					Sem vložte název registrované právnické osoby							
Číslo dokumentu: P22					Název dokumentu: **Politika protokolování a monitorování**							
Verze: 1.0		Datum účinnosti: 01.01.2025			Vlastník dokumentu:							
X	Politika		Standard		Postup		Formulář		Registr		Jiné	

Historie revizí				
Číslo revize	**Datum revize**	**Změny**	**Přezkoumal**	**Vlastník procesu**

Schválení			
Jméno	**Funkce**	**Datum**	**Podpis**

1. Účel

1.1 Účelem této politiky je stanovit jasné a vymahatelné požadavky na generování, ochranu, přezkum a analýzu logů, které zachycují klíčové systémové a bezpečnostní události v IT prostředí organizace.

1.2 Protokolování a monitorování jsou zásadní pro detekci anomálií, reakci na hrozby, forenzní šetření, připravenost na audit a soulad s právními požadavky. Tato politika zajišťuje, aby všechny systémem generované události byly řádně zaznamenávány, uchovávány a korelovány s přesně synchronizovanými časovými údaji.

1.3 Tato politika je nezbytná pro podporu požadavků ISO/IEC 27001, kapitoly 8.1, a přílohy A, opatření 8.15 (protokolování), 8.16 (monitorování) a 8.17 (synchronizace času), a je přímo navázána na regulatorní povinnosti podle GDPR, směrnice NIS2, nařízení DORA a COBIT 2019.

2. Rozsah

2.1 Tato politika se vztahuje na všechny systémy, služby a prostředí, které ukládají, zpracovávají nebo přenášejí data spadající do rozsahu systému řízení bezpečnosti informací (ISMS), včetně:

2.1.1 lokální infrastruktury, cloudových služeb (např. IaaS, PaaS, SaaS) a hybridních prostředí

2.1.2 operačních systémů, databází, aplikací a síťových zařízení

2.1.3 bezpečnostních systémů, jako jsou SIEM, firewally, platformy EDR (detekce a reakce na koncových bodech), koncentrátory VPN a poskytovatelé identit

2.2 Do rozsahu působnosti spadají tyto zainteresované strany:

2.2.1 interní uživatelé se systémovými nebo administrátorskými oprávněními

2.2.2 pracovníci infrastruktury a IT provozu

2.2.3 bezpečnostní operační centrum (SOC) a týmy detekce hrozeb

2.2.4 vývojáři softwaru a vlastníci aplikací

2.2.5 poskytovatelé služeb třetích stran spravující systémy generující logy

3. Cíle

3.1 Zajistit, aby všechny kritické systémy generovaly logy bezpečnostních událostí a záznamy o systémových činnostech, které budou uchovávány v souladu s regulatorními, právními a smluvními požadavky.

3.2 Stanovit minimální typy událostí a obsah logů potřebné k detekci neoprávněných činností, dohledání uživatelských akcí a podpoře forenzního šetření.

3.3 Uplatňovat ochranná opatření, která zabrání manipulaci s logy, jejich neoprávněnému mazání nebo nekontrolovanému přístupu k údajům v logách.

3.4 Zavést centralizované systémy protokolování a upozorňování (např. SIEM) pro agregaci, korelaci a eskalaci podezřelých aktivit v téměř reálném čase.

3.5 Zajistit synchronizaci systémových hodin pro přesnou korelaci napříč systémy a analýzu incidentů.

3.6 Podporovat průběžné zlepšování a soulad prostřednictvím integrace monitorování logů s procesy auditu, řízení rizik a řízení incidentů.

4. Role a odpovědnosti

4.1 ředitel informační bezpečnosti (CISO)

4.1.1 Odpovídá za tuto politiku a zajišťuje její soulad s apetitem organizace k riziku, požadavky auditu a povinnostmi v rámci ISMS.

4.1.2 Schvaluje rozsah protokolování pro regulované systémy nebo systémy s vysokým rizikem a vykonává dohled nad vykazováním souladu.

4.2 manažer bezpečnostního operačního centra (SOC)

4.2.1 Provozuje a udržuje centralizované platformy pro správu logů (např. SIEM).

4.2.2 Definuje pravidla agregace logů, prahové hodnoty upozornění a eskalační postupy pro triáž incidentů.

4.2.3 Denně přezkoumává reporty a zajišťuje, aby anomálie byly analyzovány, zdokumentovány a podle potřeby eskalovány.

[... Oddíly 4.3–8 nejsou součástí tohoto náhledu. Pro přístup k úplnému obsahu zakupte celý dokument. ...]

9. Požadavky na přezkoumávání a aktualizaci

9.1 Tato politika musí být přezkoumána každoročně nebo dříve v reakci na:

9.1.1 významné změny systémové architektury nebo infrastruktury protokolování (např. migraci SIEM)

9.1.2 změny regulatorních požadavků na protokolování (např. požadavky směrnice NIS2 nebo nařízení DORA)

9.1.3 zjištění z auditů nebo rozborů po incidentech

9.1.4 nově vznikající hrozby vyžadující posílené monitorování (např. vnitřní hrozby, kompromitaci dodavatelského řetězce)

9.2 Proces přezkumu řídí manažer bezpečnostního operačního centra (SOC) v koordinaci s CISO, řízením rizik, funkcí compliance a týmy IT infrastruktury.

9.3 Schválené změny musí být vedeny v režimu správy verzí v registru řízení dokumentace ISMS a oznámeny:

9.3.1 všem zainteresovaným stranám odpovědným za údržbu systémů protokolování

9.3.2 vlastníkům aplikací a systémů

9.3.3 poskytovatelům třetích stran s povinnostmi v oblasti telemetrie nebo integrace SIEM

9.4 Všechny nahrazené verze musí být bezpečně archivovány, přičemž přístup k nim je omezen na oprávněné správce ISMS pro účely auditu a právní účely.

10. Související politiky a vazby

10.1 P1 – Politika informační bezpečnosti. Stanoví základní závazek chránit systémy a data, v jehož rámci protokolování a monitorování plní klíčovou roli detekčních kontrol a podpory reakce.

10.2 P4 – Politika řízení přístupu. Zajišťuje, aby privilegovaný přístup, přihlášení uživatelů a autorizační události byly zachycovány v logách a monitorovány z hlediska zneužití nebo anomálního chování.

10.3 P5 – Politika řízení změn. Ukládá povinnost protokolovat systémové změny, nasazení záplat a aktualizace konfigurace, které mohou zavést riziko nebo neoprávněné změny.

10.4 P21 – Politika zabezpečení sítě. Vyžaduje protokolování na síťové úrovni (např. logy firewallu, upozornění IDS/IPS, aktivitu VPN) a integraci se SIEM pro zajištění viditelnosti provozních anomálií a ochrany perimetru.

10.5 P23 – Politika synchronizace času. Vynucuje konzistenci času napříč systémy, což je nezbytné pro spolehlivé protokolování a korelaci bezpečnostních událostí napříč více prostředími.

10.6 P30 – Politika reakce na incidenty. Využívá data z logů a mechanismy upozorňování k identifikaci, šetření a řešení bezpečnostních incidentů a současně zachovává forenzní artefakty pro přezkum po incidentu.

11. Referenční normy a rámce

11.1 ISO/IEC 27001

11.1.1 Kapitola 8.1 – Operační plánování a řízení: Vyžaduje opatření pro monitorování provozu a ochranu před neoprávněným přístupem a zneužitím systému.

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

11.2.1 Definuje podrobné požadavky na protokolování, včetně toho, které události musí být zaznamenávány, jak chránit a analyzovat logy a jak zajistit spolehlivost časových razítek napříč systémy.

11.3 NIST SP 800-53 Rev. 5

11.3.1 AU-2 až AU-12: Pokrývá výběr událostí, protokolování, ochranu, auditní přezkum, reakci na selhání auditování a uchovávání auditních záznamů.

11.3.2 SI-4 – Monitorování systému: Vyžaduje aktivní monitorování systému s upozorněními založenými na anomální aktivitě.

11.3.3 SC-45 – Synchronizace systémového času: Posiluje přesnost času pro dohledatelnost událostí a korelaci incidentů.

11.4 GDPR EU (2016/679)

11.4.1 Článek 32 – Zabezpečení zpracování: Vyžaduje technická opatření, jako jsou protokolování a monitorování, k zajištění bezpečnosti a odpovědnosti, zejména při přístupu k osobním údajům.

11.5 směrnice NIS2 EU (2022/2555)

11.5.1 Článek 21 odst. 2 písm. e): Ukládá povinnost zavést systémy protokolování událostí a monitorování pro rychlou detekci bezpečnostních incidentů a reakci na ně.

11.6 nařízení DORA EU (2022/2554)

11.6.1 Článek 9 – Řízení rizik v oblasti ICT: Vyžaduje mechanismy pro detekci anomální aktivity, protokolování incidentů a uchovávání forenzních dat.

11.6.2 Článek 11 – Testování plánů kontinuity činností v oblasti ICT: Zdůrazňuje kontinuitu monitorování a ověřování dostupnosti logů během provozních narušení.

11.7 COBIT 2019

11.7.1 DSS01.05 – Správa bezpečnostních logů: Vyžaduje zavedení schopností protokolování pro veškerou kritickou infrastrukturu.

11.7.2 DSS05.04 – Monitorování bezpečnostních událostí: Ukládá monitorování a analýzu logů v reálném čase pro detekci událostí a reakci na ně.

11.7.3 MEA03 – Monitorování, vyhodnocování a posuzování souladu: Vyžaduje pravidelný přezkum postupů protokolování a jejich souladu s cíli bezpečnostních opatření.