					Ovdje unesite naziv registrirane pravne osobe							
Broj dokumenta: P20S					Naziv dokumenta: **Politika zaštite krajnjih uređaja 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 propisima

Standard/regulativa	Točka/članak	Napomena
ISO/IEC 27001:2022	Točka 8	Operativne kontrole za zaštitu od zlonamjernog softvera
ISO/IEC 27002:2022	Kontrola 8	Kontrolne mjere za zaštitu krajnjih uređaja
NIST SP 800-53 Rev.5	SI-3, SI-4	Zaštita od zlonamjernog koda i odgovor na incidente
EU NIS2	Članci 21(2)(d), (e)	Zaštita od zlonamjernog softvera i upravljanje rizicima za ključne/važne subjekte
EU DORA	Članci 10(1), 15	Operativna otpornost i provjera trećih strana
COBIT 2019	DSS05.02, DSS05.04	Zaštita krajnjih uređaja/mreže i praćenje
EU GDPR	Članci 32(1)(b), 33	Tehničke/organizacijske mjere i obavješćivanje o povredi podataka

1. Svrha

1.1 Ova politika utvrđuje minimalne tehničke, proceduralne i ponašajne zahtjeve za zaštitu svih krajnjih uređaja, kao što su prijenosna i stolna računala, mobilni uređaji i prijenosni mediji, od zlonamjernog koda, uključujući viruse, ransomware, špijunski softver, rootkite i druge prijetnje zlonamjernim softverom.

1.2 Svrha ove politike jest osigurati da su krajnji uređaji opremljeni, održavani i korišteni na način kojim se smanjuje rizik od zaraze zlonamjernim softverom, njegova širenja i kompromitacije sustava.

1.3 Organizacija prepoznaje da su krajnji uređaji česte ulazne točke za zlonamjerni softver te se stoga moraju sigurnosno očvrsnuti, nadzirati i štititi primjenom višeslojne obrane.

1.4 Ova politika podupire ciljeve certifikacije organizacije prema normi ISO/IEC 27001:2022 te je usklađena s Općom uredbom o zaštiti podataka (GDPR), Direktivom EU NIS2, Uredbom EU DORA i drugim relevantnim okvirima.

2. Područje primjene

2.1 Ova politika primjenjuje se na:

2.1.1 sve krajnje uređaje organizacije, uključujući stolna računala, prijenosna računala, tablete, mobilne telefone i POS terminale

2.1.2 privatne uređaje (BYOD) koji se koriste za pristup poslovnim aplikacijama ili podacima

2.1.3 prijenosne medije za pohranu, kao što su USB memorije i vanjski tvrdi diskovi

2.1.4 sve operacijske sustave, softver za krajnje uređaje i komunikacijske alate koji se izvršavaju na tim platformama

2.2 Ova politika jednako se primjenjuje na:

2.2.1 interno osoblje, vanjske suradnike, pripravnike i pružatelje upravljanih usluga

2.2.2 uređaje koji se koriste na lokaciji organizacije, na daljinu ili u hibridnom načinu rada

2.2.3 krajnje uređaje povezane s oblakom ili izvan mreže koji pohranjuju poslovne ili osobne podatke

3. Ciljevi

3.1 Spriječiti zarazu zlonamjernim softverom i njegovo širenje unutar internih sustava, korisničkih uređaja i vanjskih veza

3.2 Brzo otkriti i obuzdati prijetnje povezane sa zlonamjernim softverom primjenom automatiziranih tehnologija zaštite krajnjih uređaja i definiranih putova eskalacije

3.3 Osigurati da se za pristup poslovnim informacijama koriste samo odobreni, zaštićeni i nadzirani uređaji

3.4 Uspostaviti jasne odgovornosti zaposlenika i pravila ponašanja korisnika radi smanjenja rizika od incidenata povezanih sa zlonamjernim softverom

3.5 Održavati sljedive i revizijski provjerljive zapise o otkrivanju zlonamjernog softvera, odgovoru i usklađenosti s politikom

3.6 Zaštititi osobne i poslovne podatke od kompromitacije uzrokovane zlonamjernim softverom primjenom strategija višeslojne obrane

4. Uloge i odgovornosti

4.1 Glavni direktor (GM)

4.1.1 Odgovoran je za ovu politiku i osigurava dostupnost dostatnih resursa za zaštitu krajnjih uređaja

4.1.2 Odobrava antivirusni softver, alate za upravljanje mobilnim uređajima (MDM) i pravila pristupa trećih strana

4.1.3 Pregledava izvješća o incidentima povezanima sa zlonamjernim softverom, sažetke učinaka i obavijesti o povredi podataka koje uključuju krajnje uređaje

4.2 Pružatelj IT podrške / interni IT administrator

4.2.1 Odabire i uvodi antivirusni i antimalware softver te rješenja za otkrivanje i odgovor na prijetnje na krajnjim uređajima (EDR)

4.2.2 Osigurava dosljednu primjenu nadogradnji i zadržavanje zapisnika

4.2.3 Postupa po upozorenjima na zlonamjerni softver, izolira zaražene sustave i provodi otklanjanje posljedica

4.2.4 Provodi kontrole nad korištenjem USB uređaja i vanjskih medija

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

9. Zahtjevi za pregled i ažuriranje

9.1 Zahtjev za godišnji pregled

9.1.1 Ovu politiku mora formalno pregledati najmanje jednom godišnje glavni direktor, u koordinaciji s pružateljem IT podrške i koordinatorom za privatnost

9.2 Ažuriranja na temelju okidača

9.2.1 Politika se mora ažurirati i kada:

9.2.1.1 nova značajna prijetnja zlonamjernim softverom ili izbijanje zaraze cilja krajnje uređaje koje koristi organizacija

9.2.1.2 antivirusni ili EDR alati budu promijenjeni, nadograđeni ili zamijenjeni

9.2.1.3 incident povezan sa zlonamjernim softverom otkrije slabosti u području primjene ove politike ili u njezinoj provedbi

9.2.1.4 se promijene zakonski ili regulatorni zahtjevi (npr. GDPR, DORA, NIS2)

9.3 Upravljanje verzijama i komunikacija

9.3.1 Sve promjene politike moraju biti dokumentirane brojem verzije, datumom i sažetkom promjena

9.3.2 Zaposlenici moraju biti obaviješteni o ažuriranjima, osobito ako se njima mijenjaju operativni ili ponašajni zahtjevi

9.3.3 Prethodne verzije moraju se čuvati u arhivi politika najmanje 3 godine kao podrška revizijama

10. Povezane politike i upućivanja

10.1 Ova politika mora se provoditi zajedno sa sljedećim SME politikama:

10.1.1 P9S – Politika rada na daljinu: osigurava provedbu zahtjeva zaštite krajnjih uređaja na uređajima koji se koriste izvan lokacije ili u hibridnom načinu rada

10.1.2 P12S – Politika upravljanja imovinom: podupire praćenje i kontrolu svih krajnjih uređaja te osigurava da se koriste samo odobreni i zaštićeni uređaji

10.1.3 P17S – Politika zaštite podataka i privatnosti: potvrđuje sprječavanje zlonamjernog softvera kao ključnu kontrolu privatnosti za zaštitu osobnih i osjetljivih podataka od kompromitacije

10.1.4 P22S – Politika zapisivanja događaja i praćenja: utvrđuje zahtjeve za zapisivanje događaja povezanih sa zlonamjernim softverom i održavanje vidljivosti upozorenja radi pravodobnog odgovora

10.1.5 P30S – Politika odgovora na incidente: definira korake eskalacije, obuzdavanja i vanjskog obavješćivanja ako zlonamjerni softver dovede do kompromitacije podataka ili operativnog poremećaja

11. Referentni standardi i okviri

11.1 ISO/IEC 27001

11.1.1 Točka 8.1 – Zahtijeva provedbu operativnih kontrola radi smanjenja rizika kao što su napadi zlonamjernim softverom

11.2 ISO/IEC 27002

11.2.1 Kontrola 8.7 – Detaljno propisuje prakse kontrole zlonamjernog softvera, uključujući antivirus, skeniranje u stvarnom vremenu, nadogradnje i osposobljavanje korisnika

11.3 NIST SP 800-53 Rev.5

11.3.1 SI-3 – Zahtijeva uvođenje mehanizama zaštite od zlonamjernog koda na krajnjim uređajima

11.3.2 SI-4 – Propisuje praćenje, otkrivanje, analizu i aktivnosti odgovora na prijetnje i upozorenja na razini krajnjih uređaja

11.4 EU GDPR

11.4.1 Članak 32(1)(b) – Zahtijeva tehničke i organizacijske kontrole (kao što je antivirus) za zaštitu osobnih podataka

11.4.2 Članak 33 – Propisuje obavješćivanje o povredi podataka kada zlonamjerni softver ugrozi cjelovitost, povjerljivost ili dostupnost podataka

11.5 Direktiva EU NIS2

11.5.1 Članak 21(2)(d) – Zahtijeva mjere za sprječavanje i odgovor na prijetnje zlonamjernim softverom unutar ključnih i važnih subjekata

11.5.2 Članak 21(2)(e) – Propisuje višeslojne strategije upravljanja kibernetičkim rizicima, uključujući zaštitu krajnjih uređaja od zlonamjernog softvera

11.6 Uredba EU DORA

11.6.1 Članak 10(1) – Zahtijeva zaštitu IKT sustava od zlonamjernog softvera i drugih prijetnji kao dijela operativne otpornosti

11.6.2 Članak 15 – Obvezuje financijske organizacije na provjeru zaštite od zlonamjernog softvera kod pružatelja usluga trećih strana

11.7 COBIT 2019

11.7.1 DSS05.02 – Naglašava zaštitne mjere za obranu krajnjih uređaja i mreža od prijetnji zlonamjernim softverom

11.7.2 DSS05.04 – Podupire praćenje i upozoravanje na sigurnosne događaje povezane sa zlonamjernim softverom kao dio tekućih operacija