					Sem vložte název registrované právnické osoby							
Číslo dokumentu: P31S					Název dokumentu: **Politika zajišťování důkazů a forenzního šetření**							
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**

Právní upozornění (autorská práva a omezení užití)

(C) 2025 Clarysec LLC. All rights reserved.

Tento dokument je duševním vlastnictvím společnosti Clarysec LLC. Žádná jeho část nesmí být kopírována, znovu použita, distribuována ani upravována pro komerční nebo implementační účely bez výslovného písemného souhlasu.

Neoprávněné použití je přísně zakázáno a může vést k právním krokům.

V případě licencování kontaktujte: info@clarysec.com

V souladu s normami a právními předpisy

Norma / právní předpis	Kapitola / článek	Komentář
ISO/IEC 27001:2022	Kapitoly 6.1, 6.3, 8	Plánování založené na rizicích, opatření ke zlepšování a provozní kontroly pro zajištění integrity důkazů
ISO/IEC 27002:2022	Opatření 5.24–5.27	Poskytuje vodítka pro bezpečné nakládání, přezkoumání po incidentu a zlepšování založené na důkazech
ISO/IEC 27035-3:2016	Kapitoly 6.3, 6.4, 7	Zajišťuje řádné plánování, zákonné shromažďování a bezpečné nakládání s digitálními důkazy včetně dokumentace řetězce svěření
NIST SP 800-53 Rev. 5	IR-07, IR-08, AU-09, AU-12, PE-18	Forenzní připravenost, ochrana auditních záznamů a účinné začlenění do reakce na incidenty
GDPR	Články 33, 34	Dokumentace a dohledatelnost porušení zabezpečení osobních údajů
směrnice NIS2	Článek 23	Dohledatelné hlášení incidentů a bezpečné nakládání s důkazy
nařízení DORA	Článek 17(1), 17(2)	Zajišťuje sběr, ukládání a uchovávání důkazů pro incidenty související s ICT, forenzní správnost a regulační šetření
COBIT 2019	DSS05.06, DSS05.07	Spolehlivé protokolování a strukturované nakládání s důkazy pro bezpečné a auditovatelné vyšetřování

1. Účel

1.1. Tato politika stanoví, jak organizace nakládá s digitálními důkazy souvisejícími s bezpečnostními incidenty, porušením zabezpečení dat nebo interním vyšetřováním. Zajišťuje, aby byly důkazy shromažďovány, ukládány a uchovávány právně obhajitelným způsobem a tak, aby bylo možné při auditu doložit soulad, čímž podporuje jak interní rozhodování, tak případné externí kroky.

1.2. Politika umožňuje malým organizacím chránit integritu logů, souborů a obrazů systémů a současně prokazovat náležitou péči podle ISO/IEC 27001, GDPR a souvisejících norem.

1.3. Podporuje forenzní připravenost bez požadavku na pokročilé technické zdroje nebo interní IT tým na plný úvazek tím, že vymezuje jasné odpovědnosti, postupy a požadavky na uchovávání.

2. Rozsah

2.1. Tato politika se vztahuje na:

2.1.1. všechny zaměstnance, poskytovatele IT služeb a externí konzultanty zapojené do reakce na incidenty, vyšetřování nebo analýzy narušení,

2.1.2. všechny firemní systémy včetně notebooků, mobilních zařízení, serverů, e-mailových účtů, platforem SaaS a cloudových úložišť (např. Microsoft 365, Google Workspace),

2.1.3. jakoukoli událost vyžadující důkazy pro interní disciplinární opatření, právní obhajobu, pojistné události nebo komunikaci s regulačním orgánem.

2.2. To zahrnuje skutečné i podezřelé události související s:

2.2.1. únikem dat,

2.2.2. vnitřní hrozbou nebo zneužitím,

2.2.3. bezpečnostním incidentem (např. malware, neoprávněný přístup),

2.2.4. stížnostmi zákazníků vyžadujícími digitální ověření,

2.2.5. dotazy regulačních orgánů nebo orgánů činných v trestním řízení.

3. Cíle

3.1. Zajistit, aby byly všechny důkazy shromažďovány a zpracovávány způsobem, který zachovává jejich integritu, autenticitu a řetězec svěření.

3.2. Zabránit náhodné změně, smazání nebo nesprávnému nakládání s logy, soubory nebo obrazy systémů, které mohou být potřebné pro vyšetřování.

3.3. Zavést konzistentní a auditovatelný přístup ke správě důkazů, který splňuje právní a regulatorní očekávání (např. oznamování porušení podle GDPR, dohledatelnost podle NIS2).

3.4. Vymezit jasné role a odpovědnosti k zajištění rychlého, bezpečného a právně souladného zajištění důkazů během bezpečnostních incidentů.

3.5. Podporovat forenzní připravenost na úrovni SME při minimalizaci složitosti a bez narušení každodenního provozu.

4. Role a odpovědnosti

4.1. generální ředitel (GM)

4.1.1. Schvaluje všechna formální vyšetřování, která vyžadují sběr důkazů.

4.1.2. Přezkoumává a schvaluje zprávy o incidentech zahrnujících možné právní nebo disciplinární kroky.

4.1.3. Rozhoduje, zda mají být informováni externí právní zástupci nebo regulační orgány.

4.1.4. Zajišťuje pravidelný přezkum a aktualizaci této politiky.

4.2. poskytovatel IT služeb / správce systému

4.2.1. Shromažďuje a uchovává digitální důkazy v souladu s bezpečnými postupy.

4.2.2. Dokumentuje časová razítka, podrobnosti o systémech a jednotlivé kroky při nakládání s důkazy.

4.2.3. Zabezpečuje veškeré shromážděné materiály v chráněném úložišti.

4.2.4. V případě potřeby poskytuje součinnost při forenzní analýze.

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

9. Požadavky na přezkum a aktualizaci

9.1. Každoroční přezkum politiky

9.1.1. Tato politika musí být nejméně jednou za 12 měsíců přezkoumána generálním ředitelem (GM), aby bylo potvrzeno:

9.1.1.1. dodržování opatření přílohy A normy ISO/IEC 27001,

9.1.1.2. trvající relevance pro aktuální digitální platformy a IT služby,

9.1.1.3. přiměřenost postupů protokolování, uchovávání důkazů a forenzní připravenosti.

9.2. Události vyžadující aktualizaci politiky

9.2.1. Politika musí být rovněž přezkoumána a aktualizována po:

9.2.1.1. jakémkoli závažném incidentu vyžadujícím sběr důkazů,

9.2.1.2. neúspěšném auditu nebo požadavku regulačního orgánu, při němž byla zpochybněna integrita důkazů,

9.2.1.3. zavedení nových nástrojů nebo postupů pro reakci na incidenty nebo monitorování systémů,

9.2.1.4. právních změnách (např. aktualizovaných pokynech k GDPR nebo NIS2).

9.3. Schvalování změn a distribuce

9.3.1. Všechny změny musí být přezkoumány a schváleny generálním ředitelem (GM).

9.3.2. Aktualizované znění musí být sdíleno s:

9.3.2.1. poskytovateli IT služeb a konzultanty zapojenými do vyšetřování,

9.3.2.2. veškerým personálem s odpovědností za správu systémů.

9.3.3. Aktualizovaná kopie musí být uchována v archivu politik společnosti a na vyžádání sdílena auditorům.

10. Související politiky a vazby

10.1. Tato politika je provázána s následujícími politikami přizpůsobenými pro SME:

10.1.1. P2S – Politika rolí a odpovědností v oblasti správy a řízení: stanoví pravomoci pro vyšetřování incidentů, rozhodování o důkazech a právní eskalaci.

10.1.2. P4S – Politika řízení přístupu: zajišťuje, že během vyšetřování mají přístup k citlivým systémům a logům pouze autorizované osoby.

10.1.3. P22S – Politika protokolování a monitorování: poskytuje primární data používaná jako forenzní důkazy a stanoví požadavky na uchovávání, řízení přístupu a protokolování.

10.1.4. P30S – Politika reakce na incidenty: zakládá potřebu sběru důkazů a vymezuje provozní postup vedoucí k forenznímu uchování.

10.1.5. P17S – Politika ochrany dat a soukromí: zajišťuje, že s osobními údaji shromážděnými jako důkazy je nakládáno zákonně podle GDPR a souvisejících předpisů.

10.2. Tyto politiky společně podporují právní obhajitelnost, integritu vyšetřování a připravenost na audit podle ISO/IEC 27001:2022.

11. Referenční normy a rámce

11.1. ISO/IEC 27001

11.1.1. Kapitola 6.1 – Plánování založené na rizicích zahrnuje připravenost na reakci a postupy práce s důkazy.

11.1.2. Kapitola 6.3 – Podporuje opatření ke zlepšování založená na důkazech z incidentů.

11.1.3. Kapitola 8.1 – Vyžaduje provozní kontroly pro zajištění integrity důkazů.

11.2. ISO/IEC 27002

11.2.1. Opatření 5.24–5.27 – Poskytují vodítka pro bezpečné nakládání, přezkoumání po incidentu a zlepšování založené na důkazech.

11.3. ISO/IEC 27035-3

11.3.1. Kapitoly 6.3, 6.4 a 7.3 zajišťují řádné plánování, zákonné shromažďování a bezpečné nakládání s digitálními důkazy během reakce na incidenty, včetně uchování a dokumentace řetězce svěření.

11.4. NIST SP 800-53 Rev. 5

11.4.1. IR-07, IR-08, AU-09 a AU-12 zajišťují forenzní připravenost, ochranu auditních záznamů a účinné začlenění sběru důkazů do životního cyklu reakce na incidenty.

11.5. NIST SP 800-86

11.5.1. Definuje osvědčené postupy pro zajištění, analýzu a ochranu digitálních důkazů během reakce na incidenty.

11.6. GDPR

11.6.1. Články 33–34 – Vyžadují dokumentaci a dohledatelnost incidentů a důkazů při oznamování porušení zabezpečení osobních údajů.

11.7. směrnice NIS2 (2022/2555)

11.7.1. Článek 23 – Vyžaduje dohledatelné hlášení incidentů a bezpečné nakládání s důkazy pro základní a důležité subjekty.

11.8. nařízení DORA

11.8.1. Článek 17(1) – Zajišťuje, aby byly důkazy související s incidenty v oblasti ICT shromažďovány a ukládány způsobem podporujícím forenzní vyšetřování.

11.8.2. Článek 17(2) – Vyžaduje, aby finanční subjekty uchovávaly veškerá relevantní data a logy spojené s bezpečnostními událostmi v souladu s požadavky na forenzní správnost a regulační šetření.

11.9. COBIT 2019

11.9.1. DSS05.06 – monitorovat, detekovat a hlásit incidenty: zdůrazňuje spolehlivé protokolování pro podporu vyšetřování.

11.9.2. DSS05.07 – vyšetřovat incidenty a přijímat opatření: vyžaduje strukturované nakládání s důkazy, které umožňuje bezpečné a auditovatelné vyšetřování.