					Sem vnesite naziv registrirane pravne osebe							
Številka dokumenta: P20S					Naslov dokumenta: **Politika zaščite končnih točk 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	Clause 8	Operativne kontrole za zaščito pred zlonamerno programsko opremo
ISO/IEC 27002:2022	Kontrola 8	Kontrolni ukrepi za zaščito končnih točk
NIST SP 800-53 Rev.5	SI-3, SI-4	Zaščita pred zlonamerno kodo in odzivanje na incidente
Direktiva EU NIS2	Člen 21(2)(d), (e)	Zlonamerna programska oprema in obvladovanje tveganj za bistvene in pomembne subjekte
Uredba EU DORA	Člen 10(1), 15	Operativna odpornost in preverjanje tretjih oseb
COBIT 2019	DSS05.02, DSS05.04	Zaščita končnih točk in omrežja ter spremljanje
Uredba EU GDPR	Člen 32(1)(b), 33	Tehnični in organizacijski ukrepi ter prijava kršitev

1. Namen

1.1 Ta politika določa minimalne tehnične, postopkovne in vedenjske zahteve za zaščito vseh končnih točk, kot so prenosni in namizni računalniki, mobilne naprave ter prenosni mediji, pred zlonamerno kodo, vključno z virusi, izsiljevalsko programsko opremo, vohunsko programsko opremo, rootkiti in drugimi grožnjami zlonamerne programske opreme.

1.2 Njen namen je zagotoviti, da so končne točke opremljene, vzdrževane in uporabljane na način, ki zmanjšuje tveganje okužbe z zlonamerno programsko opremo, njenega širjenja in kompromitacije sistemov.

1.3 Organizacija priznava, da so končne točke pogoste vstopne točke za zlonamerno programsko opremo, zato morajo biti varnostno utrjene, spremljane in zaščitene z uporabo večplastne obrambe.

1.4 Politika podpira cilje certificiranja organizacije po standardu ISO/IEC 27001:2022 ter je usklajena z Uredbo EU GDPR, Direktivo EU NIS2, Uredbo EU DORA in drugimi relevantnimi okviri.

2. Področje uporabe

2.1 Ta politika se uporablja za:

2.1.1 vse končne točke organizacije, vključno z namiznimi računalniki, prenosnimi računalniki, tablicami, mobilnimi telefoni in terminali na prodajnih mestih,

2.1.2 naprave v osebni lasti, ki se uporabljajo za dostop do poslovnih aplikacij ali podatkov,

2.1.3 odstranljive pomnilniške naprave, kot so USB-ključi in zunanji trdi diski,

2.1.4 vse operacijske sisteme, programsko opremo za končne točke ali komunikacijska orodja, ki delujejo na teh platformah.

2.2 Uporablja se enako za:

2.2.1 notranje osebje, pogodbene izvajalce, praktikante in ponudnike upravljanih storitev (MSP),

2.2.2 naprave, ki se uporabljajo na lokaciji, na daljavo ali v okviru hibridnih oblik dela,

2.2.3 s storitvami v oblaku povezane ali nepovezane končne točke, ki hranijo poslovne informacije ali osebne podatke.

3. Cilji

3.1 Preprečiti okužbo z zlonamerno programsko opremo in njeno širjenje prek notranjih sistemov, uporabniških naprav in zunanjih povezav.

3.2 Hitro zaznati in zajeziti grožnje, povezane z zlonamerno programsko opremo, z uporabo avtomatiziranih tehnologij za varnost končnih točk in določenih eskalacijskih poti.

3.3 Zagotoviti, da se za dostop do poslovnih informacij uporabljajo samo pooblaščene, ustrezno zaščitene in spremljane naprave.

3.4 Določiti jasne odgovornosti zaposlenih in pravila ravnanja uporabnikov za zmanjšanje tveganja incidentov, povezanih z zlonamerno programsko opremo.

3.5 Vzdrževati sledljive in za revizijo primerne zapise o zaznavah zlonamerne programske opreme, odzivih in skladnosti s to politiko.

3.6 Zaščititi osebne in poslovne podatke pred kompromitacijo zaradi zlonamerne programske opreme z uporabo strategij večplastne obrambe.

4. Vloge in odgovornosti

4.1 Generalni direktor

4.1.1 Je lastnik te politike in zagotavlja, da so za zaščito končnih točk na voljo zadostni viri.

4.1.2 Odobri protivirusno programsko opremo, orodja za upravljanje mobilnih naprav (MDM) in pravila dostopa tretjih oseb.

4.1.3 Pregleduje poročila o incidentih z zlonamerno programsko opremo, povzetke vpliva in obvestila o kršitvah, ki vključujejo končne točke.

4.2 Ponudnik IT-podpore / notranji skrbnik IT

4.2.1 Izbere in uvede protivirusno programsko opremo, programsko opremo za zaščito pred zlonamerno programsko opremo ter rešitve za zaznavanje in odzivanje na končnih točkah (EDR).

4.2.2 Zagotavlja dosledno nameščanje posodobitev in hrambo dnevniških zapisov.

4.2.3 Se odziva na opozorila o zlonamerni programski opremi, izolira okužene sisteme in izvaja odpravo posledic.

4.2.4 Uveljavlja kontrole nad uporabo USB-naprav in zunanjih naprav.

[... 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 Zahteva za letni pregled

9.1.1 To politiko morajo generalni direktor, ponudnik IT-podpore in koordinator za zasebnost formalno pregledati najmanj enkrat letno.

9.2 Posodobitve na podlagi sprožilcev

9.2.1 Politiko je treba posodobiti tudi, kadar:

9.2.1.1 nova pomembna grožnja zlonamerne programske opreme ali njen izbruh cilja na končne točke, ki jih uporablja organizacija,

9.2.1.2 se protivirusna ali EDR-orodja spremenijo, nadgradijo ali zamenjajo,

9.2.1.3 incident z zlonamerno programsko opremo razkrije pomanjkljivosti v področju uporabe ali izvajanju te politike,

9.2.1.4 se posodobijo pravne ali regulativne zahteve (npr. GDPR, DORA, NIS2).

9.3 Nadzor različic in obveščanje

9.3.1 Vse spremembe politike morajo biti dokumentirane s številko različice, datumom in povzetkom sprememb.

9.3.2 Zaposlene je treba obvestiti o posodobitvah, zlasti če te spreminjajo operativne ali vedenjske zahteve.

9.3.3 Predhodne različice je treba hraniti v arhivu politik najmanj 3 leta za podporo revizijam.

10. Povezane politike in povezave

10.1 Ta politika se mora izvajati skupaj z naslednjimi SME-politikami:

10.1.1 P9S – Politika dela na daljavo: zagotavlja, da se zahteve za zaščito končnih točk uveljavljajo na napravah, ki se uporabljajo zunaj lokacije ali v hibridnih oblikah dela.

10.1.2 P12S – Politika upravljanja sredstev: podpira sledenje in nadzor nad vsemi končnimi točkami ter zagotavlja, da se uporabljajo samo pooblaščene in zaščitene naprave.

10.1.3 P17S – Politika varstva podatkov in zasebnosti: krepi preprečevanje zlonamerne programske opreme kot ključno kontrolo zasebnosti za zaščito osebnih in občutljivih podatkov pred kompromitacijo.

10.1.4 P22S – Politika beleženja in spremljanja: določa zahteve za beleženje dogodkov zlonamerne programske opreme in zagotavljanje vidnosti opozoril za zgodnje odzivanje.

10.1.5 P30S – Politika odzivanja na incidente: določa eskalacijo, zajezitev in korake zunanjega obveščanja, če zlonamerna programska oprema povzroči kompromitacijo podatkov ali operativno motnjo.

11. Referenčni standardi in okviri

11.1 ISO/IEC 27001

11.1.1 Klavzula 8.1 – zahteva uvedbo operativnih kontrol za zmanjšanje tveganj, kot so napadi z zlonamerno programsko opremo.

11.2 ISO/IEC 27002

11.2.1 Kontrola 8.7 – podrobno določa prakse obvladovanja zlonamerne programske opreme, vključno s protivirusno programsko opremo, pregledovanjem v realnem času, posodobitvami in usposabljanjem uporabnikov.

11.3 NIST SP 800-53 Rev.5

11.3.1 SI-3 – zahteva uvedbo mehanizmov za zaščito pred zlonamerno kodo na vseh končnih točkah.

11.3.2 SI-4 – določa spremljanje, zaznavanje, analizo in odzivne ukrepe za grožnje in opozorila na ravni končnih točk.

11.4 Uredba EU GDPR

11.4.1 Člen 32(1)(b) – zahteva tehnične in organizacijske kontrole (kot je protivirusna programska oprema) za zaščito osebnih podatkov.

11.4.2 Člen 33 – določa obveznost prijave kršitve, kadar zlonamerna programska oprema ogrozi celovitost, zaupnost ali razpoložljivost podatkov.

11.5 Direktiva EU NIS2

11.5.1 Člen 21(2)(d) – zahteva ukrepe za preprečevanje in odzivanje na grožnje zlonamerne programske opreme pri bistvenih in pomembnih subjektih.

11.5.2 Člen 21(2)(e) – določa večplastne strategije obvladovanja tveganj kibernetske varnosti, vključno z zaščito končnih točk pred zlonamerno programsko opremo.

11.6 Uredba EU DORA

11.6.1 Člen 10(1) – zahteva, da so sistemi IKT zaščiteni pred zlonamerno programsko opremo in drugimi grožnjami kot del operativne odpornosti.

11.6.2 Člen 15 – finančnim organizacijam nalaga preverjanje zaščite pred zlonamerno programsko opremo pri ponudnikih storitev tretjih oseb.

11.7 COBIT 2019

11.7.1 DSS05.02 – poudarja zaščitne ukrepe za obrambo končnih točk in omrežij pred grožnjami zlonamerne programske opreme.

11.7.2 DSS05.04 – podpira spremljanje in opozarjanje na varnostne dogodke, povezane z zlonamerno programsko opremo, kot del stalnega delovanja.