					Sem vnesite naziv registrirane pravne osebe							
Številka dokumenta: P22					Naslov dokumenta: **Politika beleženja in spremljanja**							
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**

1. Namen

1.1 Namen te politike je določiti jasne in zavezujoče zahteve za ustvarjanje, zaščito, pregledovanje in analizo dnevnikov, ki zajemajo ključne sistemske in varnostne dogodke v celotnem informacijskem okolju organizacije.

1.2 Revizijsko beleženje in spremljanje sta ključna za zaznavanje anomalij, odzivanje na grožnje, forenzične preiskave, pripravljenost na revizijo in pravno skladnost. Ta politika zagotavlja, da so vsi sistemsko ustvarjeni dogodki ustrezno zabeleženi, hranjeni in korelirani s časovno usklajeno natančnostjo.

1.3 Ta politika je bistvena za podporo zahtevam standarda ISO/IEC 27001, klavzula 8.1, in kontrolam Priloge A 8.15 (Beleženje), 8.16 (Spremljanje) in 8.17 (Sinhronizacija ure) ter je neposredno povezana z regulativnimi obveznostmi po GDPR, NIS2, DORA in COBIT 2019.

2. Področje uporabe

2.1 Ta politika velja za vse sisteme, storitve in okolja, ki hranijo, obdelujejo ali prenašajo podatke, vključene v sistem upravljanja informacijske varnosti (ISMS), vključno z:

2.1.1 infrastrukturo na lokaciji, storitvami v oblaku (npr. IaaS, PaaS, SaaS) in hibridnimi okolji

2.1.2 operacijskimi sistemi, podatkovnimi bazami, aplikacijami in omrežnimi napravami

2.1.3 varnostnimi sistemi, kot so SIEM, požarni zidovi, platforme za zaznavanje in odzivanje na končnih točkah (EDR), koncentratorji VPN in ponudniki identitete

2.2 V področje uporabe sodijo naslednje zainteresirane strani:

2.2.1 notranji uporabniki s sistemskimi ali skrbniškimi privilegiji

2.2.2 osebje IT infrastrukture in IT operacij

2.2.3 center za varnostne operacije (SOC) in ekipe za zaznavanje groženj

2.2.4 razvijalci programske opreme in lastniki aplikacij

2.2.5 ponudniki storitev tretjih oseb, ki upravljajo sisteme, ki ustvarjajo dnevnike

3. Cilji

3.1 Zagotoviti, da vsi kritični sistemi ustvarjajo dnevnike varnostnih dogodkov in zapise o sistemskih dejavnostih, ki se hranijo v skladu z regulativnimi, pravnimi in pogodbenimi zahtevami.

3.2 Določiti najmanjši nabor vrst dogodkov in vsebine dnevnikov, potrebnih za zaznavanje nepooblaščenih dejavnosti, sledenje dejanjem uporabnikov in podporo forenzičnim preiskavam.

3.3 Uvesti zaščitne ukrepe za preprečevanje poseganja v dnevnike, nepooblaščenega brisanja ali nenadzorovanega dostopa do podatkov iz dnevnikov.

3.4 Vzpostaviti centralizirane sisteme beleženja in opozarjanja (npr. SIEM) za združevanje, korelacijo in eskalacijo sumljivih dejavnosti v skoraj realnem času.

3.5 Zagotoviti sinhronizacijo sistemskih ur za omogočanje natančne medsistemske korelacije in analize incidentov.

3.6 Omogočiti nenehno izboljševanje in skladnost z vključitvijo spremljanja dnevnikov v procese revizije, upravljanja tveganj in upravljanja incidentov.

4. Vloge in odgovornosti

4.1 Vodja informacijske varnosti (CISO)

4.1.1 Je lastnik te politike in zagotavlja njeno usklajenost s profilom tveganja organizacije, revizijskimi zahtevami in obveznostmi ISMS.

4.1.2 Odobri obseg revizijskega beleženja za regulirane ali visoko tvegane sisteme ter nadzira poročanje o skladnosti.

4.2 Vodja centra za varnostne operacije (SOC)

4.2.1 Upravlja in vzdržuje centralizirane platforme za upravljanje dnevnikov (npr. SIEM).

4.2.2 Določa pravila korelacije dogodkov, pragove za opozarjanje in eskalacijske poti za triažo incidentov.

4.2.3 Pregleduje dnevna poročila ter zagotavlja, da so anomalije analizirane, dokumentirane in po potrebi eskalirane.

[... 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 prej kot odziv na:

9.1.1 večje spremembe v arhitekturi sistemov ali infrastrukturi beleženja (npr. migracija SIEM)

9.1.2 spremembe regulativnih zahtev glede beleženja (npr. zahteve NIS2 in DORA glede beleženja)

9.1.3 ugotovitve presoj ali pregledov po incidentu

9.1.4 nastajajoče grožnje, ki zahtevajo okrepljeno spremljanje (npr. notranje grožnje, kompromitacija dobavne verige)

9.2 Postopek pregleda vodi vodja centra za varnostne operacije (SOC) v koordinaciji s CISO, upravljanjem tveganj, funkcijo skladnosti in ekipami IT infrastrukture.

9.3 Odobrene spremembe morajo biti vodene z nadzorom različic v registru nadzora dokumentov ISMS in sporočene:

9.3.1 vsem zainteresiranim stranem, odgovornim za vzdrževanje sistemov beleženja

9.3.2 lastnikom aplikacij in sistemov

9.3.3 ponudnikom tretjih oseb z odgovornostmi glede telemetrije ali integracije SIEM

9.4 Vse nadomeščene različice morajo biti varno arhivirane, dostop pa omejen na pooblaščene skrbnike ISMS za namene presoj in pravne namene.

10. Povezane politike in povezave

10.1 P1 – Politika informacijske varnosti. Določa temeljno zavezanost varovanju sistemov in podatkov, v okviru katerega sta beleženje in spremljanje ključna omogočevalca zaznavanja in odzivanja.

10.2 P4 – Politika nadzora dostopa. Zagotavlja, da se privilegirani dostop, prijave uporabnikov in dogodki avtorizacije beležijo v dnevnike ter spremljajo zaradi zlorab ali anomalnega vedenja.

10.3 P5 – Politika upravljanja sprememb. Zahteva beleženje sistemskih sprememb, uvajanja popravkov in posodobitev konfiguracije, ki lahko uvedejo tveganje ali nepooblaščene spremembe.

10.4 P21 – Politika omrežne varnosti. Zahteva beleženje na ravni omrežja (npr. dnevniki požarnega zidu, opozorila IDS/IPS, dejavnosti VPN) ter integracijo s SIEM za vidnost anomalij omrežnega prometa in zaščite perimetra.

10.5 P23 – Politika sinhronizacije časa. Zagotavlja časovno usklajenost med sistemi, kar je bistveno za zanesljivo beleženje in korelacijo varnostnih dogodkov v več okoljih.

10.6 P30 – Politika odzivanja na incidente. Temelji na podatkih iz dnevnikov in mehanizmih opozarjanja za prepoznavanje, preiskovanje in odzivanje na varnostne incidente, hkrati pa ohranja forenzične artefakte za pregled po incidentu.

11. Referenčni standardi in okviri

11.1 ISO/IEC 27001

11.1.1 Klavzula 8.1 – Operativno načrtovanje in nadzor: zahteva kontrole za spremljanje operacij ter zaščito pred nepooblaščenim dostopom in neprimerno uporabo sistemov.

11.2 ISO/IEC 27002:2022 – Kontrole 8.15, 8.16, 8.17

11.2.1 Določa podrobne zahteve glede beleženja, vključno s tem, katere dogodke je treba beležiti, kako zaščititi in analizirati dnevnike ter kako zagotoviti zanesljivost časovnih žigov med sistemi.

11.3 NIST SP 800-53 Rev. 5

11.3.1 AU-2 do AU-12: zajema izbor dogodkov, beleženje, zaščito, revizijski pregled, odzivanje na napake pri reviziji in hrambo revizijskih zapisov.

11.3.2 SI-4 – Spremljanje sistemov: zahteva aktivno spremljanje sistemov z opozorili na podlagi anomalnih dejavnosti.

11.3.3 SC-45 – Sinhronizacija sistemskega časa: krepi zahteve glede točnosti časa za sledljivost dogodkov in korelacijo incidentov.

11.4 Uredba EU GDPR (2016/679)

11.4.1 Člen 32 – Varnost obdelave: zahteva tehnične kontrole, kot sta beleženje in spremljanje, za zagotavljanje varnosti in odgovornosti, zlasti pri dostopu do osebnih podatkov.

11.5 Direktiva EU NIS2 (2022/2555)

11.5.1 Člen 21(2)(e): zahteva sisteme za beleženje dogodkov in spremljanje za hitro zaznavanje in odzivanje na varnostne incidente.

11.6 Uredba EU DORA (2022/2554)

11.6.1 Člen 9 – Upravljanje tveganj IKT: zahteva mehanizme za zaznavanje anomalnih dejavnosti, beleženje incidentov in hrambo forenzičnih podatkov.

11.6.2 Člen 11 – Testiranje načrtov neprekinjenega poslovanja za sisteme IKT: poudarja neprekinjeno spremljanje in preverjanje razpoložljivosti dnevnikov med operativnimi motnjami.

11.7 COBIT 2019

11.7.1 DSS01.05 – Upravljanje varnostnih dnevnikov: zahteva uvedbo zmogljivosti beleženja za vso kritično infrastrukturo.

11.7.2 DSS05.04 – Spremljanje varnostnih dogodkov: zahteva spremljanje in analizo dnevnikov v realnem času za zaznavanje dogodkov in odzivanje nanje.

11.7.3 MEA03 – Nadzor, vrednotenje in ocenjevanje skladnosti: zahteva redni pregled praks beleženja in usklajenost s cilji kontrol.