					Въведете тук наименованието на регистрираното юридическо лице							
Номер на документа: P20					Заглавие на документа: **Политика за защита на крайните точки / зловреден софтуер**							
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	Клауза 8	Изисква защита на крайните точки и контроли срещу зловреден софтуер за постигане на целите на СУИС
ISO/IEC 27002:2022	Контроли 8.7, 8	Предоставя технически контроли и насоки за защита срещу зловреден софтуер, защита на крайните точки и управление на инциденти
NIST SP 800-53 Rev.5	SI-3, SI-4, CM-6	Определя изисквания за защита срещу злонамерен код, централизирано наблюдение и базови конфигурации
EU GDPR	Член 32	Изисква подходящи технически мерки за защита на личните данни, включително защита срещу зловреден софтуер
EU NIS2	Член 21(2)(d)	Изисква внедряване на механизми за откриване на заплахи и превантивни мерки на ниво крайна точка
EU DORA	Член 9	Изисква управление на ИКТ риска по отношение на зловредния софтуер и заплахите, произтичащи от крайни точки
COBIT 2019	DSS05.01, DSS01.04, MEA	Изисква защита, наблюдение и оценяване на контролите за крайни точки

1. Цел

1.1 Настоящата политика определя задължителните контроли и оперативните изисквания за защита на организационните крайни точки — включително настолни компютри, преносими компютри, мобилни устройства и сървъри — срещу зловреден софтуер и свързаните с него заплахи.

1.2 Тя установява минимални изисквания за защита на крайните точки, откриване на зловреден софтуер, действия по ограничаване и поведенчески мониторинг, като гарантира, че системите остават устойчиви както срещу масово разпространени, така и срещу усъвършенствани разновидности на зловреден софтуер.

1.3 Политиката пряко подпомага съответствието с ISO/IEC 27001:2022, Клауза 8.1, и Контрол 8.7 от Приложение A и е съгласувана с регионалните задължения по киберсигурност съгласно GDPR, NIS2 и DORA.

2. Обхват

2.1 Настоящата политика се прилага за всички крайни точки, включително:

2.1.1 Настолни компютри, преносими компютри, мобилни устройства и виртуални инстанции, притежавани от организацията или управлявани от нея

2.1.2 Лично притежавани устройства, разрешени съгласно Политиката за използване на лични устройства (BYOD), при условие че е внедрено управление на мобилни устройства или е инсталиран агент за крайна точка

2.1.3 Сървъри и инфраструктурни активи, включително виртуални машини, хоствани в облачна среда, и периферни устройства

2.1.4 Операционни системи, драйвери, локални услуги, агенти за крайни точки и контроли за сигурност, инсталирани на всеки възел

2.2 Всички лица с административна, техническа или оперативна отговорност за която и да е крайна точка попадат в обхвата на тази политика, включително:

2.2.1 Вътрешни служители и външни изпълнители

2.2.2 Доставчици на управлявани услуги (MSP), външни изпълнители по поддръжка на работни станции и ИТ администратори от трети страни

2.2.3 Потребители, упълномощени да използват преносими системи, преносими компютри с активиран VPN или мобилен достъп до организационните мрежи

2.3 Обхватът на заплахите по тази политика включва, без да се ограничава до:

2.3.1 Вируси, червеи, троянски коне, ransomware, шпионски софтуер, rootkits, adware, кийлогъри, ботмрежи

2.3.2 Безфайлов зловреден софтуер, zero-day полезен товар, зловреден софтуер за ескалация на привилегии и експлойт комплекти за браузъри

2.3.3 Злонамерен код, доставен чрез преносими носители, фишинг вектори, drive-by downloads или атаки чрез USB

3. Цели

3.1 Да се защитава целостта, наличността и поверителността на системите от крайни точки и данните, които те обработват, чрез надеждно предотвратяване, откриване и реагиране при зловреден софтуер.

3.2 Да се предотвратява изпълнението или разпространението на злонамерен код в организационните мрежи чрез прилагане на технически предпазни мерки, закаляване на устройствата и телеметрия в реално време.

3.3 Да се интегрира защитата на крайните точки с други контроли на СУИС, включително управление на уязвимости, контрол на достъпа, регистриране и мониторинг, както и реагиране при инциденти.

3.4 Да се осигури непрекъсната видимост върху крайните точки чрез централно управлявани платформи за защита, включително антивирусни/антизловредни агенти, откриване и реагиране на крайни точки (EDR) и SIEM телеметрия.

3.5 Да се спазват правните, регулаторните и стандартизационните изисквания, налагащи сигурност на крайните точки (напр. GDPR Член 32, NIS2 Член 21, DORA Член 9).

3.6 Да се определят роли с отчетност, да се прилагат SLA за внедряване на корекции и реакция по аларми и да се осигури готовност за одит чрез документация и докладване.

4. Роли и отговорности

4.1 Директор по информационна сигурност (CISO)

4.1.1 Отговаря за тази политика и осигурява нейното съгласуване със СУИС и цялостната стратегия по сигурността.

4.1.2 Преглежда на тримесечна база показателите за защита на крайните точки, тенденциите при инцидентите и ефективността на инструментите.

4.1.3 Одобрява изключенията и приемането на остатъчен риск, свързани с обхвата на защита на крайните точки.

4.2 Ръководител по сигурността на крайните точки / Мениджър на центъра за операции по сигурността (SOC)

4.2.1 Управлява системите за защита на крайните точки (напр. AV, EDR, MDM).

4.2.2 Осъществява надзор върху прилагането на политиката, настройките за откриване на заплахи и процедурите за реагиране.

4.2.3 Поддържа показатели за покритие, дневници за инциденти със зловреден софтуер и базови конфигурации на алармите.

[... 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 ежегодно или когато:

9.1.1 Възникнат съществени кампании със зловреден софтуер или инциденти, свързани със сигурността на крайните точки

9.1.2 Нови видове заплахи (напр. безфайлов зловреден софтуер, варианти на ransomware) налагат актуализирани стратегии за откриване или реагиране

9.1.3 Платформите за защита на крайните точки или архитектурите на агентите се променят съществено

9.1.4 Бъдат актуализирани правни или регулаторни изисквания, засягащи контролите за крайни точки

9.2 Прегледът се инициира от Ръководителя по сигурността на крайните точки и се координира с функциите по CISO, правни въпроси, риск и одит.

9.3 Одобрените редакции трябва да бъдат документирани в Регистъра на документите на СУИС, да им бъде присвоен нов идентификатор на версия и да бъдат съобщени на всички засегнати страни.

9.4 Заменените версии трябва да бъдат архивирани с ограничен достъп и съхранявани за целите на целостта на одитната следа съгласно графиците за съхранение на СУИС.

10. Свързани политики и връзки

10.1 P1 - Политика за информационна сигурност. Установява основните принципи за защита на системи, данни и мрежи. Настоящата политика прилага тези принципи на ниво крайна точка чрез технически и процедурни контроли срещу зловреден софтуер.

10.2 P4 - Политика за контрол на достъпа. Определя ограниченията за потребителски достъп, които се прилагат на ниво крайна точка, включително защита срещу ескалация на привилегии и неоторизирано инсталиране на непроверен софтуер.

10.3 P5 - Политика за управление на промените. Осигурява актуализациите на софтуера за защита на крайните точки, правилата на политиката или конфигурациите на агентите да подлежат на одобрение и контролирани процеси по внедряване.

10.4 P12 - Политика за управление на активите. Осигурява основата за класификация на активите и инвентар на активите, необходима за видимост върху крайните точки, покритие на корекциите и определяне на обхвата на защитата срещу зловреден софтуер.

10.5 P22 - Политика за регистриране и мониторинг. Позволява интеграция на аларми от крайни точки, състояние на агентите и разузнаване за заплахи в централизирани SIEM системи за откриване в реално време и форензична проследимост.

10.6 P30 - Политика за реагиране при инциденти. Свързва инцидентите със зловреден софтуер на крайни точки със стандартизирани работни потоци за ограничаване, отстраняване, разследване и възстановяване с определени роли и прагове за ескалация.

11. Референтни стандарти и рамки

11.1 ISO/IEC 27001:

11.1.1 Клауза 8.1 - Оперативно планиране и контрол: Изисква внедряване на технически контроли, включително предпазни мерки за крайни точки, за поддържане на целите на СУИС.

11.2 ISO/IEC 27002:2022 - Контроли 8.7, 8:

11.2.1 Предоставя подробни технически насоки относно мерките срещу зловреден софтуер, сигурното внедряване на софтуер, наблюдението и готовността за реагиране при инциденти в среди на крайни точки.

11.3 NIST SP 800-53 Rev.5:

11.3.1 SI-3 - Защита срещу злонамерен код: Изисква използване на инструменти срещу зловреден софтуер със сканиране в реално време, сканиране при достъп и поведенчески анализ.

11.3.2 SI-4 - Наблюдение на системите: Подпомага интеграцията на телеметрия с централизирани платформи за откриване.

11.3.3 CM-6 - Настройки на конфигурацията: Подсилва прилагането на базови настройки за контрол на крайните точки, включително задължително използване на агенти за защита.

11.4 EU GDPR (2016/679):

11.4.1 Член 32 - Сигурност на обработването: Изисква организациите да внедрят подходящи технически мерки за защита на личните данни, включително защита срещу заплахи от зловреден софтуер.

11.5 Директива на ЕС NIS2 (2022/2555):

11.5.1 Член 21(2)(d): Задължава субектите да внедрят мерки за откриване и предотвратяване на заплахи, включително механизми за защита срещу зловреден софтуер на ниво крайна точка.

11.6 EU DORA (2022/2554):

11.6.1 Член 9 - Изисквания за управление на ИКТ риска: Изисква финансовите субекти да приемат защитни мерки за предотвратяване, откриване и реагиране при зловреден софтуер и заплахи, произтичащи от крайни точки.

11.7 COBIT 2019:

11.7.1 DSS05.01 - Защита срещу зловреден софтуер: Изисква откриване и смекчаване на зловреден софтуер във всички организационни крайни точки.

11.7.2 DSS01.04 - Управление на наличността и капацитета: Осигурява баланс между защитата срещу зловреден софтуер, производителността на системите и непрекъсваемостта на дейността.

11.7.3 MEA03 - Наблюдение, оценяване и преценка на съответствието: Изисква периодичен одит на контролите за крайни точки и ефективността на защитата.