					Ovdje unesite naziv registrirane pravne osobe							
Broj dokumenta: P20					Naziv dokumenta: **Politika zaštite krajnjih uređaja i zaštite od zlonamjernog softvera**							
Verzija: 1.0		Datum stupanja na snagu: 01.01.2025			Vlasnik dokumenta:							
X	Politika		Standard		Postupak		Obrazac		Registar		Drugo	

Povijest revizija				
Broj revizije	**Datum revizije**	**Promjene**	**Pregledao/la**	**Vlasnik procesa**

Odobrenja			
Ime	**Radno mjesto**	**Datum**	**Potpis**

Usklađeno sa standardima i regulativom

Standard/regulativa	Točka/članak	Napomena
ISO/IEC 27001:2022	Točka 8	Kontrole zaštite krajnjih uređaja i zaštite od zlonamjernog softvera potrebne su za ostvarenje ciljeva ISMS-a
ISO/IEC 27002:2022	Kontrole 8.7, 8	Pruža tehničke kontrole i smjernice za zaštitu od zlonamjernog softvera, zaštitu krajnjih uređaja i upravljanje incidentima
NIST SP 800-53 Rev.5	SI-3, SI-4, CM-6	Definira zaštitu od zlonamjernog koda, centralizirano praćenje i zahtjeve za referentnu konfiguraciju
GDPR EU	Članak 32	Propisuje odgovarajuće tehničke mjere za zaštitu osobnih podataka, uključujući zaštitu od zlonamjernog softvera
Direktiva EU NIS2	Članak 21(2)(d)	Zahtijeva uvođenje mjera za otkrivanje prijetnji i preventivnih mjera na razini krajnjih uređaja
Uredba EU DORA	Članak 9	Zahtijeva upravljanje IKT rizicima radi zaštite od zlonamjernog softvera i prijetnji koje potječu s krajnjih uređaja
COBIT 2019	DSS05.01, DSS01.04, MEA	Propisuje zaštitu, praćenje i procjenu kontrola krajnjih uređaja

1. Svrha

1.1 Ova politika definira obvezne kontrole i operativne zahtjeve za zaštitu krajnjih uređaja organizacije, uključujući stolna i prijenosna računala, mobilne uređaje i poslužitelje, od zlonamjernog softvera i povezanih prijetnji.

1.2 Njome se uspostavljaju minimalni standardi za zaštitu krajnjih uređaja, otkrivanje zlonamjernog softvera, odgovor kroz ograničavanje te nadzor ponašanja, kako bi sustavi ostali otporni na široko rasprostranjene i napredne varijante zlonamjernog softvera.

1.3 Ova politika izravno podupire usklađenost s ISO/IEC 27001:2022, točkom 8.1 i kontrolom 8.7 iz Priloga A te je usklađena s regionalnim obvezama u području kibernetičke sigurnosti prema GDPR-u, NIS2 i DORA-i.

2. Opseg

2.1 Ova politika primjenjuje se na sve krajnje uređaje, uključujući:

2.1.1 stolna i prijenosna računala, mobilne uređaje i virtualne instance u vlasništvu organizacije ili pod upravljanjem organizacije

2.1.2 osobne uređaje odobrene u skladu s Politikom korištenja vlastitih uređaja (BYOD), uz obveznu instalaciju MDM-a ili agenta krajnje točke

2.1.3 poslužitelje i infrastrukturnu imovinu, uključujući virtualne strojeve hostirane u oblaku i uređaje u rubnom okruženju

2.1.4 operacijske sustave, upravljačke programe, lokalne usluge, agente krajnjih točaka i sigurnosne kontrole instalirane na svakom čvoru

2.2 Ova politika obuhvaća svo osoblje s administrativnom, tehničkom ili operativnom odgovornošću za bilo koji krajnji uređaj, uključujući:

2.2.1 interne zaposlenike i ugovorne izvođače

2.2.2 pružatelje upravljanih usluga (MSP), vanjsku podršku za radne stanice i IT administratore trećih strana

2.2.3 korisnike ovlaštene za rad na prijenosnim sustavima, prijenosnim računalima s omogućenim VPN-om ili za mobilni pristup mrežama organizacije

2.3 Obuhvat prijetnji prema ovoj politici uključuje, ali nije ograničen na:

2.3.1 viruse, crve, trojance, ransomware, špijunski softver, rootkite, adware, keyloggere i botnete

2.3.2 zlonamjerni softver bez datoteka, zero-day komponente učitane u memoriju, zlonamjerni softver za eskalaciju privilegija i komplete za iskorištavanje ranjivosti preglednika

2.3.3 zlonamjerni kod isporučen putem prijenosnih medija, phishing vektora, nenamjernih preuzimanja sa zlonamjernih stranica ili napada putem USB-a

3. Ciljevi

3.1 Zaštititi cjelovitost, dostupnost i povjerljivost sustava krajnjih uređaja i podataka koje obrađuju primjenom pouzdanih mjera sprječavanja, otkrivanja i odgovora na zlonamjerni softver.

3.2 Spriječiti izvršavanje ili širenje zlonamjernog koda na mrežama organizacije primjenom tehničkih zaštitnih mjera, sigurnog ojačavanja referentne konfiguracije i telemetrije u stvarnom vremenu.

3.3 Integrirati zaštitu krajnjih uređaja s drugim kontrolama ISMS-a, uključujući upravljanje ranjivostima, kontrolu pristupa, zapisivanje i praćenje te odgovor na incidente.

3.4 Osigurati neprekidnu vidljivost krajnjih uređaja putem centralno upravljanih platformi zaštite, uključujući antivirusni softver / zaštitu od zlonamjernog softvera, otkrivanje i odgovor na krajnjim točkama (EDR) te SIEM telemetriju.

3.5 Ispuniti zakonske, regulatorne i normativne zahtjeve koji propisuju sigurnost krajnjih uređaja, primjerice članak 32 GDPR-a, članak 21 NIS2 i članak 9 DORA-e.

3.6 Definirati odgovorne uloge, propisati SLA-ove za zakrpavanje i odgovor na upozorenja te osigurati revizijsku spremnost putem dokumentiranja i izvješćivanja.

4. Uloge i odgovornosti

4.1 Glavni direktor informacijske sigurnosti (CISO)

4.1.1 Vlasnik je ove politike i osigurava njezinu usklađenost s ISMS-om i ukupnom sigurnosnom strategijom.

4.1.2 Tromjesečno pregledava metrike zaštite krajnjih uređaja, trendove incidenata i učinkovitost alata.

4.1.3 Odobrava iznimke i prihvaćanje preostalog rizika povezanog s obuhvatom zaštite krajnjih uređaja.

4.2 Voditelj sigurnosti krajnjih uređaja / voditelj centra za sigurnosne operacije

4.2.1 Upravlja sustavima za zaštitu krajnjih uređaja, primjerice AV-om, EDR-om i MDM-om.

4.2.2 Nadgleda provedbu politike, podešavanje otkrivanja prijetnji i operativne postupke odgovora.

4.2.3 Održava statistiku obuhvata, evidenciju incidenata sa zlonamjernim softverom i referentne konfiguracije upozorenja.

[... Odjeljci 4.3–8 nisu uključeni u ovaj pregled. Kupite cijeli dokument za pristup potpunom sadržaju. ...]

9. Zahtjevi za pregled i ažuriranje

9.1 Ova politika mora se pregledati najmanje jednom godišnje ili kada:

9.1.1 dođe do velikih kampanja zlonamjernog softvera ili sigurnosnih incidenata na krajnjim uređajima

9.1.2 nove vrste prijetnji, primjerice zlonamjerni softver bez datoteka ili varijante ransomwarea, zahtijevaju ažurirane strategije otkrivanja ili odgovora

9.1.3 platforme za zaštitu krajnjih uređaja ili arhitekture agenata budu značajno promijenjene

9.1.4 budu ažurirani zakonski ili regulatorni zahtjevi koji utječu na kontrole krajnjih uređaja

9.2 Pokretanje pregleda odgovornost je Voditelja sigurnosti krajnjih uređaja, a provodi se u koordinaciji s CISO-om, pravnom funkcijom, funkcijom upravljanja rizicima i revizijom.

9.3 Odobrene izmjene moraju se dokumentirati u registru upravljanja dokumentima ISMS-a, dobiti novi identifikator verzije i biti priopćene svim pogođenim stranama.

9.4 Zamijenjene verzije moraju se arhivirati, pristup njima mora biti ograničen i moraju se zadržati radi cjelovitosti revizijskog traga u skladu s rasporedima zadržavanja ISMS-a.

10. Povezane politike i poveznice

10.1 P1 - Politika informacijske sigurnosti. Uspostavlja temeljna načela za zaštitu sustava, podataka i mreža. Ova politika provodi ta načela na razini krajnjih uređaja kroz tehničke i postupovne kontrole zaštite od zlonamjernog softvera.

10.2 P4 - Politika kontrole pristupa. Definira ograničenja pristupa korisnika koja se provode na razini krajnjih uređaja, uključujući zaštitu od eskalacije privilegija i neovlaštene instalacije neprovjerenog softvera.

10.3 P5 - Politika upravljanja promjenama. Osigurava da ažuriranja softvera za zaštitu krajnjih uređaja, pravila politike ili konfiguracija agenata podliježu odobrenju i kontroliranom procesu uvođenja.

10.4 P12 - Politika upravljanja imovinom. Pruža referentnu osnovu za klasifikaciju imovine i popis imovine potrebnu za vidljivost krajnjih uređaja, obuhvat zakrpavanja i definiranje opsega zaštite od zlonamjernog softvera.

10.5 P22 - Politika bilježenja i praćenja. Omogućuje integraciju upozorenja s krajnjih uređaja, statusa ispravnosti agenata i obavještajnih podataka o prijetnjama u centralizirane SIEM sustave radi otkrivanja u stvarnom vremenu i forenzičke sljedivosti.

10.6 P30 - Politika odgovora na incidente. Povezuje incidente sa zlonamjernim softverom na krajnjim uređajima sa standardiziranim tijekovima rada za ograničavanje, uklanjanje prijetnje, istragu i oporavak, uz dodijeljene uloge i pragove eskalacije.

11. Referentni standardi i okviri

11.1 ISO/IEC 27001:

11.1.1 Točka 8.1 - Operativno planiranje i kontrola: zahtijeva provedbu tehničkih kontrola, uključujući zaštitne mjere za krajnje uređaje, radi održavanja ciljeva ISMS-a.

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

11.2.1 Pruža detaljne tehničke smjernice o mjerama zaštite od zlonamjernog softvera, sigurnom uvođenju softvera, praćenju i spremnosti za incidente u okruženjima krajnjih uređaja.

11.3 NIST SP 800-53 Rev.5:

11.3.1 SI-3 - Zaštita od zlonamjernog koda: zahtijeva uporabu alata za zaštitu od zlonamjernog softvera sa skeniranjem u stvarnom vremenu, skeniranjem pri pristupu i analizom ponašanja.

11.3.2 SI-4 - Praćenje sustava: podupire integraciju telemetrije s centraliziranim platformama za otkrivanje.

11.3.3 CM-6 - Postavke konfiguracije: dodatno osnažuje referentne konfiguracije na krajnjim uređajima, uključujući obveznu primjenu zaštitnih agenata.

11.4 GDPR EU (2016/679):

11.4.1 Članak 32 - Sigurnost obrade: zahtijeva da organizacije provedu odgovarajuće tehničke mjere za zaštitu osobnih podataka, uključujući zaštitu od prijetnji zlonamjernim softverom.

11.5 Direktiva EU NIS2 (2022/2555):

11.5.1 Članak 21(2)(d): obvezuje subjekte na uvođenje mjera za otkrivanje i sprječavanje prijetnji, uključujući mehanizme zaštite od zlonamjernog softvera na razini krajnjih uređaja.

11.6 Uredba EU DORA (2022/2554):

11.6.1 Članak 9 - Zahtjevi za upravljanje IKT rizicima: zahtijeva da financijski subjekti usvoje zaštitne mjere za sprječavanje, otkrivanje i odgovor na zlonamjerni softver i prijetnje koje potječu s krajnjih uređaja.

11.7 COBIT 2019:

11.7.1 DSS05.01 - Zaštita od zlonamjernog softvera: propisuje otkrivanje i ublažavanje zlonamjernog softvera na svim krajnjim uređajima organizacije.

11.7.2 DSS01.04 - Upravljanje dostupnošću i kapacitetom: osigurava da je zaštita od zlonamjernog softvera uravnotežena s performansama sustava i kontinuitetom poslovanja.

11.7.3 MEA03 - Praćenje, vrednovanje i procjena usklađenosti: zahtijeva periodičnu reviziju kontrola krajnjih uređaja i djelotvornosti zaštite.