					Ovdje unesite naziv registrirane pravne osobe							
Broj dokumenta: P22					Naziv dokumenta: **Politika zapisivanja 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**

1. Svrha

1.1 Svrha ove politike jest uspostaviti jasne i provedive zahtjeve za generiranje, zaštitu, pregled i analizu dnevničkih zapisa koji bilježe ključne sustavske i sigurnosno relevantne događaje u cjelokupnom IT okruženju organizacije.

1.2 Zapisivanje i praćenje ključni su za otkrivanje anomalija, odgovor na prijetnje, forenzičke istrage, spremnost za reviziju i usklađenost sa zakonskim zahtjevima. Ova politika osigurava da se svi sustavski generirani događaji pravilno evidentiraju, čuvaju i koreliraju uz vremenski usklađenu točnost.

1.3 Ova je politika ključna za potporu zahtjevima norme ISO/IEC 27001 iz točke 8.1 i kontrolama iz Priloga A 8.15 (zapisivanje), 8.16 (praćenje) i 8.17 (sinkronizacija vremena) te je izravno povezana s regulatornim obvezama prema GDPR-u, NIS2, DORA-i i COBIT-u 2019.

2. Područje primjene

2.1 Ova politika primjenjuje se na sve sustave, usluge i okruženja koja pohranjuju, obrađuju ili prenose podatke obuhvaćene sustavom upravljanja informacijskom sigurnošću (ISMS), uključujući:

2.1.1 infrastrukturu u vlastitim podatkovnim centrima, usluge u oblaku (npr. IaaS, PaaS, SaaS) i hibridna okruženja

2.1.2 operacijske sustave, baze podataka, aplikacije i mrežne uređaje

2.1.3 sigurnosne sustave kao što su SIEM, vatrozidi, platforme za otkrivanje i odgovor na prijetnje na krajnjim uređajima, VPN koncentratori i pružatelji identiteta

2.2 Sljedeći dionici obuhvaćeni su ovom politikom:

2.2.1 interni korisnici sa sustavskim ili administrativnim privilegijama

2.2.2 osoblje za infrastrukturu i IT operacije

2.2.3 centar sigurnosnih operacija (SOC) i timovi za otkrivanje prijetnji

2.2.4 razvojni inženjeri i vlasnici aplikacija

2.2.5 pružatelji usluga treće strane koji upravljaju sustavima koji generiraju dnevničke zapise

3. Ciljevi

3.1 Osigurati da svi kritični sustavi generiraju dnevnike sigurnosnih događaja i zapise o aktivnostima sustava koji se čuvaju u skladu s regulatornim, zakonskim i ugovornim zahtjevima.

3.2 Definirati minimalne vrste događaja i sadržaj dnevničkih zapisa potrebne za otkrivanje neovlaštenih aktivnosti, praćenje radnji korisnika i potporu forenzičkim istragama.

3.3 Uspostaviti zaštitne mjere radi sprječavanja neovlaštene izmjene dnevničkih zapisa, njihova neovlaštenog brisanja ili nekontroliranog pristupa podacima iz dnevnika.

3.4 Uspostaviti centralizirane sustave za zapisivanje i upozoravanje (npr. SIEM) radi agregacije, korelacije i eskalacije sumnjivih aktivnosti gotovo u stvarnom vremenu.

3.5 Osigurati sinkronizaciju sustavskih satova kako bi se omogućila točna korelacija među sustavima i analiza incidenata.

3.6 Omogućiti kontinuirano poboljšavanje i usklađenost integracijom praćenja dnevničkih zapisa s procesima revizije, upravljanja rizicima i upravljanja incidentima.

4. Uloge i odgovornosti

4.1 glavni direktor za informacijsku sigurnost (CISO)

4.1.1 Vlasnik je ove politike i osigurava njezinu usklađenost s profilom rizika organizacije, revizijskim zahtjevima i obvezama ISMS-a.

4.1.2 Odobrava opseg zapisivanja za regulirane sustave ili sustave visokog rizika te nadzire izvješćivanje o usklađenosti.

4.2 voditelj centra sigurnosnih operacija (SOC)

4.2.1 Upravlja i održava centralizirane platforme za upravljanje dnevničkim zapisima (npr. SIEM).

4.2.2 Definira pravila agregacije dnevničkih zapisa, pragove upozorenja i putove eskalacije za trijažu incidenata.

4.2.3 Pregledava dnevna izvješća i osigurava da se anomalije analiziraju, dokumentiraju i prema potrebi eskaliraju.

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

9. Zahtjevi za pregled i ažuriranje

9.1 Ova politika mora se pregledati najmanje jednom godišnje ili ranije kao odgovor na:

9.1.1 značajne promjene u arhitekturi sustava ili infrastrukturi zapisivanja (npr. migracija SIEM-a)

9.1.2 izmjene regulatornih zahtjeva za zapisivanje (npr. zahtjevi NIS2 ili DORA za zapisivanje)

9.1.3 nalaze revizije ili zaključke naknadnih analiza incidenata

9.1.4 nove prijetnje koje zahtijevaju pojačano praćenje (npr. insajderske prijetnje, kompromitacija opskrbnog lanca)

9.2 Postupak pregleda vodi voditelj centra sigurnosnih operacija (SOC) u koordinaciji s CISO-om, funkcijom upravljanja rizicima, funkcijom usklađenosti i timovima za IT infrastrukturu.

9.3 Odobrene promjene moraju biti pod verzijskim nadzorom u Registru upravljanja dokumentima ISMS-a i priopćene:

9.3.1 svim dionicima odgovornima za održavanje sustava zapisivanja

9.3.2 vlasnicima aplikacija i sustava

9.3.3 pružateljima usluga treće strane s obvezama u području telemetrije ili integracije sa SIEM-om

9.4 Sve zamijenjene verzije moraju se sigurno arhivirati, uz pristup ograničen na ovlaštene skrbnike ISMS-a za potrebe revizije i pravnih postupaka.

10. Povezane politike i poveznice

10.1 P1 – Politika informacijske sigurnosti. Uspostavlja temeljnu obvezu zaštite sustava i podataka, u okviru koje zapisivanje i praćenje imaju ključnu ulogu detektivnih kontrola i omogućavanja odgovora.

10.2 P4 – Politika kontrole pristupa. Osigurava da se privilegirani pristup, prijave korisnika i događaji autorizacije bilježe u dnevničkim zapisima i prate radi otkrivanja zlouporabe ili anomalnog ponašanja.

10.3 P5 – Politika upravljanja promjenama. Propisuje bilježenje promjena sustava, uvođenja zakrpa i ažuriranja konfiguracije koji mogu unijeti rizik ili dovesti do neovlaštenih izmjena.

10.4 P21 – Politika mrežne sigurnosti. Zahtijeva zapisivanje na mrežnoj razini (npr. dnevnici vatrozida, upozorenja IDS/IPS-a, VPN aktivnosti) i integraciju sa SIEM-om radi vidljivosti anomalija mrežnog prometa i zaštite granica sustava.

10.5 P23 – Politika sinkronizacije vremena. Propisuje dosljednost vremena među sustavima, što je ključno za pouzdano zapisivanje i korelaciju sigurnosnih događaja u više okruženja.

10.6 P30 – Politika odgovora na incidente. Oslanja se na podatke iz dnevničkih zapisa i mehanizme upozoravanja za identifikaciju, istragu i odgovor na sigurnosne incidente, uz očuvanje forenzičkih artefakata za pregled nakon incidenta.

11. Referentni standardi i okviri

11.1 ISO/IEC 27001

11.1.1 Točka 8.1 – Operativno planiranje i kontrola: zahtijeva kontrole za praćenje operacija i zaštitu od neovlaštenog pristupa i zlouporabe sustava.

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

11.2.1 Definira detaljne zahtjeve za zapisivanje, uključujući koje događaje treba evidentirati, kako zaštititi i analizirati dnevničke zapise te kako osigurati pouzdanost vremenskih oznaka u svim sustavima.

11.3 NIST SP 800-53 Rev. 5

11.3.1 AU-2 do AU-12: obuhvaća odabir događaja, zapisivanje, zaštitu, pregled revizijskih zapisa, odgovor na neuspjehe revizije i čuvanje revizijskih zapisa.

11.3.2 SI-4 – Praćenje sustava: zahtijeva aktivni nadzor sustava uz upozorenja temeljena na anomalnim aktivnostima.

11.3.3 SC-45 – Sinkronizacija vremena sustava: dodatno naglašava točnost vremena radi sljedivosti događaja i korelacije incidenata.

11.4 GDPR EU (2016/679)

11.4.1 Članak 32 – Sigurnost obrade: zahtijeva tehničke kontrole kao što su zapisivanje i praćenje radi osiguravanja sigurnosti i odgovornosti, osobito za pristup osobnim podacima.

11.5 Direktiva EU NIS2 (2022/2555)

11.5.1 Članak 21(2)(e): nalaže sustave za zapisivanje događaja i praćenje radi brzog otkrivanja i odgovora na sigurnosne incidente.

11.6 Uredba EU DORA (2022/2554)

11.6.1 Članak 9 – upravljanje IKT rizicima: zahtijeva mehanizme za otkrivanje anomalnih aktivnosti, bilježenje incidenata i čuvanje forenzičkih podataka.

11.6.2 Članak 11 – testiranje planova kontinuiteta poslovanja za IKT: naglašava kontinuitet praćenja i provjeru dostupnosti dnevničkih zapisa tijekom operativnih poremećaja.

11.7 COBIT 2019

11.7.1 DSS01.05 – Upravljanje sigurnosnim dnevničkim zapisima: zahtijeva uspostavu mogućnosti zapisivanja za svu kritičnu infrastrukturu.

11.7.2 DSS05.04 – Praćenje sigurnosnih događaja: nalaže praćenje i analizu dnevničkih zapisa u stvarnom vremenu radi otkrivanja i odgovora na događaje.

11.7.3 MEA03 – Praćenje, vrednovanje i procjena usklađenosti: zahtijeva redoviti pregled praksi zapisivanja i njihovu usklađenost s ciljevima kontrola.