					Въведете тук наименованието на регистрираното юридическо лице							
Номер на документа: P19S					Заглавие на документа: **Политика за управление на уязвимостите и корекциите**							
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 с приложимите стандарти и регулации

Стандарт/регулация	Клауза/член	Коментар
ISO/IEC 27001:2022	Clause 8	
ISO/IEC 27002:2022	Controls 8.8, 8.9	
NIST SP 800-53 Rev.5	RA-5, SI-2, CM-2	
EU NIS2	Articles 21(2)(d), 21(2)(e)	
EU DORA	Articles 8(1), 10(2)	
COBIT 2019	DSS05.02, APO12	
EU GDPR	Article 32(1)(b)	

1. Цел

1.1 Настоящата политика определя начина, по който организацията идентифицира, оценява и смекчава уязвимости в системи, приложения и инфраструктура.

1.2 Целта ѝ е да намали киберриска чрез своевременно прилагане на корекции и отстраняване, основано на риска, съобразено с нуждите на малките и средните предприятия (SME).

1.3 Настоящата политика подпомага съответствието с ISO/IEC 27001:2022 и изпълнението на регулаторните задължения по GDPR, NIS2 и DORA, като изисква проактивно управление на техническите уязвимости.

1.4 Организацията приема, че системите без приложени корекции представляват съществен риск за информационната сигурност и трябва да се управляват систематично и без неоправдано забавяне.

2. Обхват

2.1 Настоящата политика се прилага за:

2.1.1 Всички сървъри, настолни компютри, преносими компютри, мобилни устройства, мрежово оборудване и облачно хоствани платформи, използвани от организацията

2.1.2 Всички операционни системи, софтуер от трети страни, приставки и приложения, използвани в дейността на организацията

2.1.3 Вътрешния ИТ персонал и външните доставчици на услуги, отговорни за поддръжката, актуализациите или наблюдението на системи

2.1.4 Всеки разработен по поръчка код или вграден софтуер, поддържан от организацията или от нейно име

2.2 Политиката обхваща както инфраструктурата, управлявана пряко от организацията, така и системите, администрирани от договорни доставчици или хостинг доставчици.

3. Цели

3.1 Да се идентифицират и оценяват своевременно и последователно известните уязвимости във всички ИТ активи

3.2 Да се прилагат корекции по сигурността и софтуерни актуализации съобразно тежестта и риска за дейността на организацията или за личните данни

3.3 Да се предотвратява експлоатирането на технически слабости, които могат да доведат до прекъсване на услуги, нарушение на сигурността на данните или регулаторно несъответствие

3.4 Да се поддържат точни записи за приложените корекции, неотстранените проблеми и изключенията, с цел осигуряване на готовност за одит

3.5 Да се използват инструменти и процеси, съобразени с размера на организацията и оперативната ѝ сложност, без компромис с ефективността

3.6 Да се подпомага правното и регулаторното съответствие, включително с член 32 от GDPR и контролите от Annex A на ISO

4. Роли и отговорности

4.1 Управител

4.1.1 Носи цялостна отговорност за осигуряване на изпълнението на дейностите по управление на уязвимостите и корекциите

4.1.2 Одобрява изключения, основани на риска, когато корекции не могат да бъдат приложени, и преглежда свързаните мерки за смекчаване

4.1.3 Преглежда отчетите за състоянието на корекциите и осигурява необходимите ресурси за изпълнение на задълженията по прилагане на корекции

4.2 Доставчик на ИТ поддръжка / Вътрешен ИТ администратор

4.2.1 Наблюдава системите за уязвимости и налични корекции чрез известия от доставчици, бюлетини за заплахи и уведомления на ниво операционна система

4.2.2 Прилага актуализации на операционни системи, фърмуер и приложения в рамките на определените срокове

4.2.3 Поддържа формален журнал на корекциите и документира неотстранените или отложените актуализации

4.2.4 Извършва тестване и планиране на критични актуализации с цел минимизиране на оперативните прекъсвания

[... 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 най-малко веднъж годишно от Управителя, с участието на Доставчика на ИТ услуги и Координатора по защита на данните

9.2 Основания за преглед

9.2.1 Междинни прегледи трябва да се извършват, ако:

9.2.1.1 Съществена уязвимост или експлойт засяга системи в обхвата

9.2.1.2 Настъпят съществени промени в системите или софтуера

9.2.1.3 Одит установи пропуски в процесите по управление на корекциите

9.2.1.4 Бъде регистриран инцидент или нарушение, свързани с корекции

9.3 Управление на версиите на политиката

9.3.1 Всички актуализации трябва да бъдат отразени в регистър на версиите с обобщение на промените

9.3.2 Промените трябва да бъдат съобщавани на засегнатия персонал

9.3.3 Неактуалните версии трябва да бъдат архивирани с ограничен достъп

10. Свързани политики и връзки

10.1 Настоящата политика подпомага и е свързана с няколко други политики за SME:

10.1.1 P12S – Политика за управление на активите: Определя собствеността и класификацията на системите, като гарантира, че всички активи, за които се изисква прилагане на корекции, са отчетени и включени в инвентара

10.1.2 P14S – Политика за съхранение и унищожаване на данни: Гарантира, че системите, планирани за извеждане от употреба, се актуализират по сигурен начин или се изтриват, като по този начин се намалява експозицията към уязвимости

10.1.3 P17S – Политика за защита на данните и поверителност: Приоритизира отстраняването на уязвимости за системи, обработващи лични данни, с цел съответствие със законодателството в областта на защитата на данните

10.1.4 P22S – Политика за регистриране и мониторинг: Подпомага откриването на системи без приложени корекции или на подозрително поведение, което може да е признак за експлоатиране на уязвимост

10.1.5 P30S – Политика за реагиране при инциденти: Определя процедурите за реагиране при уязвимости, водещи до инциденти по сигурността, включително стъпки за ескалация и докладване

11. Референтни стандарти и рамки

11.1 ISO/IEC 27001

11.1.1 Клауза 8.1 – Изисква внедряване на контроли за третиране на оперативния риск, включително управление на уязвимостите

11.2 ISO/IEC 27002

11.2.1 Контрол 8.8 – Определя процеси за сканиране и отстраняване на известни слабости в системите

11.2.2 Контрол 8.9 – Подчертава сигурната конфигурация, валидирането на корекциите и управлението на промените с цел избягване на нови експозиции по време на актуализации

11.3 NIST SP 800-53 Rev.5

11.3.1 RA-5 – Изисква идентифициране на уязвимости и отстраняването им в рамките на определени срокове

11.3.2 SI-2 – Изисква своевременно прилагане на корекции и актуализации според тежестта

11.3.3 CM-2 – Регламентира базовите конфигурации на системите и документирането на актуализациите, за да се осигури последователна защита

11.4 EU GDPR

11.4.1 Член 32(1)(b) – Изисква организациите да внедрят подходящи технически мерки, включително прилагане на корекции, за поддържане на сигурността на обработването

11.5 Директива EU NIS2

11.5.1 Член 21(2)(d) – Изисква третиране на уязвимостите чрез систематично сканиране и отстраняване

11.5.2 Член 21(2)(e) – Изисква сигурна конфигурация и управление на корекциите с цел осигуряване на устойчивост на ИКТ

11.6 EU DORA

11.6.1 Член 8(1) – Изисква откриване и смекчаване на ИКТ рискове, включително технически уязвимости

11.6.2 Член 10(2) – Изисква финансовите субекти да отстраняват слабости, засягащи ИКТ системите и операциите

11.7 COBIT 2019

11.7.1 DSS05.02 – Изисква третиране на известни технически уязвимости с цел поддържане на защитени операции

11.7.2 APO12.01 – Съгласува управлението на риска с проактивния мониторинг и коригирането на системни слабости