					Sem zadajte názov registrovanej právnickej osoby							
Číslo dokumentu: P31S					Názov dokumentu: **Politika zberu dôkazov a forenznej analýzy**							
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**

V súlade s normami a predpismi

Norma/predpis	Kapitola/článok	Poznámka
ISO/IEC 27001:2022	Kapitoly 6.1, 6.3, 8	Plánovanie založené na riziku, opatrenia na zlepšovanie a prevádzkové kontroly na zabezpečenie integrity dôkazov
ISO/IEC 27002:2022	Kontroly 5.24–5.27	Usmerňujú bezpečné nakladanie, revízie po incidente a zlepšovanie na základe dôkazov
ISO/IEC 27035-3:2016	Kapitoly 6.3, 6.4, 7	Zabezpečuje riadne plánovanie, zákonný zber a bezpečné nakladanie s digitálnymi dôkazmi vrátane dokumentácie reťazca zverenia
NIST SP 800-53 Rev. 5	IR-07, IR-08, AU-09, AU-12, PE-18	Forenzná pripravenosť, ochrana auditných záznamov a účinná integrácia do reakcie na incidenty
GDPR EÚ	Články 33, 34	Dokumentácia a sledovateľnosť pri porušeniach ochrany osobných údajov
Smernica EÚ NIS2	Článok 23	Sledovateľné nahlasovanie incidentov a bezpečné nakladanie s dôkazmi
Nariadenie EÚ DORA	Článok 17(1), 17(2)	Zabezpečuje zber, uchovávanie a retenciu dôkazov pri incidentoch súvisiacich so systémami IKT, forenznú spoľahlivosť a podporu regulačných zisťovaní
COBIT 2019	DSS05.06, DSS05.07	Spoľahlivé logovanie a štruktúrované nakladanie s dôkazmi pre bezpečné a auditovateľné vyšetrovania

1. Účel

1.1. Táto politika stanovuje, ako organizácia nakladá s digitálnymi dôkazmi súvisiacimi s bezpečnostnými incidentmi, porušeniami ochrany údajov alebo internými vyšetrovaniami. Zabezpečuje, aby sa dôkazy zhromažďovali, uchovávali a zachovávali právne obhájiteľným spôsobom tak, aby podporovali pripravenosť na audit, interné rozhodovanie aj prípadné externé kroky.

1.2. Politika umožňuje malým organizáciám chrániť integritu logov, súborov a obrazov systémov a zároveň preukázať náležitú starostlivosť podľa ISO/IEC 27001, GDPR a súvisiacich noriem.

1.3. Podporuje forenznú pripravenosť bez potreby pokročilých technických zdrojov alebo interného IT tímu na plný úväzok tým, že vymedzuje jasné zodpovednosti, procesy a požiadavky na uchovávanie.

2. Rozsah

2.1. Táto politika sa vzťahuje na:

2.1.1. všetkých zamestnancov, poskytovateľov IT služieb a externých konzultantov zapojených do reakcie na incidenty, vyšetrovania alebo analýzy porušenia ochrany údajov,

2.1.2. všetky systémy spoločnosti vrátane notebookov, mobilných zariadení, serverov, e-mailových účtov, platforiem SaaS a cloudového úložiska (napr. Microsoft 365, Google Workspace),

2.1.3. každú udalosť vyžadujúcu dôkazy na účely interného disciplinárneho konania, právnej obhajoby, poistných nárokov alebo komunikácie s regulátorom.

2.2. To zahŕňa skutočné aj podozrivé udalosti súvisiace s:

2.2.1. únikom údajov,

2.2.2. vnútornou hrozbou alebo zneužitím,

2.2.3. bezpečnostnými incidentmi (napr. malvér, neoprávnený prístup),

2.2.4. sťažnosťami zákazníkov vyžadujúcimi digitálne overenie,

2.2.5. požiadavkami regulátorov alebo orgánov činných v trestnom konaní.

3. Ciele

3.1. Zabezpečiť, aby sa všetky dôkazy zhromažďovali a spracúvali spôsobom, ktorý zachováva ich integritu, autentickosť a reťazec zverenia.

3.2. Zabrániť náhodnej úprave, výmazu alebo nesprávnemu nakladaniu s logmi, súbormi alebo obrazmi systémov, ktoré môžu byť potrebné na vyšetrovanie.

3.3. Zaviesť konzistentný a auditovateľný prístup k správe dôkazov, ktorý spĺňa právne a regulačné očakávania (napr. oznamovanie porušenia ochrany údajov podľa GDPR, sledovateľnosť podľa NIS2).

3.4. Vymedziť jasné roly a zodpovednosti s cieľom zabezpečiť rýchle, bezpečné a právne súladné zaistenie dôkazov počas bezpečnostných incidentov.

3.5. Podporiť forenznú pripravenosť na úrovni MSP pri minimalizácii zložitosti a bez narušenia bežnej prevádzky.

4. Roly a zodpovednosti

4.1. Generálny manažér (GM)

4.1.1. schvaľuje všetky formálne vyšetrovania, ktoré vyžadujú zber dôkazov,

4.1.2. preskúmava a formálne schvaľuje správy o incidentoch zahŕňajúce možné právne alebo disciplinárne opatrenia,

4.1.3. rozhoduje o tom, či majú byť informovaní externí právni poradcovia alebo regulátori,

4.1.4. zabezpečuje pravidelné preskúmanie a aktualizáciu tejto politiky.

4.2. Poskytovateľ IT služieb / systémový administrátor

4.2.1. zhromažďuje a uchováva digitálne dôkazy v súlade s bezpečnými postupmi,

4.2.2. dokumentuje časové pečiatky, údaje o systémoch a jednotlivé kroky pri nakladaní s dôkazmi,

4.2.3. zabezpečuje všetky zhromaždené materiály v chránenom úložisku,

4.2.4. podľa potreby podporuje forenznú analýzu.

[... 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 politiky

9.1.1. Túto politiku musí generálny manažér (GM) preskúmať najmenej raz za 12 mesiacov s cieľom potvrdiť:

9.1.1.1. súlad s kontrolami prílohy A normy ISO/IEC 27001,

9.1.1.2. priebežnú relevantnosť pre aktuálne digitálne platformy a IT služby,

9.1.1.3. primeranosť postupov logovania, uchovávania dôkazov a forenznej pripravenosti.

9.2. Spúšťacie udalosti na revíziu politiky

9.2.1. Politika sa musí preskúmať a aktualizovať aj po:

9.2.1.1. každom závažnom incidente vyžadujúcom zber dôkazov,

9.2.1.2. neúspešnom audite alebo regulačnej požiadavke, pri ktorých bola spochybnená integrita dôkazov,

9.2.1.3. zavedení nových nástrojov alebo postupov na reakciu na incidenty alebo monitorovanie systémov,

9.2.1.4. právnych zmenách (napr. aktualizované usmernenia GDPR alebo NIS2).

9.3. Schvaľovanie zmien a distribúcia

9.3.1. Všetky zmeny musí preskúmať a schváliť GM.

9.3.2. Aktualizovaná verzia musí byť sprístupnená:

9.3.2.1. poskytovateľom IT služieb a konzultantom zapojeným do vyšetrovaní,

9.3.2.2. všetkým pracovníkom so zodpovednosťou za správu systémov.

9.3.3. Aktualizovaná kópia sa musí uchovávať v archíve politík spoločnosti a na požiadanie sprístupniť audítorom.

10. Súvisiace politiky a väzby

10.1. Táto politika je vzájomne previazaná s týmito politikami zosúladenými pre MSP:

10.1.1. P2S – Politika rolí a zodpovedností v oblasti správy a riadenia: stanovuje právomoci pri vyšetrovaní incidentov, rozhodovaní o dôkazoch a právnej eskalácii.

10.1.2. P4S – Politika riadenia prístupu: zabezpečuje, aby počas vyšetrovania mali prístup k citlivým systémom a logom len autorizované osoby.

10.1.3. P22S – Politika logovania a monitorovania: poskytuje primárne údaje používané ako forenzné dôkazy a stanovuje požiadavky na uchovávanie, riadenie prístupu a logovanie.

10.1.4. P30S – Politika reakcie na incidenty: spúšťa potrebu zberu dôkazov a vymedzuje prevádzkový postup vedúci k ich forenznému zachovaniu.

10.1.5. P17S – Politika ochrany údajov a súkromia: zabezpečuje, aby sa s osobnými údajmi zhromaždenými ako dôkaz nakladalo zákonným spôsobom podľa GDPR a súvisiacich predpisov.

10.2. Tieto politiky spoločne podporujú právnu obhájiteľnosť, integritu vyšetrovania a plnú pripravenosť na audit podľa ISO/IEC 27001:2022.

11. Referenčné normy a rámce

11.1. ISO/IEC 27001

11.1.1. Kapitola 6.1 – Plánovanie založené na riziku zahŕňa pripravenosť na reakciu a postupy nakladania s dôkazmi.

11.1.2. Kapitola 6.3 – Podporuje opatrenia na zlepšovanie na základe dôkazov z incidentov.

11.1.3. Kapitola 8.1 – Vyžaduje prevádzkové kontroly na zabezpečenie integrity dôkazov.

11.2. ISO/IEC 27002

11.2.1. Kontroly 5.24–5.27 – Usmerňujú bezpečné nakladanie, revízie po incidente a zlepšovanie na základe dôkazov.

11.3. ISO/IEC 27035-3

11.3.1. Kapitoly 6.3, 6.4 a 7.3 zabezpečujú riadne plánovanie, zákonný zber a bezpečné nakladanie s digitálnymi dôkazmi počas reakcie na incidenty vrátane ich zachovania a dokumentácie reťazca zverenia.

11.4. NIST SP 800-53 Rev. 5

11.4.1. IR-07, IR-08, AU-09 a AU-12 zabezpečujú forenznú pripravenosť, ochranu auditných záznamov a účinnú integráciu zberu dôkazov do životného cyklu reakcie na incidenty.

11.5. NIST SP 800-86

11.5.1. Definuje osvedčené postupy na získavanie, analýzu a ochranu digitálnych dôkazov počas reakcie na incidenty.

11.6. GDPR EÚ

11.6.1. Články 33–34 – Vyžadujú dokumentáciu a sledovateľnosť incidentov a dôkazov pri oznamovaní porušenia ochrany osobných údajov.

11.7. Smernica EÚ NIS2 (2022/2555)

11.7.1. Článok 23 – Vyžaduje sledovateľné nahlasovanie incidentov a bezpečné nakladanie s dôkazmi pre základné a dôležité subjekty.

11.8. Nariadenie EÚ DORA

11.8.1. Článok 17(1) – Zabezpečuje, aby sa dôkazy súvisiace s incidentmi týkajúcimi sa systémov IKT zhromažďovali a uchovávali spôsobom podporujúcim forenzné vyšetrovania.

11.8.2. Článok 17(2) – Vyžaduje, aby finančné subjekty uchovávali všetky relevantné údaje a logy súvisiace s bezpečnostnými udalosťami v súlade s požiadavkami forenznej spoľahlivosti a regulačných zisťovaní.

11.9. COBIT 2019

11.9.1. DSS05.06 – Monitorovanie, detekcia a nahlasovanie incidentov: zdôrazňuje spoľahlivé logovanie na podporu vyšetrovania.

11.9.2. DSS05.07 – Vyšetrovanie incidentov a prijímanie opatrení: vyžaduje štruktúrované nakladanie s dôkazmi na umožnenie bezpečných a auditovateľných vyšetrovaní.