					Въведете тук наименованието на регистрираното юридическо лице							
Номер на документа: P24S					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**

Съгласуване със стандарти и регулации

Стандарт/регулация	Клауза/член	Коментар
ISO/IEC 27001:2022	Клауза 8	Приложими контроли за сигурност за оперативни дейности, включително сигурна разработка
ISO/IEC 27002:2022	Контроли 8.25–8.27	Обхваща жизнения цикъл на разработка на системи, тестването и отговорностите по сигурността на разработчици от трети страни
NIST SP 800-53 Rev.5	SA-3 – SA-15, SI-10	Обхваща сигурен жизнен цикъл на разработка на софтуер, контрол на достъпа и обработване на уязвимости при разработка
GDPR на ЕС	Член 25	Изисква защита на личните данни още при проектиране и защита на личните данни по подразбиране при разработката на софтуер
NIS2 на ЕС	Член 21(2)(a), (e), (h)	Изисква политики за сигурна разработка, надзор върху използването на софтуер с отворен код и документиране на мерките за смекчаване
DORA на ЕС	Членове 6(7), 9(1)(c), 10(2)(c)	Изисква сигурност през целия жизнен цикъл на критични ИКТ системи във финансовия сектор
COBIT 2019	BAI	Рамка за структурирано, проследимо и устойчиво управление на сигурната разработка

1. Цел

1.1 Настоящата политика гарантира, че всички софтуерни продукти, скриптове и уеббазирани инструменти, създадени или изменени от организацията или от нейни външни партньори, се разработват по сигурен начин, така че да се сведе до минимум рискът от уязвимости, неоторизиран достъп до данни или оперативни прекъсвания.

1.2 Тя определя задължителни правила за сигурна разработка и практики за програмиране, които всички вътрешни разработчици, външни изпълнители и доставчици са длъжни да спазват, независимо от размера или сложността на проекта.

1.3 Настоящата политика има за цел да защитава данните на клиентите, да предотвратява инциденти по сигурността и да гарантира, че софтуерът, създаден или персонализиран от или за организацията, може да преминава одити по сигурността, да отговаря на правните изисквания (напр. GDPR, NIS2, DORA) и да подпомага сертифицирането по ISO/IEC 27001.

2. Обхват

2.1 Настоящата политика се прилага за всички физически и юридически лица, участващи в разработването, персонализирането, внедряването или управлението на следното от името на организацията:

2.1.1 Уебсайтове, приложения или инструменти за автоматизация

2.1.2 Вътрешно разработени скриптове или софтуер

2.1.3 Код, разработен от външни разработчици или фрийлансъри

2.1.4 Плъгини, библиотеки и софтуерни компоненти, интегрирани в продукционни системи

2.2 Тя обхваща всички среди, използвани за дейности по разработка, включително:

2.2.1 Развойни и тестови среди

2.2.2 Среди за приемателно тестване и предпродукционни среди

2.2.3 Продукционни системи, използвани за изпълнение на разработен по поръчка код

2.3 Политиката урежда и обработването на данни по време на разработка и внедряване, по-специално всяко използване на продукционни данни в непроизводствена среда.

3. Цели

3.1 Да предотвратява въвеждането на слабости в сигурността или уязвимости в софтуер, разработен по поръчка или от трети страни.

3.2 Да гарантира, че практиките за сигурна разработка и предотвратяване на уязвимости са интегрирани във всеки етап от жизнения цикъл на разработка на софтуер.

3.3 Да намалява рисковете, свързани с използването на компоненти с отворен код или от трети страни, чрез задължителна надлежна проверка и проследимост.

3.4 Да изисква формален преглед на изходния код и тестване на сигурността на приложенията преди пускане в експлоатация.

3.5 Да контролира достъпа до развойните среди и да гарантира отделянето им от продукционните системи.

3.6 Да осигурява изпълнение на задължителните изисквания по международни стандарти и регулации (напр. ISO/IEC 27001, GDPR, DORA, NIS2).

4. Роли и отговорности

4.1 Управител

4.1.1 Одобрява настоящата политика и носи обща отговорност за нейното прилагане.

4.1.2 Осигурява съответствието на всички дейности по разработка на софтуер, независимо дали са вътрешни или възложени на външни изпълнители, с настоящата политика.

4.1.3 Преглежда и подписва договори за разработка или споразумения за услуги, които включват клаузи за сигурна разработка.

4.1.4 Проверява съответствието на доставчиците чрез регулярни прегледи или чрез изискване на доказателства за сигурност.

4.2 Вътрешен разработчик или собственик на приложение

4.2.1 Спазва практиките за сигурна разработка и внедряване.

4.2.2 Прилага контролния списък за сигурна разработка към всеки проект.

4.2.3 Валидира сигурността на всички използвани компоненти с отворен код или от трети страни.

4.2.4 Докладва незабавно на Управителя всички установени уязвимости.

[... 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 бъде преглеждана от Управителя най-малко веднъж годишно с цел:

9.1.1 Да се потвърди продължаващото съответствие с ISO/IEC 27001, GDPR, NIS2 и DORA

9.1.2 Да бъдат отразени актуализирани заплахи или промени в добрите практики за сигурна разработка

9.1.3 Да се осигури съвместимост с нови инструменти, платформи или отношения с доставчици

9.2 Междинни прегледи трябва да се извършват при:

9.2.1 Всеки докладван инцидент по сигурността на софтуер

9.2.2 Въвеждане на нова рамка за разработка или хостинг платформа

9.2.3 Промяна в партньорите за разработка от трети страни

9.2.4 Регулаторни актуализации, които засягат задълженията, свързани със софтуера или сигурността

9.3 Всички промени в настоящата политика трябва да бъдат:

9.3.1 Документирани с дата, обобщение на промяната и одобрение от Управителя

9.3.2 Ясно комуникирани до целия вътрешен и външен персонал, участващ в разработката

9.3.3 Съхранявани като част от управлението на версиите и историята на промените на политиките в организацията

9.4 Актуализираните версии трябва да бъдат лесно достъпни чрез вътрешни платформи, печатна документация или облачни услуги, достъпни за доставчиците.

10. Свързани политики и връзки

10.1 Настоящата политика подпомага и зависи от ефективното прилагане на няколко други SME политики:

10.1.1 P2S – Политика за роли и отговорности в управлението: Установява отчетност за възлагането и проверката на контролите за сигурност при разработка в различните проекти и при доставчиците.

10.1.2 P4S – Политика за контрол на достъпа: Осигурява базови правила за ограничаване на достъпа до развойни среди и хранилища за код, включително разделение на задълженията.

10.1.3 P8S – Политика за осведоменост и обучение по информационна сигурност: Гарантира, че вътрешните разработчици и външните изпълнители разбират практиките за сигурно програмиране и свързаните с тях отговорности по сигурността.

10.1.4 P17S – Политика за защита на данните и поверителност: Уточнява как личните данни трябва да бъдат обработвани по време на разработка, тестване и журнализиране, за да се поддържа съответствие с GDPR.

10.1.5 P30S – Политика за реагиране при инциденти: Определя как инциденти по сигурността, свързани с разработката, трябва да бъдат докладвани, оценявани и отстранявани, включително експозиции, свързани с кода.

10.2 Всички тези политики действат съвместно, за да гарантират, че сигурната разработка е изпълнима и подлежи на проверка, дори в малка или нетехническа организация.

11. Референтни стандарти и рамки

11.1 ISO/IEC 27001

11.1.1 Клауза 8.1 – Изисква внедряване на оперативни контроли, включително сигурна разработка, които са съгласувани с бизнес целите и рисковия профил.

11.2 ISO/IEC 27002

11.2.1 Контрол 8.25 – Препоръчва интегриране на сигурността през целия жизнен цикъл на софтуера, включително контрол на изходния код, управление на версиите и достъп на разработчиците.

11.2.2 Контрол 8.26 – Определя методи за тестване на приложения и проверка на функционалностите за сигурност преди въвеждане в експлоатация.

11.2.3 Контрол 8.27 – Изисква разработчиците от трети страни да спазват същите стандарти за разработка и техните отговорности по сигурността да бъдат ясно определени.

11.3 NIST SP 800-53 Rev.5

11.3.1 SA-3 до SA-15 – Определят процеси за сигурна разработка, включително контрол на достъпа на разработчиците, тестване, моделиране на заплахи и документация.

11.3.2 SI-10 – Изисква разработчиците да идентифицират и смекчават често срещани слабости в софтуера и да използват автоматизирани инструменти, когато е приложимо.

11.4 GDPR на ЕС (2016/679)

11.4.1 Член 25 – „Защита на данните още при проектиране и защита на данните по подразбиране“ изисква интегриране на мерки за сигурност и поверителност по време на проектирането и разработката на софтуер, особено когато се обработват лични данни.

11.5 Директива NIS2 на ЕС (2022/2555)

11.5.1 Член 21(2)(a), (e) и (h) – Изисква политики за сигурна разработка, надзор върху използването на софтуер с отворен код и документирано смекчаване на рисковете, свързани с приложенията, в съществени и важни субекти.

11.6 DORA на ЕС (2022/2554)

11.6.1 Членове 6(7), 9(1)(c) и 10(2)(c) – Налагат изисквания за сигурност през жизнения цикъл на разработка за субекти от финансовия сектор, включително SME, особено за критични ИКТ системи.

11.7 COBIT 2019

11.7.1 BAI03 – „Manage Solutions Identification and Build“ подпомага внедряването на структурирани контроли за разработка, които поставят акцент върху сигурността, проследимостта и устойчивостта, съобразени с ограниченията на SME.