					Въведете тук наименованието на регистрираното юридическо лице							
Номер на документа: P28					Заглавие на документа: **Политика за външно възложена 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 регулаторни изисквания

Стандарт/регулация	Клауза/член	Коментар
ISO/IEC 27001:2022	Клауза 8.1	Неприложимо
ISO/IEC 27002:2022	Контроли 5.19-5.22, 8.27	Неприложимо
NIST SP 800-53 Rev.5	SA-4, SA-9, SA-10	Неприложимо
GDPR на ЕС	Членове 28, 32	Неприложимо
NIS2 на ЕС	Членове 21(2)(a), (h), 23	Неприложимо
DORA на ЕС	Членове 28(1), (2)	Неприложимо
COBIT 2019	APO10, BAI03, DSS05	Неприложимо

1. Цел

1.1 Настоящата политика определя задължителните контроли при възлагане на разработката на софтуер или системи на външни доставчици, изпълнители или агенции, като гарантира прилагането на сигурни практики през целия жизнен цикъл на разработката.

1.2 Целта ѝ е да предотвратява уязвимости в сигурността, загуба на данни, разкриване на интелектуална собственост (IP) и нарушения на съответствието, произтичащи от дейности по външно възложена разработка.

1.3 Политиката установява изисквания за управление на доставчиците, стандарти за сигурна разработка, управление на достъпа, задължения за мониторинг и освобождаване при приключване на договора с цел поддържане на поверителността, целостта и наличността (CIA) на разработения софтуер.

2. Обхват

2.1 Настоящата политика се прилага за всички организационни звена, които ангажират външни страни за разработка на софтуер или системи, включително:

2.1.1 уеб приложения, мобилни приложения, вградени системи, приложно-програмни интерфейси (API), скриптове, автоматизирани работни потоци или модулни компоненти на платформи

2.1.2 разработка по поръчка за вътрешни платформи, системи с достъп от клиенти или търговски продукти

2.1.3 ангажименти с външни разработчици, фрийлансъри, агенции или офшорни екипи

2.2 Политиката урежда също всяка външна страна, която получава достъп до изходен код, тестови среди или CI/CD конвейери по време на разработката.

2.3 Изискванията са задължителни независимо от вида на договора, методологията на разработка или географското местоположение на външния изпълнител.

3. Цели

3.1 Да се прилагат практики за сигурен жизнен цикъл на разработката (SDLC) във всички ангажименти за външно възложена разработка — от планирането до валидацията след внедряване.

3.2 Да се гарантира, че всички договори с външни разработчици включват задължителни клаузи за защита на данните, сигурно програмиране и запазване на правата върху интелектуалната собственост.

3.3 Да се определят изискванията за контрол на достъпа, мониторинг и одит по отношение на външни разработчици, които взаимодействат с вътрешни системи.

3.4 Да се защитава организацията от заплахи по веригата на доставки, правни нарушения и репутационни щети, свързани със софтуер, разработен от външни страни.

3.5 Да се поддържа непрекъснато съответствие с рамки за сигурност, включително ISO/IEC 27001, NIST, GDPR, NIS2, DORA и COBIT 2019.

4. Роли и отговорности

4.1 Изпълнително ръководство

4.1.1 Одобрява проекти за външно възложена разработка с висок риск и утвърждава изключения от политиката, когато са обосновани.

4.1.2 Гарантира, че решенията за външно възлагане са съгласувани със стратегическите цели и апетита към риск на организацията.

4.2 Директор по информационна сигурност (CISO)

4.2.1 Одобрява въвеждането на доставчици от гледна точка на сигурността.

4.2.2 Определя изискванията към контролите за сигурност при ангажименти с външни страни и преглежда докладите за инциденти.

[... 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 най-малко веднъж годишно или по-често при следните обстоятелства:

9.1.1 въвеждане на нови модели за външно възлагане на разработка, нови доставчици или нови юрисдикции

9.1.2 актуализации на регулаторни рамки като GDPR, NIS2 или DORA

9.1.3 след инцидент по сигурността, свързан с външен код, достъп или резултати от изпълнението

9.1.4 като част от одитни констатации от вътрешен одит или подобрения на СУИС

9.2 Директорът по информационна сигурност (CISO) носи отговорност за иницииране и координиране на прегледа на политиката след консултация със:

9.2.1.1 правни въпроси и снабдяване (за съгласуваност при прилагането на договорните изисквания)

9.2.1.2 собственици на проекти и продукти (за оперативна приложимост)

9.2.1.3 информационна сигурност и управление на риска (за актуализации на заплахите и контролите)

9.2.1.4 изпълнително ръководство (за окончателно одобрение)

9.3 Всички актуализации на политиката трябва да бъдат:

9.3.1.1 под управление на версиите и съхранявани в определено хранилище за документи

9.3.1.2 комуникирани до заинтересованите страни, участващи в дейности по външна разработка

9.3.1.3 обвързани с всички актуализации в свързани политики или процедурна документация

9.4 Всеки вариант на политиката трябва да бъде придружен от журнал на промените, който осигурява проследимост на измененията и одобренията.

10. Свързани политики и връзки

10.1 Настоящата политика подпомага и се подпомага от следните свързани документи:

10.1.1 P1 - Политика за информационна сигурност: Установява принципите за сигурност на организационно ниво, приложими както при вътрешна разработка, така и при разработка от трети страни.

10.1.2 P5 - Политика за управление на промените: Гарантира, че всички промени, свързани с внедряване от външно разработени кодови бази, се преглеждат и одобряват преди внедряване.

10.1.3 P13 - Политика за класификация и етикетиране на данни: Определя как чувствителните данни се идентифицират, преди да бъдат предоставени на доставчици за разработка или хранилища.

10.1.4 P18 - Политика за криптографски контроли: Определя как трябва да се обработват ключове, тайни и чувствителни идентификационни данни по време на разработката и предоставянето.

10.1.5 P24 - Политика за сигурна разработка: Определя базовите изисквания за вътрешни и външни практики по разработка на софтуер.

10.1.6 P30 - Политика за реагиране при инциденти: Урегулира как нарушения или инциденти по сигурността, свързани с външна разработка, се ескалират, разследват и разрешават.

10.1.7 P33 - Политика за мониторинг на одита и съответствието: Определя изискванията за преглед на дейностите по външна разработка по време на одити или прегледи за съответствие.

11. Референтни стандарти и рамки

11.1 Настоящата политика е съгласувана с международно признати рамки и регулаторни изисквания за сигурност, за да осигури сигурно външно възлагане на разработката на софтуер и практики по управление на доставчици.

11.2 ISO/IEC 27001

11.2.1 Клауза 8.1 - Оперативно планиране и контрол: Налага процесни контроли за сигурна разработка и предоставяне от трети страни.

11.3 ISO/IEC 27002:2022 - Контроли 5.19 до 5.21, 8.27.

11.3.1 Приложение A, Контрол 5.19 - Управление на взаимоотношенията с доставчици: Изисква формални споразумения с клаузи за сигурност и съответствие.

11.3.2 Приложение A, Контрол 5.20 - Разглеждане на информационната сигурност в споразуменията с доставчици: Гарантира, че в договорите са включени специфични контроли за разработка.

11.3.3 Приложение A, Контрол 5.21 - Управление на предоставянето на услуги от доставчици: Включва наблюдение върху резултатите и рисковете при разработка от трети страни.

11.3.4 Приложение A, Контрол 8.27 - Външна разработка: Налага конкретни изисквания за сигурност и контрол на достъпа върху софтуер, разработван от външни страни.

11.3.5 Тези контроли определят структурирани изисквания за подбор, договаряне и надзор върху външни разработчици, включително практики за сигурна разработка, обработване на код и валидиране на резултатността.

11.4 NIST SP 800-53 Rev.5

11.4.1 SA-4 - Процес по придобиване: Изисква изискванията за сигурна разработка да бъдат определени към момента на придобиване.

11.4.2 SA-9 - Услуги на външни системи: Урегулира как външните разработчици взаимодействат сигурно с вътрешни услуги.

11.4.3 SA-10 - Управление на конфигурацията от разработчика: Съответства на задълженията за управление на версиите, достъп до кода и проследяване на промените за външни екипи.

11.5 GDPR на ЕС (2016/679)

11.5.1 Член 28 - Задължения на обработващия лични данни: Изисква договорите с външни разработчици да определят изискванията за сигурност, контрол и одит при обработване на лични данни.

11.5.2 Член 32 - Сигурност на обработването: Налага подходящи предпазни мерки (напр. криптиране, контрол на достъпа) при разработка на системи, които обработват лични данни.

11.6 Директива (ЕС) NIS2 (2022/2555)

11.6.1 Членове 21(2)(a), (h), 23: Изискват прилагането на практики за сигурна разработка във всички ангажименти с трети страни и цифрови вериги на доставки, с надзор и техническа проверка.

11.7 DORA на ЕС (2022/2554)

11.7.1 Членове 28(1), (2): Изискват финансовите субекти да управляват ИКТ риска от трети страни чрез договорни контроли и надзор върху сигурната разработка, особено при критична външно възложена разработка.

11.8 COBIT 2019

11.8.1 APO10 - Управление на доставчици: Установява структурирани изисквания за оценка на доставчици, договори и мониторинг на резултатността.

11.8.2 BAI03 - Управление на изграждането на решения: Пряко съответства на процесите по сигурен SDLC, прегледите на кода и валидацията на разработката.

11.8.3 DSS05 - Управление на услугите по сигурност: Съответства на мониторинга и защитата на системи, разработени външно или от трети страни.