					Sem zadajte názov registrovanej právnickej osoby							
Číslo dokumentu: P20S					Názov dokumentu: **Politika ochrany koncových zariadení pred malvérom**							
Verzia: 1.0		Dátum nadobudnutia účinnosti: 01.01.2025			Vlastník dokumentu:							
X	Politika		Štandard		Postup		Formulár		Register		Iné	

História revízií				
Číslo revízie	**Dátum revízie**	**Zmeny**	**Preskúmal**	**Vlastník procesu**

Schválenia			
Meno	**Pozícia**	**Dátum**	**Podpis**

Právne upozornenie (autorské práva a obmedzenia používania)

(C) 2025 Clarysec LLC. All rights reserved.

Tento dokument je duševným vlastníctvom spoločnosti Clarysec LLC. Žiadna časť tohto dokumentu nesmie byť bez predchádzajúceho výslovného písomného súhlasu kopírovaná, znovu použitá, distribuovaná ani upravovaná na komerčné alebo implementačné účely.
Neoprávnené použitie je prísne zakázané a môže viesť k právnym krokom.
V prípade licencovania kontaktujte: info@clarysec.com

V súlade s normami a predpismi

Norma/predpis	Kapitola/článok	Poznámka
ISO/IEC 27001:2022	Kapitola 8	Prevádzkové opatrenia na ochranu pred malvérom
ISO/IEC 27002:2022	Kontrola 8	Kontrolné opatrenia na ochranu koncových zariadení
NIST SP 800-53 Rev.5	SI-3, SI-4	Ochrana pred škodlivým kódom a reakcia na incidenty
Smernica EÚ NIS2	Články 21(2)(d), (e)	Ochrana pred malvérom a riadenie rizík pre základné a dôležité subjekty
Nariadenie EÚ DORA	Články 10(1), 15	Prevádzková odolnosť a preverovanie tretích strán
COBIT 2019	DSS05.02, DSS05.04	Ochrana koncových zariadení a sietí a monitorovanie
Nariadenie EÚ GDPR	Články 32(1)(b), 33	Technické a organizačné opatrenia a oznamovanie porušenia ochrany osobných údajov

1. Účel

1.1 Táto politika stanovuje minimálne technické, procesné a behaviorálne požiadavky na ochranu všetkých koncových zariadení, ako sú notebooky, stolové počítače, mobilné zariadenia a prenosné médiá, pred škodlivým kódom vrátane vírusov, ransomvéru, spyvéru, rootkitov a iných foriem malvéru.

1.2 Jej účelom je zabezpečiť, aby boli koncové zariadenia vybavené, udržiavané a používané spôsobom, ktorý znižuje riziko infekcie malvérom, jeho šírenia a kompromitácie systémov.

1.3 Organizácia uznáva, že koncové zariadenia predstavujú bežné vstupné body pre malvér, a preto musia byť hardenované, monitorované a chránené použitím viacerých vrstiev obrany.

1.4 Táto politika podporuje ciele organizácie v oblasti certifikácie podľa ISO/IEC 27001:2022 a je zosúladená s nariadením EÚ GDPR, smernicou EÚ NIS2, nariadením EÚ DORA a ďalšími relevantnými rámcami.

2. Rozsah

2.1 Táto politika sa vzťahuje na:

2.1.1 všetky koncové zariadenia organizácie vrátane stolových počítačov, notebookov, tabletov, mobilných telefónov a POS terminálov

2.1.2 súkromné zariadenia používané na prístup k podnikovým aplikáciám alebo údajom v režime BYOD (používanie vlastných zariadení)

2.1.3 vymeniteľné úložné zariadenia, ako sú USB kľúče a externé pevné disky

2.1.4 všetky operačné systémy, softvér koncových zariadení alebo komunikačné nástroje prevádzkované na týchto platformách

2.2 Rovnako sa vzťahuje na:

2.2.1 interných používateľov, zmluvných dodávateľov, poskytovateľov služieb tretích strán, stážistov a poskytovateľov spravovaných služieb

2.2.2 zariadenia používané na pracovisku, pri práci na diaľku alebo v hybridnom režime

2.2.3 aktíva pripojené ku cloudu alebo offline koncové zariadenia uchovávajúce informácie organizácie alebo osobné údaje

3. Ciele

3.1 Predchádzať infekcii malvérom a jeho šíreniu v interných systémoch, používateľských zariadeniach a externých pripojeniach.

3.2 Rýchlo detegovať a obmedziť hrozby súvisiace s malvérom použitím automatizovaných technológií zabezpečenia koncových zariadení a definovaných eskalačných postupov.

3.3 Zabezpečiť, aby sa na prístup k informáciám organizácie používali len autorizované, zabezpečené a monitorované zariadenia.

3.4 Uplatňovať jasne definované zodpovednosti zamestnancov a pravidlá správania používateľov na zníženie rizika incidentov súvisiacich s malvérom.

3.5 Udržiavať sledovateľné a auditovateľné záznamy o detekcii malvéru, reakcii a súlade s touto politikou.

3.6 Chrániť osobné údaje a informácie organizácie pred kompromitáciou v dôsledku malvéru použitím stratégie obrany do hĺbky.

4. Roly a zodpovednosti

4.1 Generálny manažér (GM)

4.1.1 Zodpovedá za túto politiku a zabezpečuje dostatočné zdroje na ochranu koncových zariadení.

4.1.2 Schvaľuje antivírusový softvér, nástroje na správu mobilných zariadení (MDM) a pravidlá prístupu tretích strán.

4.1.3 Preskúmava správy o incidentoch súvisiacich s malvérom, súhrny dopadov a oznámenia o porušení ochrany osobných údajov týkajúce sa koncových zariadení.

4.2 Poskytovateľ IT podpory / interný IT administrátor

4.2.1 Vyberá a nasadzuje antivírusový softvér, antimalvérové riešenia a nástroje EDR (Endpoint Detection and Response).

4.2.2 Zabezpečuje konzistentné uplatňovanie aktualizácií a uchovávanie logov.

4.2.3 Reaguje na upozornenia na malvér, izoluje infikované systémy a vykonáva nápravné opatrenia.

4.2.4 Uplatňuje kontroly používania USB zariadení a externých zariadení.

[... Sekcie 4.3–8 nie sú súčasťou tohto náhľadu. Pre prístup k úplnému obsahu si zakúpte celý dokument. ...]

9. Požiadavky na preskúmanie a aktualizáciu

9.1 Požiadavka na ročné preskúmanie

9.1.1 Táto politika musí byť formálne preskúmaná aspoň raz ročne generálnym manažérom (GM) v koordinácii s poskytovateľom IT podpory a koordinátorom ochrany súkromia.

9.2 Aktualizácie na základe spúšťacej udalosti

9.2.1 Politika musí byť aktualizovaná aj vtedy, ak:

9.2.1.1 nová významná hrozba malvéru alebo jeho šírenie cieli na koncové zariadenia používané organizáciou

9.2.1.2 sú nástroje antivírusového softvéru alebo EDR zmenené, aktualizované alebo nahradené

9.2.1.3 incident súvisiaci s malvérom odhalí slabiny v rozsahu tejto politiky alebo v jej uplatňovaní

9.2.1.4 dôjde k aktualizácii právnych alebo regulačných požiadaviek (napr. GDPR, DORA, NIS2)

9.3 Riadenie verzií a komunikácia

9.3.1 Všetky zmeny politiky musia byť zdokumentované číslom verzie, dátumom a súhrnom zmien.

9.3.2 Zamestnanci musia byť o aktualizáciách informovaní, najmä ak menia prevádzkové alebo behaviorálne požiadavky.

9.3.3 Predchádzajúce verzie musia byť uchovávané v archíve politík najmenej 3 roky na podporu auditov.

10. Súvisiace politiky a väzby

10.1 Táto politika sa musí uplatňovať v spojení s nasledujúcimi politikami SME:

10.1.1 P9S – Politika práce na diaľku: zabezpečuje, aby sa požiadavky na ochranu koncových zariadení uplatňovali na zariadeniach používaných mimo pracoviska alebo v hybridnom režime

10.1.2 P12S – Politika správy aktív: podporuje sledovanie a riadenie všetkých koncových zariadení tak, aby sa používali len autorizované a chránené zariadenia

10.1.3 P17S – Politika ochrany údajov a súkromia: posilňuje prevenciu proti malvéru ako základné opatrenie na ochranu súkromia a osobných údajov a citlivých údajov pred kompromitáciou

10.1.4 P22S – Politika logovania a monitorovania: stanovuje požiadavky na logovanie udalostí súvisiacich s malvérom a zachovanie viditeľnosti upozornení na včasnú reakciu

10.1.5 P30S – Politika reakcie na incidenty: definuje eskaláciu, zamedzenie šírenia a kroky externého oznamovania, ak malvér vedie ku kompromitácii údajov alebo narušeniu prevádzky

11. Referenčné normy a rámce

11.1 ISO/IEC 27001

11.1.1 Kapitola 8 – Vyžaduje implementáciu prevádzkových kontrol na znižovanie rizík, ako sú útoky malvérom.

11.2 ISO/IEC 27002

11.2.1 Kontrola 8.7 – Podrobne opisuje postupy ochrany pred malvérom vrátane antivírusového softvéru, kontroly v reálnom čase, aktualizácií a školenia používateľov.

11.3 NIST SP 800-53 Rev.5

11.3.1 SI-3 – Vyžaduje nasadenie mechanizmov ochrany pred škodlivým kódom na koncových zariadeniach.

11.3.2 SI-4 – Ukladá povinnosť monitorovania, detekcie, analýzy a reakcie na hrozby a upozornenia na úrovni koncových zariadení.

11.4 Nariadenie EÚ GDPR

11.4.1 Článok 32(1)(b) – Vyžaduje technické a organizačné opatrenia (napríklad antivírusový softvér) na ochranu osobných údajov.

11.4.2 Článok 33 – Ukladá povinnosť oznámiť porušenie ochrany osobných údajov, ak malvér naruší dôvernosť, integritu alebo dostupnosť údajov.

11.5 Smernica EÚ NIS2

11.5.1 Článok 21(2)(d) – Vyžaduje opatrenia na prevenciu a reakciu na hrozby malvéru v rámci základných a dôležitých subjektov.

11.5.2 Článok 21(2)(e) – Ukladá viacvrstvové stratégie riadenia kybernetických rizík vrátane ochrany koncových zariadení pred malvérom.

11.6 Nariadenie EÚ DORA

11.6.1 Článok 10(1) – Vyžaduje, aby boli systémy IKT chránené pred malvérom a inými hrozbami ako súčasť prevádzkovej odolnosti.

11.6.2 Článok 15 – Ukladá finančným organizáciám povinnosť preverovať ochranu pred malvérom u poskytovateľov služieb tretích strán.

11.7 COBIT 2019

11.7.1 DSS05.02 – Zdôrazňuje ochranné opatrenia na obranu koncových zariadení a sietí pred hrozbami malvéru.

11.7.2 DSS05.04 – Podporuje monitorovanie a upozorňovanie na bezpečnostné udalosti súvisiace s malvérom ako súčasť priebežnej prevádzky.