					Въведете тук наименованието на регистрираното юридическо лице							
Номер на документа: P25					Заглавие на документа: **Политика за изискванията за сигурност на приложенията**							
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	Клауза 8	—
ISO/IEC 27002:2022	Контроли 8.25–8.26	—
NIST SP 800-53 Rev.5	SA-11, SA-15, SI-10	—
GDPR на ЕС	Членове 25, 32	—
NIS2 на ЕС	Членове 21(2)(f), 23	—
DORA на ЕС	Членове 9, 11	—
COBIT 2019	BAI03, BAI09, DSS05	—

1. Цел

1.1 Настоящата политика определя задължителни изисквания за сигурност на ниво приложение за софтуер, който се разработва, придобива, интегрира или внедрява от организацията. Тя гарантира, че всички приложения се проектират, разработват и поддържат в съответствие с принципите на сигурната разработка, правните задължения и апетита към риск на организацията.

1.2 Политиката изисква интегриране на сигурността през целия жизнен цикъл на приложението, включително автентикация на потребителите, обработване на данни, защита на интерфейсите и сигурно взаимодействие с приложно-програмни интерфейси (API) и услуги.

1.3 С приемането на настоящата политика организацията цели да предотвратява въвеждането на софтуерни уязвимости, да защитава чувствителните данни и да осигурява проследимост и устойчивост срещу експлоатация и злоупотреба.

2. Обхват

2.1 Настоящата политика се прилага за:

2.1.1 вътрешно разработени или външно доставени приложения, включително SaaS и индивидуално разработени инструменти

2.1.2 приложения, поддържащи критични бизнес операции, достъп на клиенти или обработване на регулирани данни

2.1.3 екипите по разработка, DevOps, QA, продуктов мениджмънт и сигурност

2.1.4 външни разработчици, доставчици на софтуер и партньори по интеграция с достъп до организационни приложения или приложно-програмни интерфейси (API)

2.2 Политиката се прилага във всички среди: разработка, тестване, предпроизводствени среди, продукционна среда и среда за аварийно възстановяване, независимо дали са хоствани в локална инфраструктура, в частни центрове за данни или в публични облачни среди.

3. Цели

3.1 Да се определят базови функционални и нефункционални изисквания за сигурност, които трябва да бъдат изпълнени от всички приложения, независимо от метода на разработка или технологичния стек.

3.2 Да се гарантира внедряването на защити на ниво приложение, включително валидиране на входните данни, кодиране на изхода, обработване на грешки и сигурност на сесиите.

3.3 Да се изиска сигурно внедряване на механизми за автентикация, оторизация и контрол на достъпа, съгласувани с организационните политики за управление на идентичности и достъп.

3.4 Да се въведе задължително сигурно взаимодействие с приложно-програмни интерфейси (API), уеб интерфейси и компоненти от трети страни чрез използване на одобрени протоколи и контроли за сигурност.

3.5 Да се осигури ранно откриване и ограничаване на уязвимости чрез статичен и динамичен анализ, преглед на изходния код и моделиране на заплахи.

3.6 Да се защитават чувствителните данни в съответствие с регулаторните изисквания чрез прилагане на криптиране, класификация и правила за срокове на съхранение.

3.7 Да се осигури непрекъснато валидиране на рисковата позиция по отношение на сигурността на приложенията след внедряване чрез тестване, мониторинг и готовност за одит.

4. Роли и отговорности

4.1 Директор по информационна сигурност (CISO)

4.1.1 Отговаря за настоящата политика и осигурява нейното съгласуване със стратегията на организацията за информационна сигурност и рисковия профил.

4.1.2 Одобрява изискванията за сигурност на приложенията и осигурява прилагането на задължителните контроли във функциите по разработка и снабдяване.

4.2 Ръководител „Сигурност на приложенията“ / Мениджър DevSecOps

4.2.1 Определя базовите контроли за сигурност и методологиите за тестване на компонентите на приложенията.

4.2.2 Осъществява надзор върху сигурната интеграция на инструменти като SAST, DAST, IAST и SCA в конвейера за доставка на софтуер.

4.2.3 Поддържа контролния списък с изискванията за сигурност на приложенията и критериите за валидиране.

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

9.1.1 оповестяване на критични уязвимости, засягащи широко използвани рамки или зависимости

9.1.2 актуализации на правните задължения, свързани със сигурността на приложенията (напр. NIS2, DORA)

9.1.3 съществени промени в практиките на организацията за разработка на софтуер, инструментариума или облачната архитектура

9.1.4 констатации от вътрешен одит или външни тестове за проникване

9.2 Прегледът трябва да се ръководи от Ръководителя „Сигурност на приложенията“ в координация с Директора по информационна сигурност (CISO), ръководителите на DevOps инженеринг, правния отдел, снабдяването и QA.

9.3 Всички редакции трябва да бъдат под управление на версиите в регистъра за контрол на документите на СУИС и да се разпространяват до всички засегнати екипи по разработка и продуктови екипи.

9.4 Заменените версии трябва да се архивират за не по-малко от три години с цел проследимост, възможност за одит и подпомагане на разследвания на инциденти по сигурността.

10. Свързани политики и връзки

10.1 P1 – Политика за информационна сигурност. Определя основата за защита на системите и данните, в рамките на която се изискват контроли на ниво приложение за предотвратяване на неоторизиран достъп, изтичане на данни и експлоатация.

10.2 P4 – Политика за контрол на достъпа. Определя стандартите за управление на идентичности и сесии, които трябва да се прилагат от всички приложения, включително силна автентикация, минимално необходим достъп и изисквания за преглед на достъпа.

10.3 P5 – Политика за управление на промените. Регламентира прехвърлянето на приложен код и конфигурации в продукционни среди, като гарантира, че неоторизирани, непланирани или непроверени промени се блокират.

10.4 P17 – Политика за защита на данните и поверителност. Изисква приложенията да прилагат поверителност още при проектиране и да осигуряват законосъобразно обработване, криптиране и срокове за съхранение на лични и чувствителни данни във всички среди.

10.5 P24 – Политика за сигурна разработка. Осигурява по-широката рамка за вграждане на сигурността в жизнения цикъл на разработка на системи, в рамките на която настоящата политика определя конкретните изисквания и технически контроли, които трябва да се прилагат на ниво приложение.

10.6 P30 – Политика за реагиране при инциденти. Изисква структурирано обработване на инциденти по сигурността на приложенията, включително уязвимости, идентифицирани след внедряване или по време на тестове за проникване, и определя процедурите за ескалация, ограничаване и възстановяване.

11. Референтни стандарти и рамки

11.1 ISO/IEC 27001:2022

11.1.1 Клауза 8.1 – Оперативно планиране и контрол: изисква сигурността на приложенията да бъде вградена в процесите и системите, за да се гарантират поверителност, цялост и наличност.

11.2 ISO/IEC 27002:2022

11.2.1 Контроли 8.25–8.26: определят очакванията за сигурност на ниво приложение, включително практики за сигурна разработка, моделиране на заплахи, архитектурни контроли и валидиране на софтуер от трети страни.

11.2.2 Контрол 8.25 от Приложение A – жизнен цикъл на сигурната разработка: изисква интегриране на сигурността през целия жизнен цикъл на приложението.

11.2.3 Контрол 8.26 от Приложение A – изисквания за сигурност на приложенията: налага определянето и прилагането на технически контроли за защита на приложенията срещу злоупотреба и компрометиране.

11.3 NIST SP 800-53 Rev.5

11.3.1 SA-11 – Тестване и оценка на сигурността от разработчика: изисква статично и динамично тестване, както и тестове за проникване по време на разработката.

11.3.2 SA-15 – Процес, стандарти и инструменти за разработка: установява формални стандарти за сигурна разработка на приложения.

11.3.3 SI-10 – Валидиране на входна информация: изисква контролни механизми за предотвратяване на атаки чрез инжектиране и грешки при обработката на входните данни.

11.4 GDPR на ЕС (2016/679)

11.4.1 Член 25 – Защита на данните още при проектиране и по подразбиране: изисква интегриране на защитата на данните и поверителността в логиката на приложенията и работните потоци.

11.4.2 Член 32 – Сигурност на обработването: изисква подходящи технически мерки, като валидиране на входа, криптиране и сигурни контроли за достъп.

11.5 Директива NIS2 на ЕС (2022/2555)

11.5.1 Член 21(2)(f): изисква обработване на уязвимости и практики за сигурен жизнен цикъл на приложенията за съществени и важни субекти.

11.5.2 Член 23 – Докладване на инциденти по сигурността: налага възможности за журналиране и мониторинг на ниво приложение за откриване и докладване на значими инциденти.

11.6 DORA на ЕС (2022/2554)

11.6.1 Член 9 – Управление на риска, свързан с ИКТ: задължава финансовите субекти да осигуряват, че приложенията са защитени, тествани и устойчиви на киберзаплахи.

11.6.2 Член 11 – Тестване на ИКТ инструменти: насърчава периодични тестове за проникване и red teaming на критични приложения и услуги.

11.7 COBIT 2019

11.7.1 BAI03 – Управление на идентифицирането и изграждането на решения: установява изисквания за проектиране и контрол по време на разработката на приложения.

11.7.2 BAI09 – Управление на приложенията: акцентира върху сигурната поддръжка, мониторинг и усъвършенстване на действащите приложения.

11.7.3 DSS05 – Управление на услугите по сигурност: свързва защитата на приложенията с по-широките операции и контроли по сигурността в организацията.