					Sem zadajte názov registrovanej právnickej osoby							
Číslo dokumentu: P22					Názov dokumentu: **Politika logovania a monitorovania**							
Verzia: 1.0		Dátum nadobudnutia účinnosti: 01.01.2025			Vlastník dokumentu:							
X	Politika		Štandard		Postup		Formulár		Register		Iné	

História revízií				
Číslo revízie	**Dátum revízie**	**Zmeny**	**Preskúmal**	**Vlastník procesu**

Schválenia			
Meno	**Pozícia**	**Dátum**	**Podpis**

1. Účel

1.1 Účelom tejto politiky je stanoviť jasné a záväzné požiadavky na generovanie, ochranu, preskúmavanie a analýzu logov, ktoré zaznamenávajú kľúčové systémové a bezpečnostné udalosti v celom IT prostredí organizácie.

1.2 Logovanie a monitorovanie sú kľúčové pre detekciu anomálií, reakciu na hrozby, forenzné vyšetrovanie, pripravenosť na audit a súlad s právnymi a regulačnými požiadavkami. Táto politika zabezpečuje, aby všetky systémom generované udalosti boli riadne zaznamenávané, uchovávané a korelované s časovo synchronizovanou presnosťou.

1.3 Táto politika je nevyhnutná na podporu požiadaviek kapitoly 8.1 normy ISO/IEC 27001 a kontrol prílohy A 8.15 (Logovanie), 8.16 (Monitorovanie) a 8.17 (Synchronizácia času) a je priamo mapovaná na regulačné povinnosti podľa GDPR, NIS2, DORA a COBIT 2019.

2. Rozsah

2.1 Táto politika sa vzťahuje na všetky systémy, služby a prostredia, ktoré ukladajú, spracúvajú alebo prenášajú údaje zahrnuté do systému manažérstva informačnej bezpečnosti (ISMS), vrátane:

2.1.1 infraštruktúry v lokálnom prostredí, cloudových služieb (napr. IaaS, PaaS, SaaS) a hybridných prostredí

2.1.2 operačných systémov, databáz, aplikácií a sieťových zariadení

2.1.3 bezpečnostných systémov, ako sú SIEM, firewally, platformy EDR, koncentrátory VPN a poskytovatelia identít

2.2 Do rozsahu tejto politiky patria tieto zainteresované strany:

2.2.1 interní používatelia so systémovými alebo administrátorskými oprávneniami

2.2.2 pracovníci infraštruktúry a IT prevádzky

2.2.3 centrum bezpečnostných operácií (SOC) a tímy detekcie hrozieb

2.2.4 vývojári softvéru a vlastníci aplikácií

2.2.5 poskytovatelia služieb tretích strán spravujúci systémy generujúce logy

3. Ciele

3.1 Zabezpečiť, aby všetky kritické systémy generovali logy bezpečnostných udalostí a záznamy o systémových aktivitách, ktoré sa uchovávajú v súlade s regulačnými, právnymi a zmluvnými požiadavkami.

3.2 Definovať minimálne typy udalostí a obsah logov potrebný na detekciu neoprávnených činností, sledovanie používateľských aktivít a podporu forenzných vyšetrovaní.

3.3 Uplatňovať ochranné opatrenia na zabránenie manipulácii s logmi, neoprávnenému výmazu alebo nekontrolovanému prístupu k údajom z logov.

3.4 Zaviesť centralizované systémy logovania a upozorňovania (napr. SIEM) na agregáciu, koreláciu a eskaláciu podozrivej aktivity v takmer reálnom čase.

3.5 Zabezpečiť synchronizáciu systémového času na umožnenie presnej korelácie medzi systémami a analýzy incidentov.

3.6 Umožniť nepretržité zlepšovanie a súlad integráciou monitorovania logov s procesmi auditu, riadenia rizík a riadenia incidentov.

4. Roly a zodpovednosti

4.1 riaditeľ informačnej bezpečnosti (CISO)

4.1.1 Zodpovedá za túto politiku a zabezpečuje jej zosúladenie s rizikovým profilom organizácie, požiadavkami auditu a povinnosťami v rámci ISMS.

4.1.2 Schvaľuje rozsah logovania pre regulované alebo vysoko rizikové systémy a dohliada na vykazovanie súladu.

4.2 manažér centra bezpečnostných operácií (SOC)

4.2.1 Prevádzkuje a udržiava centralizované platformy na správu logov (napr. SIEM).

4.2.2 Definuje pravidlá agregácie logov, prahové hodnoty upozornení a eskalačné postupy pre triáž incidentov.

4.2.3 Denne preskúmava reporty a zabezpečuje, aby boli anomálie analyzované, zdokumentované a podľa potreby eskalované.

[... Sekcie 4.3–8 nie sú súčasťou tohto náhľadu. Pre prístup k úplnému obsahu si zakúpte celý dokument. ...]

9. Požiadavky na preskúmanie a aktualizáciu

9.1 Táto politika musí byť preskúmaná každoročne alebo skôr v reakcii na:

9.1.1 významné zmeny architektúry systémov alebo infraštruktúry logovania (napr. migrácia SIEM)

9.1.2 zmeny regulačných požiadaviek na logovanie (napr. povinnosti logovania podľa NIS2, DORA)

9.1.3 zistenia z auditov alebo poincidentných analýz

9.1.4 nové hrozby vyžadujúce rozšírené monitorovanie (napr. vnútorné hrozby, kompromitácia dodávateľského reťazca)

9.2 Proces preskúmania vedie manažér centra bezpečnostných operácií (SOC) v koordinácii s CISO, riadením rizík, funkciou súladu a tímami IT infraštruktúry.

9.3 Schválené zmeny musia podliehať riadeniu verzií v Registri dokumentov ISMS a musia byť oznámené:

9.3.1 všetkým zainteresovaným stranám zodpovedným za údržbu systémov logovania

9.3.2 vlastníkom aplikácií a systémov

9.3.3 poskytovateľom tretích strán s povinnosťami v oblasti telemetrie alebo integrácie SIEM

9.4 Všetky nahradené verzie musia byť bezpečne archivované, pričom prístup k nim je obmedzený na oprávnených správcov ISMS na účely auditu a právnej obhájiteľnosti.

10. Súvisiace politiky a väzby

10.1 P1 – Politika informačnej bezpečnosti. Stanovuje základný záväzok chrániť systémy a údaje, pričom logovanie a monitorovanie plnia úlohu kľúčových detekčných opatrení a mechanizmov podpory reakcie.

10.2 P4 – Politika riadenia prístupu. Zabezpečuje, aby privilegovaný prístup, prihlásenia používateľov a autorizačné udalosti boli zachytené v logoch a monitorované z hľadiska zneužitia alebo anomálneho správania.

10.3 P5 – Politika riadenia zmien. Vyžaduje logovanie systémových zmien, nasadenia záplat a aktualizácií konfigurácie, ktoré môžu zaviesť riziko alebo neoprávnené úpravy.

10.4 P21 – Politika bezpečnosti siete. Vyžaduje logovanie na úrovni siete (napr. logy firewallu, upozornenia IDS/IPS, aktivita VPN) a integráciu so SIEM na zabezpečenie viditeľnosti anomálií prevádzky a ochrany perimetra.

10.5 P23 – Politika synchronizácie času. Presadzuje konzistentnosť systémového času naprieč systémami, čo je nevyhnutné na spoľahlivé logovanie a koreláciu bezpečnostných udalostí vo viacerých prostrediach.

10.6 P30 – Politika reakcie na incidenty (P30). Vychádza z údajov z logov a mechanizmov upozorňovania pri identifikácii, vyšetrovaní a riešení bezpečnostných incidentov a zároveň zabezpečuje uchovanie forenzných artefaktov na poincidentné preskúmanie.

11. Referenčné normy a rámce

11.1 ISO/IEC 27001

11.1.1 Kapitola 8.1 – Prevádzkové plánovanie a riadenie: Vyžaduje kontroly na monitorovanie prevádzky a ochranu pred neoprávneným prístupom a zneužitím systémov.

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

11.2.1 Definuje podrobné požiadavky na logovanie vrátane toho, ktoré udalosti sa musia zaznamenávať, ako sa majú logy chrániť a analyzovať a ako zabezpečiť spoľahlivosť časových pečiatok naprieč systémami.

11.3 NIST SP 800-53 Rev.5

11.3.1 AU-2 až AU-12: Pokrýva výber udalostí, logovanie, ochranu, auditné preskúmavanie, reakciu na zlyhania auditovania a uchovávanie auditných záznamov.

11.3.2 SI-4 – Monitorovanie systémov: Vyžaduje aktívne monitorovanie systémov s upozorneniami založenými na anomálnej aktivite.

11.3.3 SC-45 – Synchronizácia systémového času: Posilňuje presnosť času na účely sledovateľnosti udalostí a korelácie incidentov.

11.4 Nariadenie EÚ GDPR (2016/679)

11.4.1 Článok 32 – Bezpečnosť spracúvania: Vyžaduje technické kontroly, ako je logovanie a monitorovanie, na zabezpečenie bezpečnosti a preukázateľnej zodpovednosti, najmä pri prístupe k osobným údajom.

11.5 Smernica EÚ NIS2 (2022/2555)

11.5.1 Článok 21(2)(e): Vyžaduje systémy logovania a monitorovania udalostí na rýchlu detekciu bezpečnostných incidentov a reakciu na ne.

11.6 Nariadenie EÚ DORA (2022/2554)

11.6.1 Článok 9 – Riadenie rizík IKT: Vyžaduje mechanizmy na detekciu anomálnej aktivity, logovanie incidentov a uchovávanie forenzných údajov.

11.6.2 Článok 11 – Testovanie plánov kontinuity činností IKT: Zdôrazňuje kontinuitu monitorovania a overovanie dostupnosti logov počas prevádzkových narušení.

11.7 COBIT 2019

11.7.1 DSS01.05 – Správa bezpečnostných logov: Vyžaduje implementáciu schopností logovania pre všetku kritickú infraštruktúru.

11.7.2 DSS05.04 – Monitorovanie bezpečnostných udalostí: Vyžaduje monitorovanie a analýzu logov v reálnom čase na detekciu udalostí a reakciu na ne.

11.7.3 MEA03 – Monitorovanie, hodnotenie a posudzovanie súladu: Vyžaduje pravidelné preskúmavanie postupov logovania a ich zosúladenie s cieľmi kontrol.