до невалидните версии

10. Свързани политики и връзки

10.1. Настоящата политика трябва да се прилага съвместно със следните политики за МСП, за да се осигури последователна и задължителна защита на чувствителните данни:

10.1.1. P13S – Политика за класификация и етикетиране на данни: Определя нивата на класификация (напр. „Поверително – лични данни“), които определят кога трябва да се прилагат маскиране или псевдонимизация. Настоящата политика налага правила за трансформиране според нивото на чувствителност на данните.

10.1.2. P14S – Политика за съхранение и унищожаване на данни: Осигурява трансформираните набори от данни, включително резервни копия, съдържащи маскирани или псевдонимизирани данни, да се съхраняват и унищожават съгласно приложимите правила, включително изтриване на ключовете за съпоставяне, когато вече не са необходими.

10.1.3. P17S – Политика за защита на данните и поверителност: Съгласува практиките за трансформиране с по-широките задължения за поверителност, включително изискванията на GDPR за минимизиране на данните и използване на псевдонимизация като защитна мярка при обработването на лични данни.

10.1.4. P30S – Политика за реагиране при инциденти: Обхваща процедурите за докладване и ескалация при неоторизирано разкриване на данни, включително неправомерна употреба или обратно възстановяване на маскирани или псевдонимизирани данни.

10.1.5. P2S – Политика за роли и отговорности в управлението: Определя общата отчетност за прилагането на политиката, приемането на риска и одобряването на изключения, основно от Управителя (GM).

10.2. Тези политики формират интегрирана рамка за защита на данните, като гарантират, че дейностите по маскиране и псевдонимизация подпомагат съответствието с ISO 27001 и изпълнението на множество регулаторни изисквания.

11. Референтни стандарти и рамки

11.1. ISO/IEC 27001

11.1.1. Клауза 6.1.3: Изисква третиране на рисковете за информационната сигурност, което включва ограничаване на експозицията чрез техники за трансформиране на данни.

11.1.2. Клауза 8.1: Изисква внедряване на необходимите контроли за постигане на целите по сигурността, включително псевдонимизация и маскиране.

11.2. ISO/IEC 27002

11.2.1. Контрол 8.11: Предоставя насоки за маскиране на чувствителни данни в тестови и развойни системи.

11.2.2. Контрол 8.12: Предлага подходи за предотвратяване на изтичане на данни чрез контролирано трансформиране и практики за достъп.

11.3. NIST SP 800-53 Rev.5

11.3.1. SC-12: Осигурява поверителност на информацията чрез обфускация на данни.

11.3.2. SC-28: Защитава информацията в покой и при използване.

11.3.3. PT-2/PT-3: Насърчават използването на технологии за повишаване на поверителността, включително псевдонимизация, при обработване на PII.

11.4. EU GDPR

11.4.1. Член 4(5): Дава правна дефиниция на псевдонимизацията и изисква контроли върху ключовете за съпоставяне и идентификаторите.

11.4.2. Член 5(1)(c): Подкрепя принципите за минимизиране на данните чрез маскиране.

11.4.3. Член 32: Признава псевдонимизацията като технически контрол, който намалява рисковете за поверителността.

11.5. Директива EU NIS2

11.5.1. Член 21(2)(c): Изисква пропорционални технически мерки за минимизиране на риска за сигурността на данните, включително псевдонимизация като част от контрола на риска.

11.6. Регламент EU DORA

11.6.1. Член 10(1): Изисква контроли за ИКТ риска, които включват защитни мерки за трансформиране на данни с цел непрекъсваемост и поверителност при външно възлагане и разработка на системи.

11.7. COBIT 2019

11.7.1. DSS05.01: Изисква защита на информационните активи, включително трансформиране, когато е приложимо.

11.7.2. DSS06.06: Изисква подходящи техники за обфускация и псевдонимизация за ограничаване на експозицията на данни в среди с по-ниско ниво на доверие.