					Sem vnesite naziv registrirane pravne osebe							
Številka dokumenta: P20					Naslov dokumenta: **Politika zaščite končnih točk / zaščite pred zlonamerno programsko opremo**							
Različica: 1.0		Datum začetka veljavnosti: 01.01.2025			Lastnik dokumenta:							
X	Politika		Standard		Postopek		Obrazec		Register		Drugo	

Zgodovina revizij				
Številka revizije	**Datum revizije**	**Spremembe**	**Pregledal**	**Lastnik procesa**

Odobritve			
Ime	**Delovno mesto**	**Datum**	**Podpis**

Usklajenost s standardi in predpisi

Standard/predpis	Klavzula/člen	Komentar
ISO/IEC 27001:2022	Klavzula 8	Zahtevane so kontrole za zaščito končnih točk in zaščito pred zlonamerno programsko opremo za doseganje ciljev sistema upravljanja informacijske varnosti (ISMS).
ISO/IEC 27002:2022	Kontroli 8.7, 8	Določa tehnične kontrole in usmeritve za zaščito pred zlonamerno programsko opremo, zaščito končnih točk in upravljanje incidentov.
NIST SP 800-53 Rev.5	SI-3, SI-4, CM-6	Opredeljuje zahteve za zaščito pred zlonamerno kodo, centralizirano spremljanje in izhodiščne konfiguracijske zahteve.
Uredba EU GDPR	Člen 32	Zahteva ustrezne tehnične ukrepe za varstvo osebnih podatkov, vključno z zaščito pred zlonamerno programsko opremo.
Direktiva EU NIS2	Člen 21(2)(d)	Zahteva uvedbo zaznavanja groženj na ravni končnih točk in preventivnih ukrepov.
Uredba EU DORA	Člen 9	Zahteva upravljanje tveganj IKT za zaščito pred zlonamerno programsko opremo in grožnjami, ki izvirajo iz končnih točk.
COBIT 2019	DSS05.01, DSS01.04, MEA	Zahteva zaščito, spremljanje in presojo kontrol končnih točk.

1. Namen

1.1 Ta politika določa obvezne kontrole in operativne zahteve za zaščito organizacijskih končnih točk, vključno z namiznimi računalniki, prenosniki, mobilnimi napravami in strežniki, pred zlonamerno programsko opremo in povezanimi grožnjami.

1.2 Določa minimalne standarde za zaščito končnih točk, zaznavanje zlonamerne programske opreme, zajezitveni odziv ter spremljanje vedenja, s čimer zagotavlja, da sistemi ostanejo odporni proti splošno razširjenim in naprednim vrstam zlonamerne programske opreme.

1.3 Ta politika neposredno podpira skladnost s klavzulo 8.1 standarda ISO/IEC 27001:2022 in kontrolo 8.7 Priloge A ter je usklajena z regionalnimi obveznostmi na področju kibernetske varnosti v okviru GDPR, NIS2 in DORA.

2. Področje uporabe

2.1 Ta politika velja za vse končne točke, vključno z:

2.1.1 namiznimi računalniki, prenosniki, mobilnimi napravami in virtualnimi instancami, ki so v lasti organizacije ali jih organizacija upravlja,

2.1.2 napravami v osebni lasti, odobrenimi v skladu s politiko uporabe lastnih naprav, pri čemer je zahtevana namestitev MDM ali agenta končne točke,

2.1.3 strežniki in infrastrukturnimi sredstvi, vključno z virtualnimi stroji, gostovanimi v oblaku, in robnimi napravami,

2.1.4 operacijskimi sistemi, gonilniki, lokalnimi storitvami, agenti končnih točk in varnostnimi kontrolami, nameščenimi na posameznem vozlišču.

2.2 Ta politika velja za vse osebe z administrativno, tehnično ali operativno odgovornostjo za katero koli končno točko, vključno z:

2.2.1 notranjimi zaposlenimi in pogodbenimi izvajalci,

2.2.2 ponudniki upravljanih storitev (MSP), zunanjimi izvajalci podpore namiznim sistemom in skrbniki IT tretjih oseb,

2.2.3 uporabniki, pooblaščenimi za uporabo prenosnih sistemov, prenosnikov z omogočenim VPN ali mobilnega dostopa do organizacijskih omrežij.

2.3 Obseg groženj po tej politiki med drugim vključuje:

2.3.1 viruse, črve, trojance, izsiljevalsko programsko opremo, vohunsko programsko opremo, rootkite, oglaševalsko programsko opremo, zapisovalnike tipk in botnete,

2.3.2 zlonamerno programsko opremo brez datotek, obremenitve tipa zero-day, zlonamerno programsko opremo za povišanje privilegijev in komplete za izrabo ranljivosti v brskalnikih,

2.3.3 zlonamerno kodo, dostavljeno prek izmenljivih medijev, vektorjev lažnega predstavljanja, nenamernih prenosov ob obisku spletnih mest ali napadov prek USB.

3. Cilji

3.1 Zaščititi celovitost, razpoložljivost in zaupnost sistemov končnih točk ter podatkov, ki jih obdelujejo, z zanesljivim preprečevanjem, zaznavanjem in odzivanjem na zlonamerno programsko opremo.

3.2 Preprečiti izvajanje ali širjenje zlonamerne kode v organizacijskih omrežjih z uveljavitvijo tehničnih varoval, izhodiščnega utrjevanja in telemetrije v realnem času.

3.3 Zaščito končnih točk vključiti v druge kontrole ISMS, vključno z upravljanjem ranljivosti, nadzorom dostopa, beleženjem in spremljanjem ter odzivanjem na incidente.

3.4 Zagotoviti neprekinjeno vidljivost nad končnimi točkami s centralno upravljanimi platformami zaščite, vključno z antivirusnimi/antimalware agenti, zaznavanjem in odzivanjem na končnih točkah (EDR) ter telemetrijo SIEM.

3.5 Zagotoviti skladnost s pravnimi, regulativnimi in standardnimi zahtevami, ki predpisujejo varnost končnih točk (npr. člen 32 GDPR, člen 21 NIS2, člen 9 DORA).

3.6 Določiti odgovorne vloge, uveljaviti sporazume o ravni storitev (SLA) za nameščanje popravkov in odzivanje na opozorila ter zagotoviti revizijsko pripravljenost z ustrezno dokumentacijo in poročanjem.

4. Vloge in odgovornosti

4.1 vodja informacijske varnosti (CISO)

4.1.1 Je lastnik te politike in zagotavlja njeno usklajenost z ISMS ter celotno varnostno strategijo.

4.1.2 Četrtletno pregleduje kazalnike zaščite končnih točk, trende incidentov in učinkovitost orodij.

4.1.3 Odobri izjeme in sprejem preostalega tveganja v zvezi s pokritostjo končnih točk.

4.2 vodja varnosti končnih točk / vodja SOC

4.2.1 Upravlja sisteme za zaščito končnih točk (npr. AV, EDR, MDM).

4.2.2 Nadzira izvajanje politike, prilagajanje zaznavanja groženj in odzivne priročnike.

4.2.3 Vzdržuje statistiko pokritosti, evidence incidentov zlonamerne programske opreme in izhodiščne konfiguracije opozoril.

[... Razdelki 4.3–8 niso vključeni v ta predogled. Kupite celoten dokument za dostop do celotne vsebine. ...]

9. Zahteve za pregled in posodobitev

9.1 To politiko je treba pregledati letno ali kadar:

9.1.1 pride do večjih kampanj zlonamerne programske opreme ali varnostnih incidentov na končnih točkah,

9.1.2 nove vrste groženj (npr. zlonamerna programska oprema brez datotek, različice izsiljevalske programske opreme) zahtevajo posodobljene strategije zaznavanja ali odzivanja,

9.1.3 se platforme za zaščito končnih točk ali arhitekture agentov bistveno spremenijo,

9.1.4 se posodobijo pravne ali regulativne zahteve, ki vplivajo na kontrole končnih točk.

9.2 Pregled mora začeti vodja varnosti končnih točk in ga uskladiti z vodjo informacijske varnosti (CISO), pravno funkcijo, funkcijo upravljanja tveganj in revizijsko funkcijo.

9.3 Odobrene spremembe morajo biti dokumentirane v registru nadzora dokumentov ISMS, prejeti nov identifikator različice in biti sporočene vsem relevantnim deležnikom.

9.4 Nadomeščene različice morajo biti arhivirane, z omejenim dostopom, in hranjene zaradi zagotavljanja celovitosti revizijske sledi v skladu z roki hrambe ISMS.

10. Povezane politike in povezave

10.1 P1 - Politika informacijske varnosti. Določa temeljna načela za zaščito sistemov, podatkov in omrežij. Ta politika ta načela na ravni končnih točk uveljavlja s tehničnimi in postopkovnimi kontrolami za zaščito pred zlonamerno programsko opremo.

10.2 P4 - Politika nadzora dostopa. Določa omejitve uporabniškega dostopa, ki se uveljavljajo na ravni končnih točk, vključno z zaščito pred povišanjem privilegijev in nepooblaščenimi namestitvami nepreverjene programske opreme.

10.3 P5 - Politika upravljanja sprememb. Zagotavlja, da so posodobitve programske opreme za zaščito končnih točk, pravil politik ali konfiguracij agentov predmet odobritve in nadzorovanih postopkov uvajanja.

10.4 P12 - Politika upravljanja sredstev. Določa razvrščanje sredstev in izhodiščni popis, ki sta potrebna za vidljivost končnih točk, pokritost s popravki in opredelitev obsega zaščite pred zlonamerno programsko opremo.

10.5 P22 - Politika beleženja in spremljanja. Omogoča vključitev opozoril končnih točk, operativnega stanja agentov in obveščevalnih podatkov o grožnjah v centralizirane sisteme SIEM za zaznavanje v realnem času in forenzično sledljivost.

10.6 P30 - Politika odzivanja na incidente. Povezuje incidente zlonamerne programske opreme na ravni končnih točk s standardiziranimi delovnimi tokovi za zajezitev, odstranitev, preiskavo in obnovitev z dodeljenimi vlogami in pragovi eskalacije.

11. Referenčni standardi in okviri

11.1 ISO/IEC 27001:

11.1.1 Klavzula 8.1 - operativno načrtovanje in nadzor: zahteva uvedbo tehničnih kontrol, vključno z varovali končnih točk, za ohranjanje ciljev ISMS.

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

11.2.1 Podaja podrobne tehnične usmeritve glede ukrepov za zaščito pred zlonamerno programsko opremo, varnega uvajanja programske opreme, spremljanja in pripravljenosti na incidente v okoljih končnih točk.

11.3 NIST SP 800-53 Rev.5:

11.3.1 SI-3 - zaščita pred zlonamerno kodo: zahteva uporabo orodij za zaščito pred zlonamerno programsko opremo s pregledovanjem v realnem času, pregledovanjem ob dostopu in analizo vedenja.

11.3.2 SI-4 - spremljanje sistemov: podpira integracijo telemetrije s centraliziranimi platformami zaznavanja.

11.3.3 CM-6 - nastavitve konfiguracije: krepi izhodiščne konfiguracijske nastavitve na končnih točkah, vključno z uveljavitvijo zaščitnih agentov.

11.4 Uredba EU GDPR (2016/679):

11.4.1 Člen 32 - varnost obdelave: zahteva, da organizacije uvedejo ustrezne tehnične ukrepe za varstvo osebnih podatkov, vključno z zaščito pred grožnjami zlonamerne programske opreme.

11.5 Direktiva EU NIS2 (2022/2555):

11.5.1 Člen 21(2)(d): zavezance obvezuje k uvedbi ukrepov za zaznavanje in preprečevanje groženj, vključno z mehanizmi zaščite pred zlonamerno programsko opremo na ravni končnih točk.

11.6 Uredba EU DORA (2022/2554):

11.6.1 Člen 9 - zahteve za upravljanje tveganj IKT: zahteva, da finančni subjekti sprejmejo zaščitne ukrepe za preprečevanje, zaznavanje in odzivanje na zlonamerno programsko opremo ter grožnje, ki izvirajo iz končnih točk.

11.7 COBIT 2019:

11.7.1 DSS05.01 - zaščita pred zlonamerno programsko opremo: zahteva zaznavanje in ublažitev zlonamerne programske opreme na vseh organizacijskih končnih točkah.

11.7.2 DSS01.04 - upravljanje razpoložljivosti in zmogljivosti: zagotavlja, da je zaščita pred zlonamerno programsko opremo uravnotežena s sistemsko zmogljivostjo in neprekinjenim poslovanjem.

11.7.3 MEA03 - spremljanje, vrednotenje in presoja skladnosti: zahteva periodično revizijo kontrol končnih točk in učinkovitosti zaščite.