					Въведете тук наименованието на регистрираното юридическо лице							
Номер на документа: P25S					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 регулаторни изисквания

Стандарт/регулация	**Клауза/член**	**Коментар**
ISO/IEC 27001:2022	Клауза 8	Оперативни контроли, включително сигурност на приложенията
ISO/IEC 27002:2022	Контроли 8.25–8.26	Сигурно проектиране, разработване, тестване и преглед на изходния код
NIST SP 800-53 Rev.5	SA-11, SI-10	Тестване от разработчиците/на приложенията, анализ на кода, предотвратяване на дефекти
GDPR на ЕС	Член 25	Защита на данните още при проектиране и по подразбиране
NIS2 на ЕС	Член 21(2)(a), (e)	Технически мерки за защита на приложенията и откриване на рискове
DORA на ЕС	Членове 9(2)(c), 10(2)(c)	Сигурност на приложенията за цифрова оперативна устойчивост
COBIT 2019	BAI03	Управление на сигурното разработване/придобиване на софтуер

1. Цел

1.1 Настоящата политика определя минималните задължителни контроли за сигурност на приложенията, приложими за всички софтуерни и системни решения, използвани от организацията, независимо дали са разработени вътрешно или са придобити от външни доставчици.

1.2 Тя гарантира, че приложенията се проектират, внедряват и поддържат по начин, който защитава данните на клиенти, служители и служебната информация от неоторизиран достъп, неправомерно използване, изменение или унищожаване.

1.3 Настоящата политика подпомага усилията на организацията за постигане и поддържане на сертификация по ISO/IEC 27001, изпълнение на задълженията по GDPR и NIS2 и намаляване на оперативните рискове, свързани с несигурно внедряване на софтуер.

1.4 Тя допринася за установяването на последователен и подлежащ на одит подход към сигурността на приложенията в МСП чрез въвеждане на единен контролен списък с функционалности и практики за сигурност, адаптиран за среди с ограничени вътрешни технически ресурси.

2. Обхват

2.1 Настоящата политика се прилага за всички приложения, системи, инструменти и платформи, които:

2.1.1 са разработени вътрешно, персонализирани или създадени чрез скриптове за вътрешна употреба

2.1.2 са придобити като търговски софтуер, SaaS или облачно базирани системи

2.1.3 обработват, съхраняват или пренасят лични данни, служебни записи или чувствителна оперативна информация

2.1.4 са достъпни за служители, външни изпълнители, клиенти или партньори чрез вътрешни мрежи, интернет или мобилни платформи

2.2 Политиката обхваща:

2.2.1 разработчици (вътрешни или външни)

2.2.2 доставчици на софтуер и доставчици на облачни услуги

2.2.3 персонал по ИТ поддръжка или администратори, отговорни за внедряване и поддръжка

2.2.4 собственици на приложения и бизнес потребители, участващи в одобряването и надзора върху системите

3. Цели

3.1 Да се гарантира, че всички приложения, използвани от организацията, разполагат с вградени и проверими контроли за сигурност, които ограничават често срещани софтуерни уязвимости.

3.2 Да се защитят поверителността, целостта и наличността на данните, обработвани от приложенията, независимо от мястото на тяхното хостване.

3.3 Да се изискват формално тестване, преглед и валидиране на сигурността на приложенията, преди което и да е ново приложение или съществена актуализация да бъдат одобрени за използване в продукционна среда.

3.4 Да се осигури последователно и сигурно обработване на идентификационни данни на потребителите, данни за сесии и права за достъп във всички системи от критично значение за бизнеса.

3.5 Да се изискват сигурно регистриране на събития, възможности за одит и функции за мониторинг във всички приложения в подкрепа на откриването и реагирането при подозрителна дейност.

3.6 Да се намалят правните рискове и рисковете по съответствие чрез гарантиране, че приложенията отговарят на приложимите регулаторни изисквания за сигурност.

4. Роли и отговорности

4.1 Управител (GM)

4.1.1 Носи цялостната отговорност за сигурността на приложенията в рамките на организацията.

4.1.2 Одобрява настоящата политика и гарантира, че всички дейности по придобиване или разработване са в съответствие с нея.

4.1.3 Гарантира, че доставчиците и външните доставчици на услуги са договорно обвързани с изискванията за сигурност на приложенията.

4.1.4 Преглежда и одобрява изключенията, основани на риска, когато пълно съответствие не може да бъде постигнато поради бизнес ограничения.

4.2 Собственик на приложение (ако е определен)

4.2.1 Идентифицира специфичните за приложението изисквания за сигурност при избор на система или стартиране на проект.

4.2.2 Проверява дали са включени ключови функционалности като защита на вписването, криптиране и регистри на дейностите.

4.2.3 Участва в прегледите преди внедряване и потвърждава, че контролите за сигурност отговарят на бизнес потребностите.

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

9. Изисквания за преглед и актуализиране

9.1 Настоящата политика трябва да бъде преглеждана от Управителя най-малко веднъж през всяка календарна година, за да:

9.1.1 отразява промени в регулаторните изисквания (напр. GDPR, NIS2, DORA)

9.1.2 включва нови или възникващи заплахи и техники за атака

9.1.3 актуализира формулировките и изискванията с оглед на промени в платформите, доставчиците или методите за разработване

9.2 Междинни прегледи трябва да се извършват и когато:

9.2.1 се въвеждат нови приложения

9.2.2 съществуващи приложения преминават през съществени актуализации или интеграция

9.2.3 възникне инцидент или нарушение, свързани с приложение

9.2.4 бъдат идентифицирани нови рискове от външни предупреждения или уведомления от индустрията

9.3 Всички актуализации на настоящата политика трябва да бъдат:

9.3.1 одобрени от Управителя

9.3.2 документирани с история на версиите и причина за промяната

9.3.3 комуникирани до всички служители, разработчици и доставчици, участващи в управлението на приложенията

9.3.4 съхранявани по сигурен начин за целите на одита и съответствието

10. Свързани политики и връзки

10.1 Настоящата политика е пряко подкрепена от следните политики за сигурност, съгласувани с нуждите на МСП, и допринася за тяхното прилагане:

10.1.1 P2S – Политика за роли и отговорности в управлението: Определя отговорностите за одобряване на приложения, прилагане на политиката и управление на доставчици.

10.1.2 P4S – Политика за контрол на достъпа: Гарантира, че достъпът до приложения е съобразен с принципа на минимално необходимия достъп и контрола на сесиите.

10.1.3 P8S – Политика за информираност и обучение по информационна сигурност: Гарантира, че потребителите и разработчиците са обучени да разпознават и докладват заплахи, свързани с приложения.

10.1.4 P17S – Политика за защита на данните и поверителност: Осигурява мерките за защита на поверителността на данните, които трябва да се прилагат от всяко приложение, обработващо лична информация.

10.1.5 P14S – Политика за съхранение на данни и унищожаване: Регламентира как регистрите, резервните копия и чувствителните данни, генерирани от приложенията, трябва да се съхраняват, архивират и унищожават по сигурен начин.

10.1.6 P30S – Политика за реагиране при инциденти: Определя стъпките за идентифициране, докладване и ограничаване на събития по сигурността, свързани с приложения.

10.2 Заедно тези политики гарантират, че сигурността на приложенията е напълно интегрирана в Системата за управление на информационната сигурност (СУИС) на организацията и подлежи на одит.

11. Референтни стандарти и рамки

11.1 ISO/IEC 27001

11.1.1 Клауза 8.1 – Изисква организациите да установят оперативни контроли за адресиране на рисковете за информационната сигурност, включително рисковете, свързани с приложения и софтуерни системи.

11.2 ISO/IEC 27002

11.2.1 Контрол 8.25 – Препоръчва прилагането на практики за сигурно проектиране, разработване и преглед на изходния код за всички приложения, включително предоставените от доставчици.

11.2.2 Контрол 8.26 – Препоръчва формално тестване на контролите за сигурност на приложенията, особено в области, свързани с контрол на достъпа, валидиране на входните данни и управление на сесиите.

11.3 NIST SP 800-53 Rev.5

11.3.1 SA-11 – Определя изисквания за тестване от разработчиците, анализ на кода и динамично сканиране на приложения преди внедряване.

11.3.2 SI-10 – Обхваща откриването и предотвратяването на често срещани софтуерни дефекти, с акцент върху осведомеността на разработчиците и техническите предпазни мерки.

11.4 GDPR на ЕС (2016/679)

11.4.1 Член 25 – „Защита на данните още при проектиране и по подразбиране“ изисква поверителността и сигурността да бъдат вградени в основния дизайн на приложенията, обработващи лични данни.

11.5 Директива NIS2 на ЕС (2022/2555)

11.5.1 Член 21(2)(a) и (e) – Изисква съществените и важните субекти да прилагат технически мерки за защита на приложенията и откриване на рискове, свързани със софтуера.

11.6 DORA на ЕС (2022/2554)

11.6.1 Членове 9(2)(c), 10(2)(c) – Изисква МСП във финансовия сектор да внедряват контроли за сигурност на ниво приложение и да извършват редовни оценки за поддържане на цифровата оперативна устойчивост.

11.7 COBIT 2019

11.7.1 BAI03 – „Управление на идентифицирането и разработването на решения“ насочва разработването или придобиването на сигурен софтуер, съобразен с риска, съответствието и бизнес изискванията, включително в среди на МСП с ограничени ресурси.