					Въведете тук наименованието на регистрираното юридическо лице							
Номер на документа: P29S					Заглавие на документа: **Политика за тестови данни и тестови среди**							
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**

Съгласуване със стандарти и регулации

Стандарт/регулация	Клауза/член	Коментар
ISO/IEC 27001:2022	Клаузи 6.1, 8	
ISO/IEC 27002:2022	Контроли 8.28–8.29	
NIST SP 800-53 Rev. 5	SA-11, SA-12, SC-32	
GDPR на ЕС	Членове 5(1)(c), 25, 32	
NIS2 на ЕС	Член 21(2)(e), (h)	
DORA на ЕС	Член 9	
COBIT 2019	BAI07, DSS05	

1. Цел

1.1 Настоящата политика определя как се управляват тестовите данни и тестовите среди, за да се предотвратят случайно разкриване на информация, нарушения на сигурността на данните или оперативни прекъсвания по време на дейности по тестване.

1.2 Тя гарантира, че реални клиентски данни никога не се използват неправомерно при тестване на софтуер или системи и че тестовите среди са логически и технически отделени от продукционните системи.

1.3 Политиката е разработена, за да подпомага МСП при изпълнение на изискванията за сертифициране по ISO/IEC 27001 и приложимото законодателство за защита на данните, като същевременно остава практична и приложима за организации без собствен ИТ екип.

2. Обхват

2.1 Настоящата политика се прилага за:

2.1.1 Всички тестови среди (напр. сървъри за предпроизводствена среда, изолирани тестови системи, среди за разработка)

2.1.2 Всички тестови данни, независимо дали са създадени ръчно, генерирани или извлечени от работещи системи

2.1.3 Целия персонал, участващ в дейности по тестване, включително служители, външни изпълнители, лица на свободна практика и доставчици на ИТ услуги

2.1.4 Всяко тестване, което може да повлияе на клиентски платформи, вътрешни бизнес системи или услуги на трети страни

2.2 Политиката обхваща както техническите среди, така и процесите, използвани в подкрепа на:

2.2.1 Разработване на уебсайтове, приложения и инструменти

2.2.2 Надграждане на системи, тестване на конфигурации и интеграционно тестване

2.2.3 Автоматизирани и ръчни функционални тестове или тестове за сигурност

3. Цели

3.1 Да се предотврати използването на реални, идентифицируеми клиентски данни при тестване, освен ако не са анонимизирани и изрично одобрени.

3.2 Да се поддържа строго разделение между тестови и продукционни системи, за да се избегнат неволно разкриване на данни или смущения в оперативната дейност.

3.3 Да се защитят тестовите системи и данни от неоторизиран достъп, случайно разкриване или повторна употреба в различни среди без подходящи контроли.

3.4 Да се спазват приложимите регулаторни изисквания за защита на данните (напр. GDPR, NIS2), като се гарантира, че всички тестови данни се обработват законосъобразно, добросъвестно и сигурно.

3.5 Да се подпомогне готовността на организацията за външни одити и сертифициране по ISO/IEC 27001 чрез документиране на практиките по тестване и прилагане на последователни мерки за защита.

4. Роли и отговорности

4.1 Управител

4.1.1 Носи цялостна отговорност за защитата на тестовите данни и сигурността на тестовите системи.

4.1.2 Одобрява всяко използване на реални данни при тестване след потвърждение, че са въведени подходящи мерки за защита (напр. анонимизация или маскиране на данни).

4.1.3 Проверява, че дейностите по тестване са надлежно документирани и са в съответствие с настоящата политика.

4.2 Ръководител на проект

4.2.1 Координира проектирането и изпълнението на процесите по тестване.

4.2.2 Гарантира, че всички членове на екипа разбират и спазват настоящата политика.

4.2.3 Потвърждава, че тестовите системи са конфигурирани сигурно преди започване на тестването.

4.2.4 Докладва на Управителя всички инциденти, свързани с тестови среди или изтичане на данни.

[... 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 Планирани прегледи

9.1.1 Настоящата политика трябва да бъде преглеждана най-малко веднъж годишно от Управителя. Прегледът гарантира, че политиката остава актуална спрямо:

9.1.1.1 Промени в инструментите, платформите или средите за разработка на софтуер

9.1.1.2 Актуализирани правни задължения, включително изисквания за защита на данните или цифрова оперативна устойчивост

9.1.1.3 Сертифициране на МСП и готовност за одит по ISO/IEC 27001

9.2 Събития, задействащи междинен преглед

9.2.1 Допълнителни прегледи трябва да се извършват след:

9.2.1.1 Всеки инцидент, свързан с разкриване на данни или компрометиране в тестови среди

9.2.1.2 Използване на реални данни при тестване, дори когато са анонимизирани

9.2.1.3 Въвеждане на нови методи за тестване, системи или доставчици

9.2.1.4 Регулаторни промени, засягащи начина на обработване на данните по време на тестване

9.3 Управление на промените и комуникация

9.3.1 Управителят отговаря за:

9.3.1.1 Актуализиране на настоящата политика и документиране на всички промени с история на версиите

9.3.1.2 Уведомяване на персонала, разработчиците и съответните доставчици на услуги за актуализациите

9.3.1.3 Потвърждаване, че всички лица, участващи в дейности, свързани с тестване, разбират и прилагат най-актуалните правила

9.3.1.4 Поддържане на достъпна версия на най-новата политика за целите на преглед и одит

9.4 Одит и документация

9.4.1 Записите за всички прегледи на политиката, одобренията за използване на реални данни и всички обосновки за изключения трябва да бъдат:

9.4.1.1 Съхранявани сигурно за целите на одита

9.4.1.2 Налични при поискване по време на вътрешни или одити от трети страни

9.4.1.3 Преглеждани ежегодно, за да се гарантира съответствие с практиките по тестване

10. Свързани политики и връзки

10.1 Настоящата политика трябва да се прилага съвместно със следните SME политики, за да се поддържат сигурността и съответствието по време на тестване:

10.1.1 P2S – Политика за роли и отговорности в управлението: Определя кой носи отговорност за надзора върху разработката, тестването и отговорностите по разделяне на системите.

10.1.2 P4S – Политика за контрол на достъпа: Урежда предоставянето, управлението и премахването на удостоверителни данни за достъп до тестови системи.

10.1.3 P8S – Политика за осведоменост и обучение по информационна сигурност: Гарантира, че персоналът разбира рисковете, свързани с тестовите данни, практиките за сигурно обработване и правилното разделяне на средите.

10.1.4 P13S – Политика за класификация и етикетиране на данни: Подпомага ясната класификация на тестовите данни и насочва прилагането на стратегии за анонимизация или маскиране на данни.

10.1.5 P17S – Политика за защита на данните и поверителност: Осигурява съгласуваност със задълженията по GDPR, включително мерки за защита при обработването и съхранението на лични данни, включително в тестови среди.

10.1.6 P24S – Политика за сигурна разработка: Определя общите изисквания за сигурност към екипите по разработка, включително безопасното използване на данни по време на фазите на тестване.

10.1.7 P30S – Политика за реагиране при инциденти: Описва как да се реагира при нарушение или проблем, установен в тестова среда или причинен от неправилно обработване на тестови данни.

10.2 Тези политики формират единна рамка за сигурност в подкрепа на целостта на тестването, минимизирането на данните и пълното съответствие с ISO/IEC 27001 в дейностите по разработка и осигуряване на качеството.

11. Референтни стандарти и рамки

11.1 ISO/IEC 27001

11.1.1 Клауза 6.1 – Изисква оценка на риска и действия за третиране на риска, включително рисковете, свързани с тестването.

11.1.2 Клауза 8.1 – Изисква планиране и контрол на оперативните процеси, включително подготовката на тестови системи и среди.

11.2 ISO/IEC 27002

11.2.1 Контрол 8.28 – Изисква организациите да защитават тестовите данни и да гарантират, че те не съдържат чувствителни данни или продукционни данни от работеща среда.

11.2.2 Контрол 8.29 – Изисква ясно разделение между среди за разработка, тестване и продукционна среда.

11.3 NIST SP 800-53 Rev. 5

11.3.1 SA-11 – Обхваща изискванията към контролите при разработка и тестване.

11.3.2 SA-12 – Разглежда рисковете при тестване във веригата на доставки и оценките на сигурността.

11.3.3 SC-32 – Изисква разделяне на средите и защита на поверителността и целостта на тестовите данни.

11.4 Общ регламент на ЕС относно защитата на данните (GDPR)

11.4.1 Член 5(1)(c) – Изисква минимизиране на данните, включително използване само на необходимите данни за тестване.

11.4.2 Член 25 – Изисква защита на данните още при проектиране, включително контроли за тестови среди.

11.4.3 Член 32 – Изисква сигурно обработване на лични данни във всички системи, включително в непроизводствени среди.

11.5 Директива NIS2 на ЕС (2022/2555)

11.5.1 Член 21(2)(e), (h) – Изисква сигурна разработка и тестване на системи, особено когато цифровите услуги са изложени на киберрискове.

11.6 DORA на ЕС (2022/2554)

11.6.1 Член 9 – Подчертава значението на цифровата оперативна устойчивост, включително сигурното тестване на ИКТ системи от МСП във финансовия сектор.

11.7 COBIT 2019

11.7.1 BAI07 – Управление на приемането на промени и прехода: Включва контроли при тестване за валидиране на нови системи и обработването на данни.

11.7.2 DSS05 – Управление на услугите по сигурност: Изисква практики за тестване и разработка, които предотвратяват неправомерна употреба или разкриване на служебна информация.