					Sem zadajte názov registrovanej právnickej osoby							
Číslo dokumentu: P22S					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**

Zosúladenie s normami a predpismi

Norma/predpis	Kapitola/článok	Poznámka
ISO/IEC 27001:2022	Kapitola 8	Prevádzkové kontroly vrátane logovania
ISO/IEC 27002:2022	Kontroly 8.15, 8.16, 8.17	Logovanie udalostí, ochrana logov a monitorovanie
NIST SP 800-53 Rev.5	AU-2 až AU-12, SI-4	Obsah a preskúmavanie auditných logov, uchovávanie, detekcia anomálií, upozorňovanie
Nariadenie EÚ GDPR	Články 5(1)(f), 32, 33	Dôvernosť a integrita údajov, technické opatrenia a oznamovanie porušenia ochrany osobných údajov
Smernica EÚ NIS2	Články 21(2)(d), 23	Mechanizmy logovania na detekciu anomálií a oznamovanie incidentov do 24 hodín
Nariadenie EÚ DORA	Články 10, 15	Prevádzková odolnosť, monitorovanie a logovanie poskytovateľov služieb
COBIT 2019	DSS01.03, DSS05.02	Sledovateľnosť činností a ochrana prostredníctvom logovania a monitorovania

1. Účel

1.1 Táto politika stanovuje záväzné kontroly logovania a monitorovania s cieľom zabezpečiť bezpečnosť, vyvoditeľnosť zodpovednosti a prevádzkovú integritu IT systémov organizácie.

1.2 Vymedzuje typy udalostí, ktoré sa musia zaznamenávať do logov, spôsob uchovávania logov, spôsob ich preskúmavania a zodpovednosti zamestnancov a poskytovateľov služieb.

1.3 Logovanie a monitorovanie podporujú detekciu hrozieb, súlad s regulačnými požiadavkami, reakciu na incidenty a forenznú analýzu.

1.4 Táto politika umožňuje organizácii plniť požiadavky na prevádzkové kontroly podľa ISO/IEC 27001 a podporuje priebežnú pripravenosť na audit, dôveru zákazníkov a súlad s GDPR, NIS2 a DORA.

2. Rozsah

2.1 Táto politika sa vzťahuje na všetky systémy a používateľov v organizácii vrátane:

2.1.1 pracovných staníc, notebookov, serverov, firewallov, prepínačov, smerovačov a bezdrôtových prístupových bodov,

2.1.2 cloudových služieb používaných na prevádzku organizácie (napr. e-mail, úložiská súborov, zálohovanie, nástroje na spoluprácu),

2.1.3 funkcií logovania v antivírusovom softvéri, aplikáciách, operačných systémoch a sieťových zariadeniach,

2.1.4 všetkých zamestnancov, dodávateľov a poskytovateľov riadených služieb (MSP), ktorí systémy používajú alebo spravujú,

2.1.5 akéhokoľvek miesta, kde sa používajú IT systémy spoločnosti, vrátane prostredia práce na diaľku, hybridnej práce alebo BYOD.

2.2 Politika sa vzťahuje aj na logy vytvorené službami tretích strán, ak má organizácia administrátorský prístup alebo zmluvné práva na audit.

3. Ciele

3.1 Zabezpečiť logovanie systémovej činnosti vrátane autentifikácie, zmien konfigurácie, prístupu k citlivým údajom a bezpečnostných upozornení.

3.2 Udržiavať bezpečné a presné logy na detekciu porušení politiky, systémových chýb alebo neoprávnenej činnosti.

3.3 Umožniť rýchle preskúmanie logov počas incidentov, vyšetrovaní a auditov.

3.4 Podporovať synchronizáciu času na zabezpečenie integrity a korelácie údajov v logoch.

3.5 Chrániť logy pred manipuláciou, stratou alebo predčasným vymazaním.

3.6 Plniť právne a regulačné povinnosti týkajúce sa vyvoditeľnosti zodpovednosti, sledovateľnosti a reakcie na porušenie ochrany osobných údajov.

4. Roly a zodpovednosti

4.1 Generálny riaditeľ (GM)

4.1.1 Schvaľuje túto politiku a zabezpečuje jej zavedenie vo všetkých podnikových systémoch.

4.1.2 Preskúmava upozornenia s vysokou závažnosťou a závažné zistenia auditu oznámené IT alebo funkciou ochrany súkromia.

4.1.3 Schvaľuje výnimky, ak logovanie alebo uchovávanie nemožno technicky zabezpečiť.

4.2 Poskytovateľ IT podpory / interná IT funkcia

4.2.1 Zavádza a konfiguruje logovanie pre operačné systémy, sieťové zariadenia, antivírusové nástroje a kľúčové aplikácie.

4.2.2 Zabezpečuje uchovávanie logov, ich zálohovanie a ochranu pred zmenou.

4.2.3 Preskúmava logy podľa stanoveného harmonogramu a vyšetruje podozrivú alebo neoprávnenú činnosť.

4.2.4 Udržiava systémy upozorňovania, ktoré identifikujú anomálne správanie alebo indikátory kompromitácie.

[... 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 Ročné preskúmanie

9.1.1 Túto politiku musí najmenej raz ročne preskúmať generálny riaditeľ za podpory poskytovateľa IT podpory a koordinátora ochrany súkromia.

9.2 Spúšťače preskúmania

9.2.1 Mimoriadne preskúmania sa musia vykonať v reakcii na:

9.2.1.1 zistenia týkajúce sa logov z interných alebo externých auditov,

9.2.1.2 bezpečnostné incidenty, pri ktorých logy chýbali, boli poškodené alebo nepostačovali,

9.2.1.3 významné zmeny IT infraštruktúry (napr. migrácia na platformy centralizovaného logovania v cloudovom prostredí),

9.2.1.4 aktualizácie právnych alebo regulačných povinností (napr. GDPR, NIS2, DORA).

9.3 Riadenie verzií

9.3.1 Všetky zmeny tejto politiky musia byť zaznamenané s uvedením čísla verzie, dátumu a súhrnu zmien.

9.3.2 Predchádzajúce verzie sa musia archivovať a uchovávať najmenej 3 roky.

9.3.3 Aktualizované politiky musia byť oznámené dotknutým zainteresovaným stranám, najmä tým, ktoré majú prístup na úrovni systému.

10. Súvisiace politiky a väzby

10.1 Táto politika priamo podporuje tieto SME politiky informačnej bezpečnosti a je nimi podporovaná:

10.1.1 P17S – Politika ochrany údajov a súkromia: Zabezpečuje, aby sa s údajmi v logoch obsahujúcimi osobné informácie nakladalo s primeranou integritou, dobou uchovávania a ochranou prístupu v súlade s požiadavkami GDPR.

10.1.2 P21S – Politika bezpečnosti siete: Poskytuje základ na zaznamenávanie logov súvisiacich s firewallmi, bezdrôtovým prístupom, VPN a monitorovaním segmentácie.

10.1.3 P24S – Politika bezpečného vývoja: Zabezpečuje, aby aplikačné logy (napr. pokusy o prihlásenie, chyby a výnimky) boli súčasťou návrhu softvéru a prevádzky.

10.1.4 P30S – Politika reakcie na incidenty: Opiera sa o presné a úplné údaje v logoch pri detekcii, analýze a riešení udalostí informačnej bezpečnosti.

10.1.5 P23S – Politika synchronizácie času: Zabezpečuje konzistentné a sledovateľné časové pečiatky vo všetkých systémoch, čo umožňuje koreláciu logov počas vyšetrovania.

11. Referenčné normy a rámce

11.1 ISO/IEC 27001

11.1.1 Kapitola 8.1 – Vyžaduje zavedenie prevádzkových kontrol na zmiernenie rizík informačnej bezpečnosti vrátane logovania.

11.2 ISO/IEC 27002

11.2.1 Kontrola 8.15 – Vyžaduje logovanie udalostí na podporu detekcie anomálií a vyvoditeľnosti zodpovednosti.

11.2.2 Kontrola 8.16 – Vyžaduje ochranu logov pred manipuláciou a neoprávneným prístupom.

11.2.3 Kontrola 8.17 – Vyžaduje monitorovanie systémov z hľadiska neobvyklej činnosti a potvrdzovanie účinnosti monitorovacích kontrol.

11.3 NIST SP 800-53 Rev.5

11.3.1 AU-2 až AU-12 – Pokrývajú obsah auditných logov, ich preskúmavanie, uchovávanie a automatizované upozorňovanie.

11.3.2 SI-4 – Vyžaduje detekciu systémových anomálií a oznamovanie podozrivých udalostí.

11.4 Nariadenie EÚ GDPR

11.4.1 Článok 5(1)(f) – Vyžaduje integritu a dôvernosť osobných údajov, čo zahŕňa aj logovanie prístupu.

11.4.2 Článok 32 – Ukladá technické a organizačné opatrenia na zaistenie bezpečnosti vrátane logovania a monitorovania.

11.4.3 Článok 33 – Vyžaduje včasné oznámenie porušenia ochrany osobných údajov podporené logmi, ktoré umožňujú analýzu hlavnej príčiny.

11.5 Smernica EÚ NIS2

11.5.1 Článok 21(2)(d) – Vyžaduje mechanizmy logovania, ktoré detegujú anomálie a poskytujú podporu počas vyšetrovania incidentov.

11.5.2 Článok 23 – Ukladá oznamovanie incidentov do 24 hodín, čo závisí od presných a včasných údajov v logoch.

11.6 Nariadenie EÚ DORA

11.6.1 Článok 10 – Vyžaduje digitálnu prevádzkovú odolnosť vrátane sledovateľnosti incidentov súvisiacich s IKT prostredníctvom logovania.

11.6.2 Článok 15 – Ukladá monitorovanie poskytovateľov služieb vrátane prístupu k logom a práv na ich preskúmanie.

11.7 COBIT 2019

11.7.1 DSS01.03 – Vyžaduje sledovateľnosť systémovej činnosti prostredníctvom logovania a monitorovania.

11.7.2 DSS05.02 – Rieši logovanie ako kľúčovú kontrolu pri ochrane pred malvérom a inou neoprávnenou činnosťou.