					Sem vložte název registrované právnické osoby						
Číslo dokumentu: P20S					Název dokumentu: **Politika ochrany koncových zařízení před malwarem**						
Verze: 1.0		Datum účinnosti: 01.01.2025			Vlastník dokumentu:						
X	Politika		Standard		Postup		Formulář		Registr		Jiné

Historie revizí				
Číslo revize	**Datum revize**	**Změny**	**Přezkoumal**	**Vlastník procesu**

Schválení			
Jméno	**Funkce**	**Datum**	**Podpis**

V souladu s normami a právními předpisy

Norma/právní předpis	Kapitola/článek	Komentář
ISO/IEC 27001:2022	Kapitola 8	Provozní opatření na ochranu před malwarem
ISO/IEC 27002:2022	Opatření 8	Bezpečnostní opatření na ochranu koncových zařízení
NIST SP 800-53 Rev.5	SI-3, SI-4	Ochrana před škodlivým kódem a reakce na incidenty
směrnice EU NIS2	Článek 21(2)(d), (e)	Ochrana před malwarem a řízení rizik pro základní a významné subjekty
nařízení EU DORA	Článek 10(1), 15	Provozní odolnost a ověřování třetích stran
COBIT 2019	DSS05.02, DSS05.04	Ochrana koncových zařízení/sítí a monitorování
GDPR	Článek 32(1)(b), 33	Technická a organizační opatření a oznamování porušení zabezpečení

1. Účel

1.1 Tato politika stanoví minimální technické, procesní a behaviorální požadavky na ochranu všech koncových zařízení — například notebooků, stolních počítačů, mobilních zařízení a přenosných médií — před škodlivým kódem, včetně virů, ransomwaru, spywaru, rootkitů a dalších forem malwaru.

1.2 Jejím účelem je zajistit, aby koncová zařízení byla vybavena, udržována a používána způsobem, který snižuje riziko infekce malwarem, jeho šíření a kompromitace systémů.

1.3 Organizace uznává, že koncová zařízení představují běžné vstupní body pro malware, a proto musí být zpevnění konfigurace zařízení, monitorování a ochrana zajištěny prostřednictvím vícevrstvé ochrany.

1.4 Tato politika podporuje cíle organizace v oblasti certifikace podle ISO/IEC 27001:2022 a je v souladu s GDPR, směrnicí NIS2, nařízením DORA a dalšími relevantními rámci.

2. Rozsah

2.1 Tato politika se vztahuje na:

2.1.1 všechna koncová zařízení organizace, včetně stolních počítačů, notebooků, tabletů, mobilních telefonů a platebních terminálů

2.1.2 soukromá zařízení používaná v režimu BYOD, která slouží k přístupu k podnikovým aplikacím nebo datům

2.1.3 vyměnitelná úložná média, jako jsou USB disky a externí pevné disky

2.1.4 všechny operační systémy, software koncových zařízení a komunikační nástroje provozované na těchto platformách

2.2 Vztahuje se rovněž na:

2.2.1 interní pracovníky, smluvní pracovníky, stážisty a poskytovatele řízených služeb (MSP)

2.2.2 zařízení používaná na pracovišti, vzdáleně nebo v hybridním režimu

2.2.3 aktiva připojená ke cloudu i offline koncová zařízení ukládající podniková nebo osobní data

3. Cíle

3.1 Předcházet infekci malwarem a jeho šíření napříč interními systémy, uživatelskými zařízeními a externími připojeními

3.2 Včas detekovat a omezovat hrozby související s malwarem pomocí automatizovaných technologií ochrany koncových zařízení a definovaných eskalačních postupů

3.3 Zajistit, aby pro přístup k podnikovým informacím byla používána pouze oprávněná, zabezpečená a monitorovaná zařízení

3.4 Uplatňovat jednoznačně vymezené odpovědnosti pracovníků a pravidla chování uživatelů za účelem snížení rizika incidentů souvisejících s malwarem

3.5 Udržovat dohledatelné a auditovatelné záznamy o detekci malwaru, reakci a souladu s touto politikou

3.6 Chránit osobní a podniková data před kompromitací způsobenou malwarem prostřednictvím vícevrstvé ochrany

4. Role a odpovědnosti

4.1 generální ředitel (GM)

4.1.1 Je vlastníkem této politiky a zajišťuje dostupnost dostatečných zdrojů pro ochranu koncových zařízení

4.1.2 Schvaluje antivirový software, nástroje pro správu mobilních zařízení a pravidla přístupu třetích stran

4.1.3 Přezkoumává hlášení o malwarových incidentech, souhrny dopadů a oznámení o porušení zabezpečení týkající se koncových zařízení

4.2 IT podpora / interní správce IT

4.2.1 Vybírá a nasazuje antivirový software, antimalwarový software a EDR (detekce a reakce na koncových zařízeních)

4.2.2 Zajišťuje konzistentní aplikaci aktualizací a uchovávání protokolů

4.2.3 Reaguje na upozornění na malware, izoluje infikované systémy a provádí nápravná opatření

4.2.4 Uplatňuje opatření pro používání USB zařízení a externích médií

[... Oddíly 4.3–8 nejsou součástí tohoto náhledu. Pro přístup k úplnému obsahu zakupte celý dokument. ...]

9. Požadavky na přezkoumávání a aktualizaci

9.1 Požadavek na roční přezkum

9.1.1 Tato politika musí být formálně přezkoumána nejméně jednou ročně generálním ředitelem ve spolupráci s IT podporou a koordinátorem ochrany soukromí

9.2 Aktualizace vyvolané událostí

9.2.1 Aktualizace politiky musí proběhnout také tehdy, když:

9.2.1.1 nová významná hrozba malwaru nebo rozsáhlá kampaň cílí na koncová zařízení používaná organizací

9.2.1.2 jsou antivirové nástroje nebo EDR změněny, rozšířeny nebo nahrazeny

9.2.1.3 malwarový incident odhalí slabiny v rozsahu nebo uplatňování této politiky

9.2.1.4 dojde ke změně právních nebo regulačních požadavků (např. GDPR, DORA, NIS2)

9.3 Řízení verzí a komunikace

9.3.1 Všechny změny politiky musí být zdokumentovány číslem verze, datem a shrnutím změn

9.3.2 Pracovníci musí být o aktualizacích informováni, zejména pokud mění provozní nebo behaviorální požadavky

9.3.3 Předchozí verze musí být uchovávány v archivu politik nejméně 3 roky na podporu auditů

10. Související politiky a vazby

10.1 Tato politika musí být implementována společně s následujícími SME politikami:

10.1.1 P9S – Politika práce na dálku: Zajišťuje, že požadavky na ochranu koncových zařízení jsou uplatňovány na zařízeních používaných mimo pracoviště nebo v hybridním režimu

10.1.2 P12S – Politika správy aktiv: Podporuje evidenci a řízení všech koncových zařízení a zajišťuje, že jsou používána pouze oprávněná a chráněná zařízení

10.1.3 P17S – Politika ochrany dat a soukromí: Posiluje prevenci malwaru jako klíčové opatření ochrany soukromí pro ochranu osobních a citlivých dat před kompromitací

10.1.4 P22S – Politika protokolování a monitorování: Stanoví požadavky na protokolování událostí souvisejících s malwarem a zachování viditelnosti upozornění pro včasnou reakci

10.1.5 P30S – Politika reakce na incidenty: Vymezuje kroky eskalace, zamezení šíření a externího oznamování, pokud malware vede ke kompromitaci dat nebo provoznímu narušení

11. Referenční normy a rámce

11.1 ISO/IEC 27001

11.1.1 Kapitola 8.1 – Vyžaduje implementaci provozních opatření ke snížení rizik, jako jsou útoky malwaru

11.2 ISO/IEC 27002

11.2.1 Opatření 8.7 – Popisuje postupy řízení malwaru včetně antiviru, skenování v reálném čase, aktualizací a školení uživatelů

11.3 NIST SP 800-53 Rev.5

11.3.1 SI-3 – Vyžaduje nasazení mechanismů ochrany před škodlivým kódem napříč koncovými zařízeními

11.3.2 SI-4 – Ukládá monitorování, detekci, analýzu a reakční kroky pro hrozby a upozornění na úrovni koncových zařízení

11.4 GDPR

11.4.1 Článek 32(1)(b) – Vyžaduje technická a organizační opatření (například antivirus) k ochraně osobních údajů

11.4.2 Článek 33 – Ukládá oznamovací povinnost při porušení zabezpečení, pokud malware naruší integritu, důvěrnost nebo dostupnost dat

11.5 směrnice NIS2

11.5.1 Článek 21(2)(d) – Vyžaduje opatření k prevenci a reakci na hrozby malwaru v rámci základních a významných subjektů

11.5.2 Článek 21(2)(e) – Ukládá vícevrstvé strategie řízení kybernetických rizik včetně ochrany koncových zařízení před malwarem

11.6 nařízení DORA

11.6.1 Článek 10(1) – Vyžaduje ochranu ICT systémů před malwarem a dalšími hrozbami jako součást provozní odolnosti

11.6.2 Článek 15 – Ukládá finančním organizacím ověřovat ochranu před malwarem u poskytovatelů služeb třetích stran

11.7 COBIT 2019

11.7.1 DSS05.02 – Zdůrazňuje ochranná opatření k obraně koncových zařízení a sítí před hrozbami malwaru

11.7.2 DSS05.04 – Podporuje monitorování a upozorňování na bezpečnostní události související s malwarem jako součást průběžného provozu