					Въведете тук наименованието на регистрираното юридическо лице							
Номер на документа: P28S					Заглавие на документа: **Политика за външно възложена разработка - SME**							
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**

Съответствие със стандарти и нормативни изисквания

Стандарт/регулация	Клауза/член	Коментар
ISO/IEC 27001:2022	Клаузи 5.1, 6.1, 8	Приложими контроли на СУИС и контроли, свързани с доставчици
ISO/IEC 27002:2022	Контроли 5.19, 5.20, 8.25–8.27	Контроли за доставчици и за жизнения цикъл на разработката на системи
NIST SP 800-53 Rev.5	SA-4, SA-9, SA-11, SA-15, SR-3	Изисквания за придобиване, верига на доставки, сигурна разработка и споразумения с доставчици
GDPR на ЕС	Член 28	Договорни изисквания и изисквания за защита на данните при обработване от трети страни
NIS2 на ЕС	Член 21(2)(a), (h)	Контроли за сигурност на веригата на доставки и сигурна разработка на приложения
DORA на ЕС	Член 10	Управление на риска от трети страни в областта на ИКТ, включително външно възложена разработка
COBIT 2019	BAI03, DSS05	Изисквания към външната разработка и външните доставчици на ИТ услуги

1. Цел

1.1 Настоящата политика гарантира, че всяка външно възложена разработка на софтуер — независимо дали се извършва от фрийлансъри, агенции или доставчици трети страни — се осъществява сигурно, при договорен контрол и в съответствие с приложимите правни, регулаторни и одитни изисквания.

1.2 Тя защитава организацията от рискове, свързани с несигурен код, неясна собственост, излагане на данни и неефективно управление на доставчици, чрез въвеждане на приложими стандарти за разработка и надзор над доставчиците, включително когато няма собствен ИТ екип.

1.3 Настоящата политика подпомага сертифицирането по ISO/IEC 27001:2022, като ясно определя изискванията към разработката, отчетността и документираните мерки за дейностите по разработка, извършвани от трети страни.

2. Обхват

2.1 Настоящата политика се прилага за:

2.1.1 Всички външни разработчици, включително фрийлансъри и агенции за разработка

2.1.2 Всяка дейност по разработка, свързана с вътрешни инструменти, публично достъпни уебсайтове, софтуерни приложения или автоматизация на бизнес процеси

2.1.3 Служители, отговорни за избора, управлението или надзора на външни разработчици

2.1.4 Всяка системна интеграция, скриптиране или разработка от трета страна, която взаимодейства с фирмени данни или системи

2.2 Политиката обхваща също всяка страна или платформа с достъп до фирмени идентификационни данни, хранилища на данни, хранилища за изходен код, среди за тестване или продукционни системи.

3. Цели

3.1 Да гарантира, че цялата външно възложена разработка спазва принципите на сигурната разработка и че разработчиците са договорно задължени да следват документирани стандарти и клаузи за поверителност.

3.2 Да установи собственост върху всички резултати от проекта — код, активи, идентификационни данни и документация — като гарантира пълно прехвърляне на правата към дружеството и проследимо предаване при приключване на проекта.

3.3 Да предотвратява често срещани рискове при разработката, включително повторно използване на собственически код, атаки по веригата на доставки чрез библиотеки, използване на неподдържани рамки и непроверен административен достъп.

3.4 Да изисква документация преди започване на работа за всеки външно възложен проект, включително договори, споразумения за поверителност и минимални изисквания за сигурност.

3.5 Да защитава клиентските данни, системите и вътрешните процеси чрез ефективен надзор върху разработката, тестване след предаване и сигурно управление на системния достъп.

4. Роли и отговорности

4.1 Управител

4.1.1 Одобрява всички взаимоотношения с доставчици и подписва споразуменията за разработка.

4.1.2 Гарантира, че цялата външно възложена разработка се извършва в съответствие с настоящата политика.

4.1.3 Отнема достъпа до фирмените системи след приключване на проекта.

4.1.4 Преглежда документацията и резултатите след предаването.

4.2 Собственик на проекта (обикновено вътрешен служител или определен координатор)

4.2.1 Управлява ежедневната координация с външния разработчик.

4.2.2 Проверява дали функционалните изисквания са изпълнени и резултатите са тествани.

4.2.3 Гарантира сигурното предаване на код и идентификационни данни.

4.2.4 Докладва на Управителя всички проблеми или инциденти, свързани с разработката.

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

9. Изисквания за преглед и актуализация

9.1 Годишен преглед

9.1.1 Настоящата политика трябва да се преглежда от Управителя най-малко веднъж годишно. Прегледът гарантира, че тя продължава да отговаря на:

9.1.1.1 Изискванията за сертифициране по ISO/IEC 27001

9.1.1.2 Промените в правните задължения (напр. член 28 от GDPR, член 10 от DORA)

9.1.1.3 Актуалните практики за разработка на ниво МСП и рисковете от трети страни

9.2 Междинни прегледи

9.2.1 Прегледи на политиката трябва да се извършват също когато:

9.2.1.1 Се въвежда нов доставчик или платформа за външна разработка

9.2.1.2 Настъпи значим инцидент, свързан с външно възложена разработка

9.2.1.3 Има съществени промени в използваните инструменти, платформи или среди

9.3 Процес на преглед

9.3.1 Управителят отговаря за:

9.3.1.1 Проверка, че договорите, споразуменията за поверителност и процесите за контрол на достъпа остават ефективни

9.3.1.2 Потвърждение, че текущите доставчици и фрийлансъри са приведени в съответствие с политиката

9.3.1.3 Актуализиране на условията въз основа на обратна връзка от предходни проекти или инциденти

9.4 Управление на версиите и комуникация

9.4.1 Всички промени трябва да бъдат:

9.4.1.1 Документирани с дата, причина и описание на промяната

9.4.1.2 Одобрени от Управителя и добавени към историята на версиите

9.4.1.3 Комуникирани до всички служители или собственици на проекти, работещи с външни разработчици

9.4.1.4 Повторно разпространени до всички засегнати доставчици и трети страни, когато е необходимо

10. Свързани политики и връзки

10.1 Настоящата политика пряко подпомага и зависи от прилагането на следните политики, съобразени с МСП:

10.1.1 P2S – Политика за роли и отговорности в управлението: Уточнява кой носи отговорност за одобряването на доставчици, контрола на достъпа и приемането на риска при използване на външни разработчици.

10.1.2 P4S – Политика за контрол на достъпа: Определя правилното създаване, ограничаване и прекратяване на потребителски акаунти и административен достъп, използвани при външно възложена разработка.

10.1.3 P8S – Политика за информираност и обучение по информационна сигурност: Гарантира, че вътрешният персонал разбира как да координира сигурно работата с външни разработчици, включително обработването на идентификационни данни и проектни файлове.

10.1.4 P17S – Политика за защита на данните и поверителност: Установява изискванията за сигурност и правните изисквания при обработване на лични данни, които могат да бъдат обработвани от външни разработчици съгласно GDPR.

10.1.5 P24S – Политика за сигурна разработка: Определя как вътрешната и външната разработка трябва да следва практики за сигурно програмиране и проверка на библиотеки и рамки.

10.1.6 P30S – Политика за реагиране при инциденти: Прилага се, когато външно възложената разработка води до инциденти по сигурността или уязвимости, като насочва координираното разследване и действията по отстраняване.

10.2 Тези политики трябва да се прилагат паралелно, за да се гарантира, че външно възложената разработка не създава неуправляем риск и не води до нарушение на задълженията за съответствие на МСП.

11. Референтни стандарти и рамки

11.1 ISO/IEC 27001

11.1.1 Клауза 6.1 – Организациите трябва да оценяват и третират рисковете за информационната сигурност, свързани с доставчиците.

11.1.2 Клауза 8.1 – Изисква оперативно планиране и контрол, включително за услуги от трети страни, като външно възложена разработка.

11.2 ISO/IEC 27002

11.2.1 Контрол 5.19 – Препоръчва оценяване на способността на доставчиците да изпълняват изискванията за информационна сигурност.

11.2.2 Контрол 5.20 – Насърчава редовно наблюдение и периодичен преглед на услугите от трети страни.

11.2.3 Контроли 8.25–8.27 – Определят практики за жизнения цикъл на разработката на системи, приложими към външно възложена разработка.

11.3 NIST SP 800-53 Rev.5

11.3.1 SA-4 – Изисква стратегиите за придобиване да включват мерки за информационна сигурност.

11.3.2 SA-9 – Разглежда външната разработка на системи и рисковете по веригата на доставки.

11.3.3 SA-11 – Определя практики за сигурна разработка, включително преглед на кода и отстраняване на дефекти.

11.3.4 SA-15 – Насърчава използването на автоматизирани инструменти за откриване на дефекти и осигуряване на софтуера.

11.3.5 SR-3 – Изисква споразуменията с доставчици да включват изисквания за киберсигурност.

11.4 Общ регламент относно защитата на данните на ЕС (GDPR)

11.4.1 Член 28 – Изисква договорите с трети страни, обработващи лични данни, да осигуряват подходящи предпазни мерки за защита на данните, което е пряко приложимо към разработчици, които обработват или имат достъп до лични данни.

11.5 Директива NIS2 на ЕС (2022/2555)

11.5.1 Член 21(2)(a), (h) – Изисква контроли за сигурност на веригата на доставки и практики за сигурна разработка на софтуер за доставчици на цифрови услуги в обхвата, включително МСП, когато е приложимо.

11.6 Регламент на ЕС за цифрова оперативна устойчивост (DORA)

11.6.1 Член 10 – Изисква управление на риска от трети страни в областта на ИКТ, включително споразумения за разработка, задължения за сигурност и контроли на риска, свързани с доставчици трети страни.

11.7 COBIT 2019

11.7.1 BAI03 – Управление на идентифицирането и изграждането на решения – гарантира, че външната разработка отговаря на бизнес изискванията и очакванията за сигурност.

11.7.2 DSS05 – Управление на услугите по сигурност – изисква външните услуги по сигурност и доставчиците на услуги по разработка да работят при прилагани правила за сигурност и надзор.