					Въведете тук наименованието на регистрираното юридическо лице							
Номер на документа: P29					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 регулаторни изисквания

Стандарт/регулация	Клауза/член	Коментар
ISO/IEC 27001:2022	Клауза 8	Относима към сигурното планиране и контрол на тестовите данни и среди
ISO/IEC 27002:2022	Контроли 8.28–8.29	Обхваща сигурното управление на тестовите данни и защитата на тестовите среди
NIST SP 800-53 Rev. 5	SA-11, SC-28, SC-32	Разглежда тестване и оценяване от разработчиците, защита на данни в покой и цялостност на информацията
GDPR на ЕС	Членове 5, 25, 32	Обхваща минимизиране на данните, защита на личните данни още при проектирането и сигурност на обработването в контекста на тестването
NIS2 на ЕС	Член 21(2)(e), (h)	Отнася се до практики за сигурна разработка и тестване
DORA на ЕС	Член 9	Отнася се до ИКТ системи, протоколи и сигурността на тестовите данни
COBIT 2019	DSS05, BAI07	Обхваща управлението на услугите по сигурност и приемането/прехода на промените

1. Цел

1.1. Настоящата политика определя задължителните изисквания за управление на тестовите среди и тестовите данни с цел осигуряване на сигурност, поверителност и оперативна цялост през целия жизнен цикъл на разработката и тестването на софтуер.

1.2. Политиката има за цел да предотвратява неоторизиран достъп, изтичане на данни и компрометиране на продукционни системи вследствие на неправилно управлявани тестови среди или използване на реални данни при тестване.

1.3. Политиката изисква сигурно обработване на данните, използвани за тестване, закаляване на тестовата инфраструктура и ролево базиран контрол на достъпа, като същевременно осигурява съответствие с приложимите регулаторни и договорни задължения.

2. Обхват

2.1. Настоящата политика се прилага за всички тестови среди, данни, инструменти и процеси, използвани за тестване на софтуер, системи, приложения и инфраструктура в рамките на организацията.

2.2. Политиката обхваща:

2.2.1. Тестови среди, предоставени в локална инфраструктура, в облака или чрез платформи на трети страни

2.2.2. Тестови данни, използвани при функционално тестване, тестване на производителността, регресионно тестване и тестване на сигурността

2.2.3. Ръчно, скриптово или автоматизирано тестване (напр. CI/CD конвейери)

2.2.4. Всички лица, участващи в тестването, включително вътрешни екипи, доставчици и външни изпълнители

2.3. Политиката се прилага независимо от критичността на системата, типа приложение или от това дали разработката е вътрешна или възложена на външен изпълнител.

3. Цели

3.1. Да се предотврати използването на реални, чувствителни или регулирани данни (напр. лично идентифициращa информация (PII), данни на картодържатели) в тестови среди, освен ако не са анонимизирани или изрично одобрени.

3.2. Да се осигури пълно мрежово и логическо разделяне между тестови и продукционни среди с цел предотвратяване на неоторизиран достъп до данни или компрометиране на системи.

3.3. Да се изисква криптиране, маскиране на данни или генериране на синтетични данни, когато за целите на тестването са необходими представителни данни.

3.4. Да се намали вероятността от несъответствия, експозиция на клиентски данни или оперативни прекъсвания, произтичащи от незащитени тестови данни или среди.

3.5. Да се съгласува обработването на тестови данни със стандарти на индустрията (ISO, NIST, COBIT) и регулации като GDPR, NIS2 и DORA.

4. Роли и отговорности

4.1. Директор по информационна сигурност (CISO)

4.1.1. Отговаря за тази политика и осигурява прилагането на технически и административни контроли за тестовите данни и среди.

4.1.2. Одобрява използването на реални или чувствителни данни при тестване при наличие на подходяща обосновка и компенсиращи контроли.

4.2. Ръководители на QA/тестване

4.2.1. Координират планирането на тестовете и осигуряват всички дейности по тестване да се извършват в съответствие с изискванията на тази политика.

4.2.2. Валидират правилното разделяне, достъпа и подготовката на данните за всеки етап на тестване.

[... Раздели 4.3–8 не са включени в тази предварителна версия. Закупете пълния документ за достъп до пълното съдържание. ...]

9. Преглед и актуализиране на изискванията

9.1. Настоящата политика трябва да се преглежда ежегодно и да се актуализира при необходимост, за да отразява:

9.1.1. Промени в регулаторните изисквания (напр. GDPR, DORA, NIS2)

9.1.2. Внедряването на нови инструменти за тестване, платформи или конвейери за автоматизация

9.1.3. Констатации от вътрешен одит или препоръки след инцидент

9.1.4. Разширяване на процесите по разработка или QA, които променят обработването на тестови данни или използването на среди

9.2. CISO носи отчетност за иницииране на прегледа в сътрудничество със:

9.2.1. Ръководители на QA/тестване

9.2.2. Мениджъри по DevOps и инфраструктура

9.2.3. Екипи по разработка на приложения

9.2.4. Длъжностното лице по защита на данните (DPO) и правен консултант

9.3. Всички редакции трябва да бъдат:

9.3.1. Под управление на версиите и съхранявани в централното хранилище за документи

9.3.2. Комуникирани на засегнатия персонал чрез формални канали (напр. уведомления в СУИС, екипни инструктажи)

9.3.3. Обвързани с актуализации на съответните технически стандарти, контроли и оперативни процедури

9.4. Междинни прегледи, задействани от събитие, трябва да се извършват незабавно след всяко:

9.4.1. Изтичане на данни или инцидент по сигурността, свързан с тестови среди

9.4.2. Одитно несъответствие, свързано с обработването на тестови данни

9.4.3. Съществени промени в правните задължения или ИТ архитектурата

10. Свързани политики и зависимости

10.1. Настоящата политика е тясно интегрирана със следните политики, за да осигури сигурно и съответстващо обработване на тестови данни и среди:

10.1.1. P1 – Политика за информационна сигурност: Установява общите принципи за сигурност, които уреждат защитата на тестовите данни и управлението на средите.

10.1.2. P5 – Политика за управление на промените: Прилага се за създаване, актуализация и извеждане от експлоатация на тестови среди и конвейери за разгръщане.

10.1.3. P13 – Политика за класификация и етикетиране на данни: Определя насоки за избор на тестови данни и прилагане на контроли според чувствителността.

10.1.4. P14 – Политика за съхранение на данни и унищожаване: Определя срокове за съхранение и изисквания за сигурно унищожаване на тестови набори от данни.

10.1.5. P15 – Политика за архивиране и възстановяване: Установява задължителни практики за архивиране и валидиране на възстановяването за тестови среди.

10.1.6. P18 – Политика за криптографски контроли: Определя задължителните стандарти за криптиране на данни в покой и данни при пренос в рамките на тестовите платформи.

10.1.7. P22 – Политика за регистриране и мониторинг: Регламентира видимостта и откриването на аномалии за дейностите в тестовите среди.

10.1.8. P30 – Политика за реагиране при инциденти: Определя ескалацията и действията за отстраняване при нарушения или инциденти, свързани с тестови системи.

10.1.9. P33 – Политика за мониторинг на одита и съответствието: Осигурява валидиране на спазването на политиката и непрекъснато уверение.

11. Референтни стандарти и рамки

11.1. Настоящата политика е съгласувана с глобални стандарти по киберсигурност и регулаторни рамки, които изискват сигурно обработване на тестови данни и защита на непроизводствени среди.

11.2. ISO/IEC 27001:

11.2.1. Клауза 8.1 – Изисква сигурно планиране и контрол на тестовите данни и среди.

11.3. ISO/IEC 27002:2022 – Контроли 8.28–8.29:

11.3.1. Приложение A, Контрол 8.28 – Сигурни тестови данни: Изисква защита на тестовите данни, използвани във фазите на разработка и тестване, чрез анонимизация, маскиране или синтетично генериране.

11.3.2. Приложение A, Контрол 8.29 – Защита на тестовите среди: Изисква разделяне от продукционната среда, контрол на достъпа и закаляване на средата за тестовите системи.

11.3.3. Тези контроли определят изисквания за сигурно управление на данните, използвани по време на тестване, и за защита на непроизводствените системи от злоупотреба, компрометиране или замърсяване.

11.4. NIST SP 800-53 Rev. 5:

11.4.1. SA-11 – Тестване и оценяване от разработчици: Установява очаквания за сигурни и повторяеми процедури за тестване с подходящи контроли върху данните.

11.4.2. SC-28 – Защита на информацията в покой: Съответства на криптирането на тестови данни, съхранявани в непроизводствени системи.

11.4.3. SC-32 – Цялостност на информацията: Подкрепя валидирането на данните, предотвратяването на повреждане и контролите на входа/изхода по време на тестване.

11.5. GDPR на ЕС (2016/679):

11.5.1. Член 5 – Минимизиране на данните: Забранява ненужното използване на лични данни при тестване.

11.5.2. Член 25 – Защита на личните данни още при проектирането: Изисква техники за защита на данните да бъдат прилагани от самото начало на цикъла на разработка и тестване.

11.5.3. Член 32 – Сигурност на обработването: Изисква предпазни мерки за тестови среди, които обработват лични или чувствителни данни.

11.6. Директива NIS2 на ЕС (2022/2555):

11.6.1. Член 21(2)(e), (h): Изисква процеси за сигурна разработка и тестване на софтуер с акцент върху защитата от неоторизиран достъп и изтичане на данни.

11.7. DORA на ЕС (2022/2554):

11.7.1. Член 9 – ИКТ системи и протоколи: Изисква процесите по тестване да подпомагат устойчивостта и да защитават оперативните данни от компрометиране или неоторизирано разкриване.

11.8. COBIT 2019:

11.8.1. DSS05 – Управление на услугите по сигурност: Подкрепя прилагането на политиките за сигурност във всички среди, включително непроизводствени.

11.8.2. BAI07 – Управление на приемането и прехода на промените: Обхваща формалния процес на преход от тестване към продукционна среда, включително контроли върху данните и средата.