					Sem vložte název registrované právnické osoby							
Číslo dokumentu: P14S					Název dokumentu: **Politika uchovávání údajů**							
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**

V souladu s normami a právními předpisy

Norma / právní předpis	Článek / ustanovení	Komentář
ISO/IEC 27001:2022	Články 6.1.3, 8	Zahrnuje ošetření rizik, provozní opatření a požadavky na uchovávání
ISO/IEC 27002:2022	Opatření 5	Pokyny k dobám uchovávání a metodám bezpečné likvidace
NIST SP 800-53 Rev.5	AU-11, MP-6, SI-12	Uchovávání auditních záznamů, sanitizace médií, limity uchovávání údajů a jejich prosazování
EU NIS2	Článek 21(2)(a)	Vyžaduje politiku řízení životního cyklu přiměřenou riziku
EU DORA	Článek 5(1)	Řízení rizik v oblasti ICT: dostupnost a odstranění dat
COBIT 2019	BAI03.04, DSS01	Opatření pro životní cyklus informací, bezpečná likvidace
GDPR	Článek 5(1)(e), 17	Údaje nesmí být uchovávány déle, než je nezbytné; právo na výmaz

1. Účel

1.1 Účelem této politiky je stanovit závazná pravidla pro uchovávání a bezpečnou likvidaci informací v prostředí SME. Zajišťuje, aby byly záznamy uchovávány pouze po dobu vyžadovanou právními předpisy, smluvními povinnostmi nebo obchodní potřebou a následně bezpečně zlikvidovány.

1.2 Tato politika má za cíl snižovat informační rizika, řídit právní expozici a omezovat ukládání nadbytečných nebo zastaralých dat. Podporuje soulad s ISO/IEC 27001 a rámci ochrany soukromí, jako je GDPR, tím, že minimalizuje neoprávněné uchovávání osobních nebo citlivých informací.

1.3 Dobře strukturovaný rámec uchovávání a likvidace snižuje provozní náklady, zlepšuje výkonnost systémů a zvyšuje připravenost na audit. Pro SME s omezenou IT kapacitou představuje praktický způsob odpovědného řízení digitálních a fyzických informačních aktiv.

2. Rozsah

2.1 Tato politika se vztahuje na:

2.1.1 všechny záznamy, soubory, protokoly, komunikaci a datové soubory vytvořené, shromážděné, zpracovávané nebo uchovávané organizací,

2.1.2 všechny zaměstnance, smluvní pracovníky a externí poskytovatele, kteří nakládají s daty organizace,

2.1.3 všechny formáty dat (např. papírové, elektronické, obrazové, zvukové nebo protokolové) a všechna úložná média (např. lokální disky, cloudové služby, e-mailové servery, zálohy).

2.2 Rozsah zahrnuje:

2.2.1 obchodní dokumenty (např. faktury, smlouvy, projektové zprávy),

2.2.2 provozní záznamy (např. protokoly, historie přístupů, snímky záloh),

2.2.3 osobní údaje (např. personální spisy, komunikaci s klienty, záznamy podpory),

2.2.4 data hostovaná interně, externě nebo v hybridních systémech,

2.2.5 archivovaná a záložní data, ať již aktivní, nebo neaktivní.

2.3 Do rozsahu spadají všechny fáze životního cyklu dat od jejich vytvoření až po autorizovanou likvidaci.

3. Cíle

3.1 Stanovit konzistentní pravidla uchovávání na základě právních, provozních a regulatorních kritérií.

3.2 Zabránit předčasnému výmazu kritických záznamů a eliminovat zbytečné hromadění dat.

3.3 Zajistit bezpečnou a nevratnou likvidaci dat, jakmile jejich uchovávání již není vyžadováno.

3.4 Přiřadit odpovědnost za prosazování rozhodnutí o uchovávání a výmazu s ohledem na personální omezení typická pro SME.

3.5 Poskytovat dokumentaci připravenou pro audit za účelem doložení náležité péče podle ISO 27001, GDPR, NIS2 a dalších rámců.

3.6 Podporovat bezpečné nakládání s daty v průběhu jejich životního cyklu bez zbytečné technické zátěže pro nespecializovaný personál.

4. Role a odpovědnosti

4.1 generální ředitel (GM)

4.1.1 Schvaluje tuto politiku a odpovídá za její vlastnictví.

4.1.2 Zajišťuje, aby byly postupy uchovávání a likvidace zavedeny způsobem odpovídajícím právním a obchodním rizikům.

4.1.3 V případě potřeby schvaluje výjimky a pozastavení výmazu.

4.1.4 Zahajuje přezkumy politiky a schvaluje aktualizace na základě změn obchodních nebo regulatorních požadavků.

4.2 určený vlastník dat

4.2.1 Je určen pro každou kategorii dat (např. finanční, personální, klientské záznamy).

4.2.2 Klasifikuje záznamy a stanovuje odpovídající dobu uchovávání v souladu s touto politikou a právními požadavky.

4.2.3 Schvaluje výmaz po splnění požadavků na uchovávání.

4.2.4 Podporuje interní audity poskytováním kontextu k logice uchovávání a událostem likvidace.

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

9. Požadavky na přezkoumávání a aktualizaci

9.1 Tato politika musí být přezkoumána nejméně jednou ročně nebo při:

9.1.1 změnách příslušných právních předpisů (např. ochrana osobních údajů, finanční výkaznictví),

9.1.2 zavedení nových systémů nebo procesů ovlivňujících životní cyklus dat,

9.1.3 zjištěních auditu nebo incidentech odhalujících nedostatky v postupech uchovávání.

9.2 Přezkumy musí zajistit, aby registr uchovávání zůstal úplný a odrážel všechny hlavní kategorie záznamů.

9.3 Aktualizace politiky musí být schváleny GM a oznámeny dotčenému personálu. Nejnovější verze musí být přístupná a vedena v režimu správy verzí.

10. Související politiky a vazby

10.1 P2S – Politika rolí a odpovědností v oblasti správy a řízení: Vymezuje vlastnictví politiky a pravomoc ke schvalování výjimek.

10.2 P13S – Politika klasifikace a označování dat: Určuje, jak se pravidla uchovávání vztahují ke klasifikaci dat.

10.3 P12S – Politika správy aktiv: Upravuje úložná média obsahující data podléhající uchovávání / likvidaci.

10.4 P17S – Politika ochrany dat a soukromí: Zajišťuje minimalizaci dat a podporuje zákonné zpracování podle GDPR.

10.5 P30S – Politika reakce na incidenty: Aktivuje se v případě, že selhání likvidace nebo uchovávání vede k potenciální expozici dat.

11. Referenční normy a rámce

11.1 ISO/IEC 27001

11.1.1 Článek 6.1.3: Vyžaduje ošetření rizik souvisejících s informacemi, včetně rizik spojených s uchováváním.

11.1.2 Článek 8.1: Vymezuje provozní opatření v rámci životního cyklu.

11.2 ISO/IEC 27002

11.2.1 Opatření 5.33: Pokyny pro stanovení dob uchovávání a metod bezpečné likvidace.

11.3 NIST SP 800-53 Rev. 5

11.3.1 AU-11: Vyžaduje uchovávání auditních záznamů.

11.3.2 MP-6: Vymezuje postupy sanitizace médií.

11.3.3 SI-12: Řeší limity uchovávání údajů a jejich prosazování.

11.4 GDPR

11.4.1 Článek 5(1)(e): Údaje musí být uchovávány nejdéle po dobu nezbytnou.

11.4.2 Článek 17: Právo na výmaz se uplatní, pokud již data nejsou zákonně uchovávána.

11.5 EU NIS

11.5.1 Článek 21(2)(a): Vyžaduje organizační politiky přiměřené riziku, včetně řízení životního cyklu.

11.6 EU DORA

11.6.1 Článek 5(1): Řízení rizik v oblasti ICT zahrnuje dostupnost a odstranění dat.

11.7 COBIT 2019

11.7.1 BAI03.04: Vyžaduje opatření pro životní cyklus informací.

11.7.2 DSS01.06: Postupy bezpečné likvidace jako součást ochrany informačních aktiv.