					Въведете тук наименованието на регистрираното юридическо лице							
Номер на документа: P24					Заглавие на документа: **Политика за сигурна разработка**							
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**

1. Цел

1.1 Настоящата политика определя задължителните изисквания за сигурност при дейности по разработване на софтуер и системи в рамките на организацията, включително вътрешни проекти, външно възложена разработка и интегриране на код от трети страни.

1.2 Целта е да се гарантира, че сигурността е интегрирана във всички етапи от жизнения цикъл на разработка на софтуер (SDLC) и че уязвимостите се идентифицират, ограничават и предотвратяват преди внедряване в продукционна среда.

1.3 Тази политика подпомага прилагането на ISO/IEC 27001:2022, Клауза 8.1, и контролите от Приложение A 8.25–8.28, чрез стандартизиране на управлението на сигурната разработка, практиките за валидиране на кода и надзора върху разработката от трети страни.

2. Обхват

2.1 Тази политика се прилага за всички:

2.1.1 Софтуер, приложения, скриптове, интеграции и инструменти за автоматизация, разработени вътрешно или външно

2.1.2 Екипи по разработка, продуктови собственици, DevOps, QA, архитекти, ръководители на проекти и външни изпълнители

2.1.3 SDLC среди, включително среди за разработка, тестване, стейджинг и предпродукционни среди

2.1.4 Компоненти с отворен код и компоненти от трети страни, интегрирани във вътрешни приложения

2.1.5 Софтуер, внедряван в локална инфраструктура, частни облачни, хибридни или публични облачни среди

2.2 Всички потребители и страни, участващи в разработка, тестване или внедряване на системи в рамките на организацията, са длъжни да спазват тази политика, включително управлявани доставчици на услуги и доставчици на платформи.

3. Цели

3.1 Да се внедрят контроли за сигурност във всички етапи на разработката на софтуер — от проектирането до внедряването — така че намаляването на риска да бъде проактивно и непрекъснато.

3.2 Да се предотврати въвеждането на експлоатируеми уязвимости, като инжекционни уязвимости, незащитена автентикация и експозиция към известни слабости в компоненти от трети страни.

3.3 Да се установят и прилагат практики за сигурна разработка, съгласувани с OWASP, SANS CWE и указания, специфични за приложимите рамки.

3.4 Да се гарантира, че целият код преминава партньорска проверка, автоматизиран анализ и валидиране на сигурността преди внедряване.

3.5 Да се управляват рисковете при разработка, произтичащи от външно възложени дейности, включване на код от трети страни и повторно използване на софтуер с отворен код.

3.6 Да се защитят средите за разработка, тестване и стейджинг от неоторизиран достъп и да се предотврати използването на продукционни данни без одобрено маскиране или анонимизиране на данните.

3.7 Да се насърчава осведомеността по сигурност сред разработчици, продуктови мениджъри и специалисти по осигуряване на качеството чрез ролево базирано обучение и непрекъснати актуализации относно нововъзникващи заплахи.

4. Роли и отговорности

4.1 Директор по информационна сигурност (CISO)

4.1.1 Отговаря за тази политика и гарантира, че изискванията за сигурна разработка се прилагат в цялата организация.

4.1.2 Одобрява стандартите за сигурно програмиране и споразуменията за разработка от трети страни.

4.1.3 Валидира решенията за третиране на риска за неотстранени или отложени уязвимости.

4.2 Ръководител по сигурността на приложенията / Мениджър DevSecOps

4.2.1 Разработва, поддържа и популяризира указания за сигурно програмиране.

4.2.2 Интегрира статично и динамично тестване на сигурността в CI/CD конвейерите.

4.2.3 Извършва прегледи на сигурността на кода и определя задължителни коригиращи действия.

[... 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 трябва да се преглежда ежегодно или по-често в отговор на:

9.1.1 Съществени промени в методологиите за разработка или DevOps инструментите

9.1.2 Съществени инциденти по сигурността, произтичащи от уязвимости в приложенията

9.1.3 Промени в регулаторните изисквания, свързани със сигурния софтуер (напр. GDPR, DORA)

9.1.4 Нови индустриални стандарти или разузнавателна информация за заплахи (напр. OWASP Top 10, SLSA, MITRE CWE)

9.2 Прегледът на политиката се ръководи от Ръководителя по сигурността на приложенията в координация с Директора по информационна сигурност (CISO), софтуерните архитекти, ръководството на QA и правен консултант (по отношение на последиците от използването на код от трети страни).

9.3 Всички редакции трябва да бъдат регистрирани в регистъра за контрол на документи на СУИС, да бъдат под управление на версиите и да бъдат комуникирани към засегнатите екипи чрез бележки по изданието или задължително обучение.

9.4 Предходните версии трябва да се съхраняват в архивното хранилище за целите на правната и одитната проследимост.

10. Свързани политики и връзки

10.1 P1 – Политика за информационна сигурност. Определя стратегическия мандат за интегриране на сигурността във всички информационни системи, като сигурната разработка е основна оперативна контролна мярка.

10.2 P4 – Политика за контрол на достъпа. Определя контролните мерки за ограничаване на достъпа до среди за разработка, хранилища, инструменти за компилация и CI/CD конвейери.

10.3 P5 – Политика за управление на промените. Гарантира, че промените в кода, изданията и внедряванията подлежат на надлежно одобрение, планиране на връщане към предходно състояние и проверка след внедряване.

10.4 P12 – Политика за управление на активите. Подпомага инвентаризацията на средите за разработка, хранилищата за изходен код и системите за компилация като управлявани активи, подлежащи на класификация и защита.

10.5 P22 – Политика за регистриране и мониторинг. Прилага се към конвейерите за разработка, като гарантира, че процесите по компилация, промотирането на код и събитията по внедряване се регистрират, наблюдават и анализират за аномалии по сигурността.

10.6 P30 – Политика за реагиране при инциденти. Осигурява рамката за анализ и реагиране на слабости в сигурността, открити след внедряване или по време на тестване на сигурността на приложенията.

11. Референтни стандарти и рамки

11.1 ISO/IEC 27001:2022

11.1.1 Клауза 8.1 – Оперативно планиране и контрол: Изисква интегриране на процеси и контроли за сигурна разработка в операциите.

11.2 ISO/IEC 27002:2022 – Контроли 8.25–8.28

11.2.1 Контрол 8.25 от Приложение A – Жизнен цикъл на сигурната разработка: Изисква формално включване на сигурността в проектирането и разработката на софтуер.

11.2.2 Контрол 8.26 от Приложение A – Изисквания за сигурност на приложенията: Изисква определяне на критерии за сигурно програмиране и приемане по сигурност.

11.2.3 Контрол 8.27 от Приложение A – Принципи за сигурна архитектура и инженеринг на системи: Изисква прилагане на принципи за сигурен дизайн и ограничаване на известни слабости.

11.2.4 Контрол 8.28 от Приложение A – Сигурно програмиране: Изисква прилагане на практики за сигурно програмиране и контрол върху уязвимостите в изходния код.

11.3 NIST SP 800-53 Rev. 5

11.3.1 SA-3 до SA-15: Установява структурирани практики за сигурна разработка на приложения, включително изисквания за дизайн, целостта на кода и тестване.

11.3.2 SI-10 – Валидиране на входните данни: Обхваща защитни мерки за сигурно програмиране.

11.3.3 SR-3 – Сигурност на веригата на доставки: Изисква проверка на софтуер от трети страни, компоненти и доставчици на разработка.

11.4 GDPR на ЕС (2016/679)

11.4.1 Член 25 – Защита на данните още при проектирането и по подразбиране: Изисква внедряване на сигурност и поверителност в разработката на системи.

11.4.2 Член 32 – Сигурност на обработването: Подкрепя технически мерки като валидиране на входните данни, контрол на достъпа и сигурно внедряване.

11.5 Директива NIS2 на ЕС (2022/2555)

11.5.1 Член 21(2)(e–f): Изисква практики за разработка на софтуер, които включват управление на уязвимостите, сигурност на кода и докладване на инциденти.

11.6 DORA на ЕС (2022/2554)

11.6.1 Член 9 – Управление на ИКТ риска: Изисква практики за сигурна разработка за финансови субекти, включително контроли за качеството на софтуера и отстраняване на дефекти.

11.6.2 Член 10 – Непрекъсваемост на дейността и тестване: Насърчава стриктно тестване и валидиране на ИКТ системи, включително приложения.

11.7 COBIT 2019

11.7.1 BAI03 – Управление на идентифицирането и изграждането на решения: Регламентира дизайна, разработката и интегрирането на сигурността в нови решения.

11.7.2 BAI07 – Управление на приемането на промени и прехода: Гарантира сигурно внедряване и оценка след внедряване.

11.7.3 DSS05 – Управление на услугите по сигурност: Прилага валидиране на сигурността към предоставянето на софтуер и услуги.