					Ovdje unesite naziv registrirane pravne osobe							
Broj dokumenta: P22S					Naziv dokumenta: **Politika evidentiranja i praćenja**							
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**

Usklađenost sa standardima i regulativom

Standard/regulativa	Točka/članak	Napomena
ISO/IEC 27001:2022	Točka 8	Operativne kontrole, uključujući evidentiranje
ISO/IEC 27002:2022	Kontrole 8.15, 8.16, 8.17	Evidentiranje događaja, zaštita i praćenje
NIST SP 800-53 Rev.5	AU-2 do AU-12, SI-4	Sadržaj i pregled revizijskih zapisa, zadržavanje, otkrivanje anomalija, upozoravanje
GDPR EU	Članci 5(1)(f), 32, 33	Povjerljivost i cjelovitost podataka, tehničke mjere i obavješćivanje o povredi
Direktiva EU NIS2	Članci 21(2)(d), 23	Mehanizmi evidentiranja za anomalije i prijavu incidenata u roku od 24 sata
Uredba EU DORA	Članci 10, 15	Operativna otpornost, praćenje i evidentiranje pružatelja usluga
COBIT 2019	DSS01.03, DSS05.02	Sljedivost aktivnosti i zaštita putem evidentiranja i praćenja

1. Svrha

1.1 Ova politika uspostavlja obvezne kontrole evidentiranja i praćenja radi osiguravanja sigurnosti, odgovornosti i operativne cjelovitosti IT sustava organizacije.

1.2 Njome se utvrđuju vrste događaja koji se moraju evidentirati, način pohrane zapisnika, način njihova pregleda te odgovornosti osoblja i pružatelja usluga.

1.3 Evidentiranje i praćenje podupiru otkrivanje prijetnji, usklađenost s regulatornim zahtjevima, odgovor na incidente i forenzičku analizu.

1.4 Ova politika omogućuje organizaciji ispunjavanje zahtjeva za operativne kontrole iz norme ISO/IEC 27001 te podupire trajnu revizijsku spremnost, povjerenje klijenata i usklađenost s GDPR-om, NIS2 i DORA-om.

2. Područje primjene

2.1 Ova politika primjenjuje se na sve sustave i sve korisnike unutar organizacije, uključujući:

2.1.1 radne stanice, prijenosna računala, poslužitelje, vatrozide, preklopnike, usmjernike i bežične pristupne točke

2.1.2 usluge u oblaku koje se koriste za poslovne operacije (npr. e-pošta, pohrana datoteka, sigurnosne kopije, alati za suradnju)

2.1.3 funkcije evidentiranja na antivirusnom softveru, aplikacijama, operativnim sustavima i mrežnoj opremi

2.1.4 sve zaposlenike, ugovorne izvođače i pružatelje upravljanih usluga (MSP) koji koriste ili administriraju sustave

2.1.5 sve lokacije na kojima se koriste IT sustavi organizacije, uključujući udaljena, hibridna ili BYOD okruženja

2.2 Ova politika primjenjuje se i na zapisnike koje generiraju usluge trećih strana kada organizacija ima administrativni pristup ili ugovorna prava na reviziju.

3. Ciljevi

3.1 Osigurati evidentiranje aktivnosti sustava, uključujući autentifikaciju, promjene konfiguracije, pristup osjetljivim podacima i sigurnosna upozorenja

3.2 Održavati sigurne i točne zapisnike radi otkrivanja kršenja politike, pogrešaka sustava ili neovlaštenih radnji

3.3 Omogućiti brz pregled zapisnika tijekom incidenata, istraga i revizija

3.4 Poduprijeti vremensku sinkronizaciju radi osiguravanja cjelovitosti i korelacije podataka iz zapisnika

3.5 Zaštititi zapisnike od neovlaštene izmjene, gubitka ili prijevremenog brisanja

3.6 Ispuniti zakonske i regulatorne obveze u pogledu odgovornosti sustava, sljedivosti i odgovora na povrede

4. Uloge i odgovornosti

4.1 glavni direktor (GM)

4.1.1 odobrava ovu politiku i osigurava njezinu provedbu u svim poslovnim sustavima

4.1.2 pregledava upozorenja visoke ozbiljnosti i značajne revizijske nalaze koje prijave IT ili funkcije privatnosti

4.1.3 daje konačno odobrenje za iznimke kada se evidentiranje ili zadržavanje ne mogu tehnički provesti

4.2 pružatelj IT podrške / interna IT funkcija

4.2.1 provodi i konfigurira evidentiranje za operativne sustave, mrežne uređaje, antivirusne alate i ključne aplikacije

4.2.2 osigurava da se zapisnici zadržavaju, sigurnosno kopiraju i štite od izmjena

4.2.3 pregledava zapisnike prema utvrđenom rasporedu i istražuje sumnjive ili neovlaštene aktivnosti

4.2.4 održava sustave upozoravanja koji označavaju anomalno ponašanje ili pokazatelje kompromitacije

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

9. Zahtjevi za pregled i ažuriranje

9.1 Godišnji pregled

9.1.1 Ovu politiku mora pregledati najmanje jednom godišnje glavni direktor uz podršku pružatelja IT podrške i koordinatora za privatnost.

9.2 Okidači za pregled

9.2.1 Izvanredni pregledi moraju se provesti kao odgovor na:

9.2.1.1 nalaze povezane sa zapisnicima iz unutarnjih ili vanjskih revizija

9.2.1.2 sigurnosne incidente u kojima su zapisnici nedostajali, bili oštećeni ili nedostatni

9.2.1.3 značajne promjene IT infrastrukture (npr. migracija na platforme za evidentiranje u oblaku)

9.2.1.4 ažuriranja zakonskih ili regulatornih obveza (npr. GDPR, NIS2, DORA)

9.3 upravljanje verzijama

9.3.1 Sve promjene ove politike moraju se evidentirati uz broj verzije, datum i sažetak izmjena

9.3.2 Prethodne verzije moraju se arhivirati i čuvati najmanje 3 godine

9.3.3 Ažurirane politike moraju se priopćiti dionicima na koje utječu, osobito onima s pristupom na razini sustava

10. Povezane politike i poveznice

10.1 Ova politika izravno podupire i povezana je sa sljedećim SME politikama informacijske sigurnosti:

10.1.1 P17S – Politika zaštite podataka i privatnosti: osigurava da se zapisima koji sadrže osobne podatke upravlja uz mjere zaštite cjelovitosti, zadržavanja i pristupa u skladu sa zahtjevima GDPR-a.

10.1.2 P21S – Politika mrežne sigurnosti: pruža osnovu za prikupljanje zapisnika povezanih s vatrozidima, bežičnim pristupom, VPN-ovima i praćenjem segmentacije.

10.1.3 P24S – Politika sigurnog razvoja: osigurava da su zapisnici aplikacija (npr. za pokušaje prijave, pogreške i iznimke) ugrađeni u dizajn i rad softvera.

10.1.4 P30S – Politika odgovora na incidente: oslanja se na točne i potpune podatke iz zapisnika radi otkrivanja, analize i odgovora na događaje informacijske sigurnosti.

10.1.5 P23S – Politika vremenske sinkronizacije: osigurava dosljedne i sljedive vremenske oznake u svim sustavima, što omogućuje korelaciju zapisnika tijekom istraga.

11. Referentni standardi i okviri

11.1 ISO/IEC 27001

11.1.1 Točka 8.1 – zahtijeva provedbu operativnih kontrola radi ublažavanja rizika informacijske sigurnosti, uključujući evidentiranje.

11.2 ISO/IEC 27002

11.2.1 Kontrola 8.15 – zahtijeva evidentiranje događaja radi podrške otkrivanju anomalija i odgovornosti.

11.2.2 Kontrola 8.16 – zahtijeva zaštitu zapisnika od neovlaštene izmjene i neovlaštenog pristupa.

11.2.3 Kontrola 8.17 – zahtijeva praćenje sustava radi otkrivanja neuobičajenih aktivnosti i potvrđivanja djelotvornosti kontrola praćenja.

11.3 NIST SP 800-53 Rev.5

11.3.1 AU-2 do AU-12 – obuhvaćaju sadržaj revizijskih zapisa, pregled, zadržavanje i automatizirano upozoravanje.

11.3.2 SI-4 – zahtijeva otkrivanje anomalija sustava i prijavu sumnjivih događaja.

11.4 GDPR EU

11.4.1 Članak 5(1)(f) – zahtijeva cjelovitost i povjerljivost osobnih podataka, što uključuje evidentiranje pristupa.

11.4.2 Članak 32 – nalaže tehničke i organizacijske mjere za osiguravanje sigurnosti, uključujući evidentiranje i praćenje.

11.4.3 Članak 33 – zahtijeva pravodobnu prijavu povrede, uz podršku zapisnika koji omogućuju analizu osnovnog uzroka.

11.5 Direktiva EU NIS2

11.5.1 Članak 21(2)(d) – zahtijeva mehanizme evidentiranja koji otkrivaju anomalije i pružaju podršku tijekom istraga incidenata.

11.5.2 Članak 23 – nalaže prijavu incidenata u roku od 24 sata, što ovisi o točnim i pravodobnim podacima iz zapisnika.

11.6 Uredba EU DORA

11.6.1 Članak 10 – zahtijeva digitalnu operativnu otpornost, uključujući sljedivost incidenata povezanih s IKT-om putem evidentiranja.

11.6.2 Članak 15 – obvezuje na praćenje pružatelja usluga, uključujući pristup zapisnicima i prava na pregled.

11.7 COBIT 2019

11.7.1 DSS01.03 – zahtijeva sljedivost aktivnosti sustava putem evidentiranja i praćenja.

11.7.2 DSS05.02 – obrađuje evidentiranje kao ključnu kontrolu u zaštiti od zlonamjernog softvera i drugih neovlaštenih aktivnosti.