					Въведете тук наименованието на регистрираното юридическо лице							
Номер на документа: P20S					Заглавие на документа: **Политика за защита на крайните точки от 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**

Съгласувано с приложимите стандарти и регулации

Стандарт/регулация	Клауза/член	Коментар
ISO/IEC 27001:2022	Клауза 8	Оперативни контроли за защита от зловреден софтуер
ISO/IEC 27002:2022	Контрол 8	Контролни мерки за защита на крайните точки
NIST SP 800-53 Rev.5	SI-3, SI-4	Защита от злонамерен код и реагиране при инциденти
EU NIS2	Членове 21(2)(d), (e)	Защита от зловреден софтуер и управление на риска за съществени/важни субекти
EU DORA	Членове 10(1), 15	Оперативна устойчивост и проверка на трети страни
COBIT 2019	DSS05.02, DSS05.04	Защита и мониторинг на крайни точки/мрежа
EU GDPR	Членове 32(1)(b), 33	Технически/организационни мерки и уведомяване при нарушение

1. Цел

1.1 Настоящата политика определя минималните технически, процедурни и поведенчески изисквания за защита на всички крайни устройства — включително преносими и настолни компютри, мобилни устройства и преносими носители — от злонамерен код, включително вируси, ransomware, spyware, rootkit и други заплахи от зловреден софтуер.

1.2 Целта ѝ е да гарантира, че крайните точки са оборудвани, поддържани и използвани по начин, който намалява риска от заразяване със зловреден софтуер, разпространението му и компрометирането на системи.

1.3 Организацията признава, че крайните точки често се използват като входна точка за зловреден софтуер и поради това трябва да бъдат укрепени, наблюдавани и защитени чрез многостепенна защита.

1.4 Политиката подпомага целите на организацията във връзка със сертифицирането по ISO/IEC 27001:2022 и е съгласувана с Общия регламент относно защитата на данните на ЕС (GDPR), Директивата NIS2, Регламента за цифрова оперативна устойчивост (DORA) и други приложими рамки.

2. Обхват

2.1 Настоящата политика се прилага за:

2.1.1 всички крайни точки на организацията, включително настолни компютри, преносими компютри, таблети, мобилни телефони и POS терминали

2.1.2 лично притежавани устройства (BYOD), използвани за достъп до служебни приложения или данни

2.1.3 преносими носители за съхранение, като USB устройства и външни твърди дискове

2.1.4 всички операционни системи, софтуер за крайни точки или комуникационни инструменти, работещи на тези платформи

2.2 Политиката се прилага еднакво за:

2.2.1 вътрешен персонал, външни изпълнители, стажанти и доставчици на управлявани услуги

2.2.2 устройства, използвани на място, дистанционно или при хибриден модел на работа

2.2.3 облачно свързани или автономни крайни точки, съхраняващи служебни или лични данни

3. Цели

3.1 Да се предотвратява заразяването и разпространението на зловреден софтуер във вътрешни системи, потребителски устройства и външни връзки.

3.2 Да се осигурява бързо откриване и ограничаване на заплахи, свързани със зловреден софтуер, чрез автоматизирани технологии за защита на крайните точки и определени канали за ескалация.

3.3 Да се гарантира, че за достъп до служебна информация се използват само разрешени, защитени и наблюдавани устройства.

3.4 Да се прилагат ясно определени отговорности на персонала и правила за поведение на потребителите с цел намаляване на риска от инциденти, свързани със зловреден софтуер.

3.5 Да се поддържат проследими и подлежащи на одит записи за откриване на зловреден софтуер, предприети действия и съответствие с политиката.

3.6 Да се защитават личните и служебните данни от компрометиране вследствие на зловреден софтуер чрез многостепенни защитни стратегии.

4. Роли и отговорности

4.1 Управител

4.1.1 Носи отговорност за настоящата политика и осигурява достатъчни ресурси за защита на крайните точки.

4.1.2 Одобрява антивирусния софтуер, инструментите за управление на мобилни устройства и правилата за достъп на трети страни.

4.1.3 Преглежда докладите за инциденти със зловреден софтуер, обобщенията на въздействието и уведомленията за нарушения, свързани с крайни точки.

4.2 Доставчик на ИТ поддръжка / вътрешен ИТ администратор

4.2.1 Избира и внедрява антивирусен и antimalware софтуер, както и решения за откриване и реагиране на крайни точки (EDR).

4.2.2 Осигурява последователното прилагане на актуализации и съхранението на журналите.

4.2.3 Реагира на предупреждения за зловреден софтуер, изолира заразени системи и извършва действия по отстраняване.

4.2.4 Прилага контроли върху използването на USB устройства и външни носители.

[... 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 Изискване за годишен преглед

9.1.1 Настоящата политика трябва да се преглежда официално поне веднъж годишно от Управителя, в координация с Доставчика на ИТ поддръжка и Координатора по поверителността.

9.2 Актуализации при настъпване на определени събития

9.2.1 Актуализации на политиката трябва да се извършват и когато:

9.2.1.1 нова съществена заплаха или масово разпространение на зловреден софтуер засяга крайни точки, използвани от организацията

9.2.1.2 антивирусните или EDR инструментите са променени, надградени или заменени

9.2.1.3 инцидент със зловреден софтуер разкрие слабости в обхвата или прилагането на тази политика

9.2.1.4 правните или регулаторните изисквания (напр. GDPR, DORA, NIS2) бъдат актуализирани

9.3 Управление на версиите и комуникация

9.3.1 Всички промени в политиката трябва да бъдат документирани с номер на версия, дата и обобщение на промените.

9.3.2 Персоналът трябва да бъде уведомяван за актуализациите, особено ако те променят оперативните изисквания или изискванията за поведение.

9.3.3 Предходните версии трябва да се съхраняват в архива на политиките поне 3 години в подкрепа на одити.

10. Свързани политики и връзки

10.1 Тази политика трябва да се прилага съвместно със следните SME политики:

10.1.1 P9S – Политика за дистанционна работа: Осигурява прилагане на изискванията за защита на крайните точки върху устройства, използвани извън обекта или в хибридна среда

10.1.2 P12S – Политика за управление на активите: Подпомага проследяването и контрола върху всички крайни точки, като гарантира, че се използват само разрешени и защитени устройства

10.1.3 P17S – Политика за защита на данните и поверителност: Подсилва превенцията срещу зловреден софтуер като основна контролна мярка за поверителност за защита на лични и чувствителни данни от компрометиране

10.1.4 P22S – Политика за регистриране и мониторинг: Определя изискванията за журналиране на събития, свързани със зловреден софтуер, и за поддържане на видимост на предупрежденията за ранно реагиране

10.1.5 P30S – Политика за реагиране при инциденти: Определя стъпките за ескалация, ограничаване и външно уведомяване, ако зловредният софтуер доведе до компрометиране на данни или оперативно прекъсване

11. Референтни стандарти и рамки

11.1 ISO/IEC 27001

11.1.1 Клауза 8.1 – Изисква внедряване на оперативни контроли за намаляване на рискове като атаки със зловреден софтуер

11.2 ISO/IEC 27002

11.2.1 Контрол 8.7 – Описва практики за контрол на зловредния софтуер, включително антивирусна защита, сканиране в реално време, актуализации и обучение на потребителите

11.3 NIST SP 800-53 Rev.5

11.3.1 SI-3 – Изисква внедряване на механизми за защита от злонамерен код на крайните точки

11.3.2 SI-4 – Изисква мониторинг, откриване, анализ и действия по реагиране при заплахи и предупреждения на ниво крайна точка

11.4 EU GDPR

11.4.1 Член 32(1)(b) – Изисква технически и организационни контроли (като антивирусна защита) за защита на личните данни

11.4.2 Член 33 – Налага уведомяване при нарушение, когато зловреден софтуер компрометира целостта, поверителността или наличността на данните

11.5 Директива EU NIS2

11.5.1 Член 21(2)(d) – Изисква мерки за предотвратяване и реагиране на заплахи от зловреден софтуер в рамките на съществени и важни субекти

11.5.2 Член 21(2)(e) – Изисква многостепенни стратегии за управление на киберрискове, включително защита на крайните точки от зловреден софтуер

11.6 EU DORA

11.6.1 Член 10(1) – Изисква ИКТ системите да бъдат защитени от зловреден софтуер и други заплахи като част от оперативната устойчивост

11.6.2 Член 15 – Задължава финансовите организации да проверяват защитата от зловреден софтуер при външни доставчици на услуги

11.7 COBIT 2019

11.7.1 DSS05.02 – Подчертава защитните мерки за защита на крайните точки и мрежите от заплахи от зловреден софтуер

11.7.2 DSS05.04 – Подкрепя мониторинга и предупрежденията за свързани със зловреден софтуер събития по сигурността като част от текущите операции