					Sem zadajte názov registrovanej právnickej osoby							
Číslo dokumentu: P31					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**

Právne upozornenie (autorské práva a obmedzenia používania)

(C) 2025 Clarysec LLC. All rights reserved.

Tento dokument je duševným vlastníctvom spoločnosti Clarysec LLC. Žiadna časť tohto dokumentu nesmie byť bez predchádzajúceho výslovného písomného súhlasu kopírovaná, znovu použitá, distribuovaná ani upravovaná na komerčné alebo implementačné účely.
Neoprávnené použitie je prísne zakázané a môže viesť k právnym krokom.
V prípade licencovania kontaktujte: info@clarysec.com

V súlade s normami a predpismi

Norma/predpis	Kapitola/článok	Poznámka
ISO/IEC 27001:2022	Kapitola 8	
ISO/IEC 27002:2022	Kontroly 5.25–5.27, 8	
ISO/IEC 27035:2016	Časti 1 a 3	
NIST SP 800-53 Rev. 5	IR-1 až IR-9, AU-6, PL-2	
NIST SP 800-101 Rev. 1	Mobilná a mediálna forenzná analýza	Mobilná a mediálna forenzná analýza
NIST SP 800-86	Integrácia forenzných techník	Integrácia forenzných techník do reakcie na incidenty
Nariadenie EÚ GDPR	Článok 5, 33–34	
Smernica EÚ NIS2	Článok 23 ods. 1–4	
Nariadenie EÚ DORA	Článok 17 ods. 1–3	
COBIT 2019	DSS01.07, DSS05	

1. Účel

1.1 Táto politika stanovuje štruktúrovaný a právne obhájiteľný rámec na identifikáciu, zber, uchovávanie, analýzu a likvidáciu digitálnych dôkazov počas potvrdených alebo podozrivých bezpečnostných incidentov.

1.2 Zabezpečuje, aby procesy forenznej pripravenosti a nakladania s dôkazmi:

1.2.1 zachovávali integritu dôkazov a reťazec zaistenia

1.2.2 podporovali interné vyšetrovania, súdne konania alebo regulačné oznamovanie

1.2.3 boli v súlade s medzinárodne uznávanými forenznými normami a kritériami právnej prípustnosti

1.3 Táto politika podporuje záväzok organizácie k proaktívnej reakcii na incidenty, dodržiavaniu právnych požiadaviek a transparentnej správe a riadeniu pri súčasnej minimalizácii prevádzkových narušení.

2. Rozsah

2.1 Táto politika sa vzťahuje na:

2.1.1 všetkých zamestnancov, zmluvných pracovníkov, dodávateľov a poskytovateľov služieb zapojených do správy systémov, riešenia incidentov alebo vyšetrovacích činností

2.1.2 všetky koncové zariadenia, servery, aplikácie, siete a cloudové platformy pod kontrolou organizácie alebo v jej zmluvnej zodpovednosti

2.1.3 každý incident alebo udalosť vyžadujúce nakladanie s dôkazmi vrátane:

2.1.3.1 vnútorných hrozieb, porušení ochrany osobných údajov alebo vyšetrovania podvodov

2.1.3.2 zneužitia systémov alebo prihlasovacích údajov

2.1.3.3 incidentov v systémoch prevádzkových technológií (OT) alebo priemyselných riadiacich systémoch

2.1.3.4 narušení fyzického prístupu zahŕňajúcich digitálne aktíva

2.2 Táto politika upravuje aj akúkoľvek interakciu s externými forenznými službami alebo orgánmi činnými v trestnom konaní počas právnej alebo regulačnej eskalácie alebo regulačných konaní.

3. Ciele

3.1 Umožniť rýchle, bezpečné a s politikou zosúladené získavanie dôkazov počas bezpečnostných udalostí alebo vyšetrovaní.

3.2 Zachovať integritu, autentickosť a prípustnosť zhromaždených digitálnych dôkazov prostredníctvom prísneho riadenia prístupu, protokolovania a overovacích postupov.

3.3 Zabezpečiť, aby všetky forenzné činnosti boli koordinované so zákonnými a regulačnými povinnosťami vrátane ochrany osobných údajov, pracovného práva a obmedzení medzinárodných prenosov.

3.4 Podporiť poincidentnú analýzu, určenie hlavnej príčiny a zlepšovanie kontrol prostredníctvom kvalitných forenzných výstupov.

3.5 Integrovať forenznú pripravenosť do celkového systému manažérstva informačnej bezpečnosti (ISMS) s podporou auditov, oznamovania porušení ochrany osobných údajov a rozhodovania vrcholového manažmentu.

4. Roly a zodpovednosti

4.1 riaditeľ informačnej bezpečnosti (CISO)

4.1.1 je vlastníkom tejto politiky a zabezpečuje, aby všetky forenzné operácie boli právne obhájiteľné, auditovateľné a založené na riziku

4.1.2 schvaľuje eskaláciu voči externým právnym subjektom a poskytovateľom forenzných služieb

4.2 forenzní analytici / pracovníci riešenia incidentov

4.2.1 vykonávajú získavanie, uchovávanie a technickú analýzu dôkazov

4.2.2 zabezpečujú riadne zaznamenanie a udržiavanie reťazca zaistenia

4.2.3 dokumentujú všetky činnosti, zistenia a nastavenia nástrojov použité počas vyšetrovaní

[... 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 najmenej raz ročne a podľa potreby aktualizovaná tak, aby zohľadňovala:

9.1.1 zmeny zákonov, predpisov alebo judikatúry ovplyvňujúce forenzné postupy alebo nakladanie s údajmi

9.1.2 aktualizácie odvetvovo uznávaných forenzných noriem alebo nástrojov

9.1.3 poznatky z poincidentných preskúmaní, právnych sporov alebo auditných zistení

9.1.4 technologické zmeny platforiem, zariadení alebo systémov, ktoré sú predmetom vyšetrovania

9.2 Za proces preskúmania zodpovedá CISO a musí zahŕňať konzultácie s:

9.2.1 právnym oddelením a compliance

9.2.2 zodpovednou osobou pre ochranu osobných údajov (DPO)

9.2.3 tímami bezpečnostných operácií a forenznej analýzy

9.2.4 interným auditom

9.3 Všetky revízie musia byť:

9.3.1 riadené verziami a uložené v úložisku politík

9.3.2 oznámené dotknutým zainteresovaným stranám vrátane forenzných tímov a tímov reakcie na incidenty

9.3.3 sprevádzané aktualizáciami príslušných prevádzkových postupov a školiacich materiálov

9.4 Mimoriadne preskúmania sa musia vykonať po každom kritickom incidente zahŕňajúcom nesprávne nakladanie s dôkazmi, zlyhanie reťazca zaistenia alebo problémy s právnou prípustnosťou.

10. Súvisiace politiky a väzby

10.1 Táto politika je zosúladená s nasledujúcimi organizačnými politikami a podporovaná nimi:

10.1.1 P1 – Politika informačnej bezpečnosti: stanovuje základný mandát pre vyšetrovanie, správu dôkazov a súlad s príslušnými právnymi predpismi.

10.1.2 P5 – Politika riadenia zmien: zabezpečuje, aby systémy, ktoré sú predmetom vyšetrovania, neboli počas aktívnych forenzných procesov menené.

10.1.3 P14 – Politika uchovávania a likvidácie údajov: upravuje bezpečnú likvidáciu a lehoty uchovávania dôkazov a údajov súvisiacich s prípadom.

10.1.4 P18 – Politika kryptografických kontrol: stanovuje požiadavky na šifrovanie pri ukladaní a prenose citlivých údajov alebo dôkazových údajov.

10.1.5 P22 – Politika protokolovania a monitorovania: zabezpečuje dostupnosť protokolov udalostí a telemetrie pre zber dôkazov a forenznú koreláciu.

10.1.6 P30 – Politika reakcie na incidenty: vymedzuje triáž incidentov a eskalačné postupy, pri ktorých sa začínajú forenzné postupy.

10.1.7 P33 – Politika monitorovania auditu a compliance: prostredníctvom pravidelných auditov overuje dodržiavanie forenzných protokolov a požiadaviek na reťazec zaistenia.

11. Referenčné normy a rámce

11.1 Táto politika je zosúladená s medzinárodnými normami pre forenznú analýzu a riešenie incidentov a zabezpečuje integritu dôkazov, právnu obhájiteľnosť a súlad naprieč jurisdikciami.

11.2 ISO/IEC 27001

11.2.1 Kapitola 8.1 – Podporuje prevádzkové riadenie forenznej pripravenosti a postupov nakladania s dôkazmi.

11.3 ISO/IEC 27002

11.3.1 Príloha A Kontrola 5.25 – Zodpovednosti za riadenie incidentov: vyžaduje vymedzené roly pri riešení incidentov informačnej bezpečnosti a vyšetrovaniach.

11.3.2 Príloha A Kontrola 5.26 – Nahlasovanie udalostí informačnej bezpečnosti: podporuje zber artefaktov súvisiacich s udalosťami ako dôkazov.

11.3.3 Príloha A Kontrola 5.27 – Reakcia na incidenty informačnej bezpečnosti: vyžaduje štruktúrované nápravné opatrenia a vyšetrovanie založené na dôkazoch.

11.3.4 Príloha A Kontrola 8.27 – Bezpečný vývoj a forenzná analýza (ak je to relevantné): rieši ochranu systémov a nástrojov počas vyšetrovaní.

11.4 ISO/IEC 27035:2016 (časti 1 a 3)

11.4.1 Stanovuje zásady detekcie incidentov, reakcie a forenznej pripravenosti vrátane plánovania, reťazca zaistenia a riadenia dôkazov o incidentoch.

11.5 NIST SP 800-53 Rev. 5

11.5.1 IR-1 až IR-9, AU-6, PL-2: definujú štruktúrované požiadavky na plánovanie, detekciu, analýzu, zamedzenie šírenia a reakciu na bezpečnostné incidenty. Podporujú zber dôkazov a ich auditovateľnosť (AU-6) a zabezpečujú zosúladenie s plánmi bezpečnosti systému a ochrany súkromia (PL-2) počas forenzných vyšetrovaní.

11.6 NIST SP 800-86

11.6.1 Poskytuje usmernenia na integráciu forenzných procesov do širšieho životného cyklu reakcie na incidenty a na zabezpečenie forenznej pripravenosti.

11.7 NIST SP 800-101 Rev. 1

11.7.1 Zameriava sa na osvedčené postupy získavania, uchovávania a analýzy digitálnych médií a dôkazov z mobilných zariadení právne obhájiteľným spôsobom.

11.8 Nariadenie EÚ GDPR (2016/679)

11.8.1 Článok 5 – Zásady spracúvania osobných údajov: vzťahuje sa na dôkazy obsahujúce osobné alebo citlivé údaje a zabezpečuje minimalizáciu a obmedzenie účelu.

11.8.2 Články 33–34 – Oznámenie porušenia ochrany osobných údajov: forenzné údaje podporujú súlad s oznamovacími povinnosťami pri porušení ochrany osobných údajov a s procesmi právneho zverejnenia.

11.9 Smernica EÚ NIS2 (2022/2555)

11.9.1 Článok 23 – Oznamovacie povinnosti: forenzná dokumentácia a zistenia podporujú včasné a presné hlásenie incidentov príslušným orgánom.

11.10 Nariadenie EÚ DORA (2022/2554)

11.10.1 Článok 17 – Nahlasovanie incidentov IKT: vyžaduje podrobné záznamy o hlavnej príčine a dôkazový materiál pri významných incidentoch súvisiacich s IKT, najmä vo finančnom sektore.

11.11 COBIT 2019

11.11.1 DSS01.07 – Riadenie bezpečnostných incidentov: vyžaduje dokumentovanie incidentov a dôsledný vyšetrovací prístup.

11.11.2 DSS05.04 – Riadenie bezpečnostných vyšetrovaní: zdôrazňuje zachovanie digitálnych dôkazov a podporu disciplinárnych a právnych krokov.