					Sem zadajte názov registrovanej právnickej osoby							
Číslo dokumentu: P14S					Názov dokumentu: **Politika uchovávania a likvidácie údajov**							
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**

Súlad s normami a predpismi

Norma/predpis	Kapitola/článok	Poznámka
ISO/IEC 27001:2022	Kapitoly 6.1.3, 8	Zahŕňa ošetrenie rizík, prevádzkové opatrenia a požiadavky na uchovávanie
ISO/IEC 27002:2022	Kontrola 5	Usmernenie k lehotám uchovávania a metódam bezpečnej likvidácie
NIST SP 800-53 Rev.5	AU-11, MP-6, SI-12	Uchovávanie auditných záznamov, sanitizácia médií, limity uchovávania údajov a ich presadzovanie
Smernica EÚ NIS2	Článok 21(2)(a)	Vyžaduje politiku riadenia životného cyklu primeranú riziku
Nariadenie EÚ DORA	Článok 5(1)	Riadenie rizík IKT: dostupnosť a odstraňovanie údajov
COBIT 2019	BAI03.04, DSS01	Kontroly životného cyklu informácií, bezpečná likvidácia
Nariadenie EÚ GDPR	Článok 5(1)(e), 17	Údaje sa nesmú uchovávať dlhšie, než je nevyhnutné; právo na vymazanie

1. Účel

1.1 Účelom tejto politiky je stanoviť záväzné pravidlá pre uchovávanie a bezpečnú likvidáciu informácií v prostredí MSP. Zabezpečuje, aby sa záznamy uchovávali len počas obdobia vyžadovaného právnymi predpismi, zmluvnými záväzkami alebo prevádzkovou potrebou a aby boli následne bezpečne zlikvidované.

1.2 Cieľom tejto politiky je znižovať informačné riziká, riadiť právnu expozíciu a obmedziť uchovávanie redundantných alebo zastaraných údajov. Podporuje súlad s ISO/IEC 27001 a rámcami ochrany súkromia, ako je GDPR, tým, že minimalizuje neoprávnené uchovávanie osobných alebo citlivých informácií.

1.3 Dobre nastavený rámec uchovávania a likvidácie znižuje prevádzkové náklady, zlepšuje výkonnosť systémov a zvyšuje pripravenosť na audit. Pre MSP s obmedzenými IT kapacitami predstavuje praktický spôsob zodpovedného riadenia digitálnych a fyzických informačných aktív.

2. Rozsah

2.1 Táto politika sa vzťahuje na:

2.1.1 všetky záznamy, súbory, logy, komunikáciu a dátové súbory vytvorené, zhromaždené, spracúvané alebo uchovávané organizáciou,

2.1.2 všetkých zamestnancov, zmluvných pracovníkov a externých poskytovateľov, ktorí nakladajú s údajmi organizácie,

2.1.3 všetky formáty údajov (napr. papierové, elektronické, obrazové, zvukové alebo logy) a všetky typy úložných médií (napr. lokálne disky, cloudové služby, e-mailové servery, zálohy).

2.2 Rozsah zahŕňa:

2.2.1 podnikové dokumenty (napr. faktúry, zmluvy, projektové správy),

2.2.2 prevádzkové záznamy (napr. logy, história prístupov, snímky záloh),

2.2.3 osobné údaje (napr. personálne spisy, komunikácia s klientmi, záznamy podpory),

2.2.4 údaje hostované interne, externe alebo v hybridných systémoch,

2.2.5 archivované a záložné údaje, či už aktívne alebo neaktívne.

2.3 Rozsah sa vzťahuje na všetky etapy životného cyklu údajov od ich vytvorenia až po autorizovanú likvidáciu.

3. Ciele

3.1 Stanoviť konzistentné pravidlá uchovávania na základe právnych, prevádzkových a regulačných kritérií.

3.2 Predchádzať predčasnému vymazaniu kritických záznamov a eliminovať zbytočné hromadenie údajov.

3.3 Zabezpečiť bezpečnú a nezvratnú likvidáciu údajov, keď ich uchovávanie už nie je potrebné.

3.4 Jednoznačne priradiť zodpovednosť za uplatňovanie rozhodnutí o uchovávaní a vymazávaní v podmienkach personálnych obmedzení typických pre MSP.

3.5 Poskytovať dokumentáciu vhodnú na audit na preukázanie náležitej starostlivosti podľa ISO 27001, GDPR, NIS2 a ďalších rámcov.

3.6 Podporovať bezpečné nakladanie s údajmi počas celého ich životného cyklu bez zbytočného technického zaťaženia pre nešpecializovaný personál.

4. Roly a zodpovednosti

4.1 Generálny manažér (GM)

4.1.1 schvaľuje túto politiku a nesie za ňu celkovú zodpovednosť,

4.1.2 zabezpečuje, aby sa postupy uchovávania a likvidácie uplatňovali spôsobom zodpovedajúcim právnym rizikám a rizikám pre organizáciu,

4.1.3 v prípade potreby schvaľuje výnimky a právne uchovanie s pozastavením výmazu,

4.1.4 iniciuje preskúmania politiky a schvaľuje aktualizácie na základe zmien v organizácii alebo regulačnom prostredí.

4.2 Určený vlastník údajov

4.2.1 je určený pre každú kategóriu údajov (napr. finančné, personálne, klientské záznamy),

4.2.2 klasifikuje záznamy a určuje primeranú dobu uchovávania podľa tejto politiky a právnych usmernení,

4.2.3 schvaľuje vymazanie po splnení požiadaviek na uchovávanie,

4.2.4 podporuje interné audity poskytovaním kontextu k logike uchovávania a udalostiam likvidácie.

[... 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 alebo pri:

9.1.1 zmenách príslušných právnych predpisov (napr. ochrana údajov, finančné výkazníctvo),

9.1.2 zavedení nových systémov alebo procesov, ktoré ovplyvňujú životný cyklus údajov,

9.1.3 auditných zisteniach alebo incidentoch odhaľujúcich nedostatky v postupoch uchovávania.

9.2 Preskúmania musia zabezpečiť, aby register uchovávania zostal úplný a odrážal všetky hlavné kategórie záznamov.

9.3 Aktualizácie politiky musí schváliť GM a musia byť oznámené dotknutým pracovníkom. Najnovšia verzia musí byť prístupná a riadená v súlade s pravidlami verziovania.

10. Súvisiace politiky a väzby

10.1 P2S – Politika rolí a zodpovedností v oblasti správy a riadenia: Definuje vlastníctvo politiky a právomoc schvaľovať výnimky.

10.2 P13S – Politika klasifikácie a označovania údajov: Určuje, ako sa pravidlá uchovávania zosúlaďujú s klasifikáciou údajov.

10.3 P12S – Politika správy aktív: Upravuje úložné médiá obsahujúce údaje podliehajúce uchovávaniu a likvidácii.

10.4 P17S – Politika ochrany údajov a súkromia: Zabezpečuje minimalizáciu údajov a podporuje zákonné spracúvanie podľa GDPR.

10.5 P30S – Politika reakcie na incidenty: Aktivuje sa, keď zlyhania pri likvidácii alebo uchovávaní vedú k možnému sprístupneniu údajov.

11. Referenčné normy a rámce

11.1 ISO/IEC 27001

11.1.1 Kapitola 6.1.3: Vyžaduje ošetrenie rizík súvisiacich s informáciami vrátane rizík spojených s uchovávaním.

11.1.2 Kapitola 8.1: Definuje prevádzkové opatrenia životného cyklu.

11.2 ISO/IEC 27002

11.2.1 Kontrola 5.33: Usmernenie na stanovenie lehôt uchovávania a metód bezpečného zničenia.

11.3 NIST SP 800-53 Rev. 5

11.3.1 AU-11: Vyžaduje uchovávanie auditných záznamov.

11.3.2 MP-6: Definuje postupy sanitizácie médií.

11.3.3 SI-12: Rieši limity uchovávania údajov a ich uplatňovanie.

11.4 Nariadenie EÚ GDPR

11.4.1 Článok 5(1)(e): Údaje sa nesmú uchovávať dlhšie, než je nevyhnutné.

11.4.2 Článok 17: Právo na vymazanie sa uplatňuje, keď sa údaje už neuchovávajú zákonným spôsobom.

11.5 Smernica EÚ NIS

11.5.1 Článok 21(2)(a): Vyžaduje organizačné politiky primerané riziku vrátane riadenia životného cyklu.

11.6 Nariadenie EÚ DORA

11.6.1 Článok 5(1): Riadenie rizík IKT zahŕňa dostupnosť a odstraňovanie údajov.

11.7 COBIT 2019

11.7.1 BAI03.04: Vyžadujú sa kontroly životného cyklu informácií.

11.7.2 DSS01.06: Postupy bezpečnej likvidácie ako súčasť ochrany informačných aktív.