					Въведете тук наименованието на регистрираното юридическо лице							
Номер на документа: P19					Заглавие на документа: **Политика за управление на уязвимости и корекции**							
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**

Съгласувана с приложимите стандарти и регулации

Стандарт/регулация	Клауза/член	Коментар
ISO/IEC 27001:2022	Clause 8	Систематично третиране на техническите уязвимости; постоянна ефективност на контролите за сигурност.
ISO/IEC 27002:2022	Controls 8.8, 8.9, 5	Насоки за внедряване относно прилагането на корекции, сканирането за уязвимости, цялостта на софтуера, сигурната конфигурация и инвентаризацията на активите.
NIST SP 800-53 Rev.5	RA-5, SI-2, CM-2, CM-6	Изисква често сканиране, отстраняване на дефекти и управление на конфигурацията.
EU GDPR	Article 32, Recital 49	Технически мерки за своевременно прилагане на корекции, третиране на уязвимости и непрекъсната сигурност.
EU NIS2	Article 21(2)(d)	Откриване, реагиране и смекчаване на уязвимости за поддържане на високо ниво на киберхигиена.
EU DORA	Articles 8, 10(2)(f)	Своевременно отстраняване на ИКТ уязвимости; непрекъснати оценки, водени от заплахите.
COBIT 2019	DSS05.02, DSS01.03, MEA	Сканиране, проследяване и смекчаване на технически слабости; мониторинг за експлоатиране; одит на ефективността, включително статуса на корекциите.

1. Цел

1.1 Настоящата политика определя задължителните изисквания на организацията за идентифициране, класифициране, отстраняване и мониторинг на технически уязвимости и софтуерни дефекти във всички информационни системи и активи в обхвата на Системата за управление на информационната сигурност (СУИС).

1.2 Политиката гарантира, че всички известни уязвимости се оценяват и адресират своевременно и въз основа на риска чрез координирано прилагане на корекции, промени в конфигурацията или компенсиращи контроли, в съответствие със служебната необходимост и задълженията, определени в политиките.

1.3 Настоящата политика подпомага съответствието с ISO/IEC 27001, Приложение A, Контрол 8.8 и насоките на ISO/IEC 27002, както и адресира регулаторните изисквания по DORA член 8, NIS2 член 21, GDPR член 32 и домейните DSS и APO на COBIT 2019.

2. Обхват

2.1 Настоящата политика се прилага за всички информационни системи, активи и среди, които съхраняват, обработват или предават данни под управлението на СУИС, включително:

2.1.1 Операционни системи, приложения, мрежови устройства, фърмуер, облачни платформи, приложно-програмни интерфейси (API) и софтуер на трети страни.

2.1.2 Системи в среди за разработка, тестови среди, продукционни среди, резервни среди и среда за аварийно възстановяване.

2.1.3 Крайни точки, сървъри, IoT устройства, виртуализирана инфраструктура и контейнери.

2.2 Политиката е задължителна за:

2.2.1 Вътрешен персонал: ИТ администратори, системни инженери, разработчици на приложения, анализатори по сигурността и инфраструктурни екипи.

2.2.2 Външни страни: външни изпълнители и доставчици на услуги от трети страни, доставчици на управлявани услуги (MSP), доставчици на софтуер и системни интегратори с технически отговорности за активи в обхвата.

2.3 Политиката обхваща пълния жизнен цикъл на управлението на уязвимости и корекции, включително:

2.3.1 Сканиране и откриване

2.3.2 Класифициране на риска и приоритизиране

2.3.3 Получаване, тестване, внедряване и връщане назад на корекции

2.3.4 Обработване на изключения и планиране на компенсиращи контроли

2.3.5 Водене на журнали, докладване и проследимост за целите на одита

3. Цели

3.1 Да гарантира, че всички известни уязвимости се идентифицират, оценяват и отстраняват по начин, който свежда до минимум експозицията на риск и е съобразен с оперативните приоритети.

3.2 Да установи последователни процеси в цялата организация за сканиране за уязвимости, класификация по тежест (напр. CVSS) и управление на корекциите, включително аварийна обработка и планиране на връщане към предходно състояние.

3.3 Да осигури управление на сигурната конфигурация чрез съответствие с базовите конфигурации, практиките за управление на промените и разузнаването за заплахи в реално време.

3.4 Да осигури измеримо съответствие с регулаторните изисквания и контролите, основани на стандарти, свързани с цялостта на системите, хигиената на корекциите и своевременното отстраняване на дефекти.

3.5 Да определи отговорности и отчетност по роли за целия жизнен цикъл на управлението на уязвимости, така че всички заинтересовани страни да действат в рамките на определените SLA и подлежащите на докладване контролни показатели.

3.6 Да подпомогне готовността за одит и да подобри устойчивостта срещу възникващи заплахи, включително zero-day уязвимости, активни вериги за експлоатиране и публично значими уведомления от доставчици.

4. Роли и отговорности

4.1 Директор по информационна сигурност (CISO)

4.1.1 Отговаря за политиката и осигурява нейното интегриране в СУИС.

4.1.2 Определя рисковия профил на организацията и осигурява съответствие с регулаторните изисквания и очакванията към контролите.

4.2 Ръководител по управление на уязвимостите / Ръководител на Центъра за операции по сигурността (SOC)

4.2.1 Осъществява надзор върху цялостните дейности по управление на уязвимости и корекции.

4.2.2 Координира графиците за сканиране, моделите за приоритизиране и сроковете за отстраняване.

4.2.3 Поддържа Регистъра на уязвимостите и съдейства при оценката на компенсиращите контроли.

[... 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 се преглежда най-малко веднъж годишно или при:

9.1.1 Съществени регулаторни актуализации (напр. промени в DORA, NIS2)

9.1.2 Промени в рамките за приоритизиране на уязвимости (напр. актуализации на CVSS)

9.1.3 Съществени промени в ИТ средата (напр. миграция към облак, мащабна промяна на EDR)

9.1.4 Публично значими нарушения на сигурността или външни уведомления, изискващи засилване на политиката

9.2 Прегледите се извършват от директора по информационна сигурност (CISO) в сътрудничество с екипите по операции по сигурността, управление на риска и ръководството на инфраструктурата.

9.3 Актуализациите на политиката трябва да бъдат:

9.3.1 Документирани в Регистъра на документите на СУИС

9.3.2 Прегледани и одобрени от изпълнителното ръководство

9.3.3 Комуникирани до всички засегнати заинтересовани страни, включително обработващи лични данни от трети страни

9.4 Историческите версии се съхраняват по сигурен начин за целите на одита и отчетността.

10. Свързани политики и връзки

10.1 P1 - Политика за информационна сигурност. Определя общия ангажимент за защита на системите и данните, включително проактивно управление на уязвимости и осигуряване на цялостта на софтуера.

10.2 P5 - Политика за управление на промените. Регламентира всяко внедряване на корекции и промени в конфигурацията, като изисква документиране, тестване, одобрение и процедури за връщане назад, които допълват процесите по отстраняване на уязвимости.

10.3 P6 - Политика за управление на риска. Подпомага класифицирането и третирането на неотстранени уязвимости чрез структурирани оценки на риска, анализ на въздействието и процедури за приемане на остатъчния риск.

10.4 P12 - Политика за управление на активите. Гарантира, че системите са инвентаризирани и класифицирани коректно, което позволява последователно сканиране за уязвимости, определяне на собствеността и покритие с корекции през целия жизнен цикъл.

10.5 P22 - Политика за регистриране и мониторинг. Определя изискванията за откриване на събития и създаване на одитна следа. Настоящата политика подпомага видимостта върху дейностите по прилагане на корекции, неоторизирани промени и опити за експлоатиране, насочени към известни уязвимости.

10.6 P30 - Политика за реагиране при инциденти. Определя протоколите за ескалация и стратегиите за ограничаване при експлоатирани уязвимости, разследвания на нарушения на сигурността и коригиращи действия, съгласувани с контролите по настоящата политика.

11. Референтни стандарти и рамки

11.1 ISO/IEC 27001: Clause 8.1 - Operational Planning and Control: Изисква систематично третиране на техническите уязвимости, за да се осигури постоянна ефективност на контролите за сигурност.

11.2 ISO/IEC 27002:2022 - Controls 8.8, 8.9, 5: Предоставя насоки за внедряване относно прилагането на корекции, сканирането за уязвимости, цялостта на софтуера и интеграцията със сигурната конфигурация и инвентаризацията на активите.

11.3 NIST SP 800-53 Rev.5: RA-5 - Мониторинг и сканиране за уязвимости: изисква често сканиране и проследяване на отстраняването. SI-2 - Отстраняване на дефекти: изисква своевременна оценка и смекчаване на дефекти чрез налични корекции или други действия. CM-2 / CM-6 - Базови конфигурации и контроли за управление на конфигурацията: установява основата за сигурни системни конфигурации, свързани с прилагането на корекции.

11.4 EU GDPR (2016/679): Член 32 - Сигурност на обработването: изисква внедряване на подходящи технически мерки, като своевременно прилагане на корекции и третиране на уязвимости, за да се осигурят поверителност и устойчивост на системите. Съображение 49: насърчава организациите да внедряват превантивни контроли срещу известни заплахи в подкрепа на сигурността и непрекъсваемостта.

11.5 Директива ЕС NIS2 (2022/2555): Член 21(2)(d): задължава съществените и важните субекти да откриват, реагират и смекчават системните уязвимости и да поддържат високо ниво на киберхигиена.

11.6 EU DORA (2022/2554): Член 8 - Управление на ИКТ риска: изисква идентифициране и своевременно отстраняване на уязвимости в информационните и комуникационните технологии, използвани във финансови системи. Член 10(2)(f): подчертава непрекъснатите оценки на уязвимости и прилагането на корекции, водени от заплахите, като част от оперативната устойчивост.

11.7 COBIT 2019: DSS05.02 - Управление на уязвимостите по сигурността: насочва организациите да сканират, проследяват и смекчават известни технически слабости. DSS01.03 - Мониторинг на инфраструктурата: гарантира, че системите се наблюдават за признаци на експлоатиране или слабости. MEA03 - Мониторинг, оценяване и преценка на съответствието: изисква редовен одит на ефективността на контролите, включително статуса на корекциите и обработването на изключения.