					Sem vložte název registrované právnické osoby							
Číslo dokumentu: P14					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	Kapitola/článek	Komentář
ISO/IEC 27001:2022	Kapitoly 6.1.3, 8.1	
ISO/IEC 27002:2022	Opatření 5.10, 5.12, 5.30, 5	
NIST SP 800-53 Rev. 5	AU-11, MP-6, SI-12, PL-2	
GDPR	Články 5(1)(e), 17, 32	
směrnice NIS2	Článek 21(2)(a-e)	
nařízení DORA	Články 5, 9	
COBIT 2019	DSS01, DSS05, MEA	

1. Účel

1.1 Účelem této politiky je stanovit organizační požadavky na uchovávání údajů a jejich bezpečnou likvidaci ve všech fázích životního cyklu informací. Tato politika zajišťuje soulad s příslušnými právními, regulačními a smluvními povinnostmi a předchází zbytečnému nebo rizikovému hromadění údajů.

1.2 Tato politika podporuje implementaci ISO/IEC 27001:2022 zavedením kontrol doby uchovávání údajů a postupů jejich nevratné likvidace. Umožňuje dohledatelné vedení záznamů, prosazuje uchovávání v souladu s úrovní citlivosti a klasifikací a zajišťuje připravenost na audit, regulatorní kontrolu a právní dokazování.

1.3 Dále si klade za cíl zachovávat důvěrnost, integritu a dostupnost údajů a současně minimalizovat obchodní rizika, provozní neefektivitu a expozici vůči porušení ochrany soukromí vyplývající z nesprávného uchovávání nebo likvidace údajů.

2. Rozsah

2.1 Tato politika se vztahuje na všechna fyzická i digitální informační aktiva vlastněná organizací, zpracovávaná organizací nebo organizací uchovávaná, včetně těch, která jsou pod kontrolou třetích stran, dceřiných společností nebo outsourcingových partnerů.

2.2 Rozsah zahrnuje mimo jiné:

2.2.1 dokumenty, soubory a záznamy (digitální i listinné),

2.2.2 databáze a archivy,

2.2.3 e-maily a záznamy instant messagingu,

2.2.4 zálohy, systémové protokoly a auditní stopy,

2.2.5 zdrojový kód, aplikační data a aktiva hostovaná v cloudu,

2.2.6 vyměnitelná média a vyřazený hardware obsahující data.

2.3 Tato politika upravuje jak provozní záznamy, tak regulované soubory dat (např. finanční, právní, HR, zákaznický obsah a obsah relevantní pro audit), bez ohledu na místo uložení nebo systém.

2.4 Vztahuje se na všechny organizační útvary a na všechny zaměstnance, smluvní pracovníky a dodavatele zapojené do vytváření, ukládání, správy nebo likvidace dat.

3. Cíle

3.1 Zajistit, aby byla data uchovávána pouze po dobu právně, smluvně nebo provozně nezbytnou a aby byla bezpečně zlikvidována, jakmile již nejsou potřebná.

3.2 Předcházet předčasnému, neoprávněnému nebo náhodnému mazání záznamů potřebných pro probíhající provoz, soulad, soudní řízení nebo účely auditu.

3.3 Zavést a uplatňovat jednotné skartační a retenční lhůty na základě klasifikace informací, typu aktiv, příslušných právních předpisů a rizikové expozice.

3.4 Chránit soukromí a důvěrnost dat během doby jejich uchovávání i při jejich likvidaci, včetně plnění práv subjektů údajů (např. výmaz podle článku 17 GDPR).

3.5 Zajistit, aby všechny metody likvidace dat byly nevratné, řádně zdokumentované a v souladu s uznávanými normami, jako je NIST SP 800-88.

3.6 Minimalizovat provozní neefektivitu, nákladovou zátěž a právní expozici způsobenou nadměrně dlouhým uchováváním nebo nesledovanými historickými daty.

3.7 Podporovat cíle kontinuity činností a obnovy po havárii prostřednictvím integrované správy retenčních lhůt záloh a obhajitelných postupů archivace dat.

4. Role a odpovědnosti

4.1 Vrcholové vedení

4.1.1 Schvaluje tuto politiku a zajišťuje odpovídající financování, personální kapacity a začlenění do řízení podnikových rizik a programů zajištění souladu.

4.1.2 Nese celkovou odpovědnost za soulad s právními a regulačními požadavky souvisejícími s uchováváním dat a jejich bezpečnou likvidací.

4.2 Ředitel informační bezpečnosti (CISO)

4.2.1 Je vlastníkem této politiky a odpovídá za vymezení a přezkum správy uchovávání a likvidace v souladu se systémem řízení bezpečnosti informací (ISMS).

4.2.2 Zajišťuje, aby byly požadavky na uchovávání a likvidaci odvozené od klasifikace implementovány v rámci organizačních útvarů a technických systémů.

4.2.3 Monitoruje dodržování politiky a v případě potřeby prosazuje nápravná opatření.

[... 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 přezkoumávána každoročně nebo při splnění kterékoli z následujících podmínek:

9.1.1 změny příslušných právních předpisů nebo regulačních požadavků ovlivňujících uchovávání dat (např. aktualizace GDPR, daňových předpisů nebo DORA),

9.1.2 změny rámce klasifikace nebo podnikových procesů ovlivňující fáze životního cyklu dat,

9.1.3 zavedení nových IT systémů, archivačních platforem nebo technologií likvidace médií,

9.1.4 zjištění interního auditu nebo doporučení regulačních orgánů poukazující na nedostatky v postupech uchovávání nebo likvidace.

9.2 Přezkum musí být veden CISO a pověřencem pro ochranu osobních údajů (DPO) za účasti právního oddělení, compliance, IT a organizačních útvarů.

9.3 MDRS a registr likvidace musí být přezkoumávány souběžně, aby bylo zajištěno:

9.3.1 že lhůty zůstávají přesné a odrážejí provozní, právní a regulační potřeby,

9.3.2 že dokumentace likvidace je úplná a auditovatelná,

9.3.3 že záznamy legal hold jsou validovány a uvolňovány, je-li to vhodné.

9.4 Jakékoli aktualizace této politiky musí:

9.4.1 být formálně verzovány a uchovávány v repozitáři dokumentace ISMS,

9.4.2 zahrnovat historii verzí a odůvodnění změny,

9.4.3 být schváleny vrcholovým vedením,

9.4.4 být oznámeny relevantnímu personálu spolu s aktualizovanými školicími nebo metodickými materiály.

9.5 Pokud dojde k významným změnám politiky, musí dotčení zaměstnanci absolvovat cílené školení do 30 dnů od vydání, aby byl zajištěn trvalý soulad.

9.6 Související politiky a vazby

10. Související politiky a vazby

10.1.1 P4 - Politika řízení přístupu: Zajišťuje, že k datům během doby jejich uchovávání přistupují pouze oprávněné osoby a že data po uplynutí retenční lhůty jsou až do likvidace odpovídajícím způsobem omezena.

10.1.2 P12 - Politika správy aktiv: Určuje, která aktiva obsahují data vyžadující plánovanou likvidaci, a sleduje jejich životní cyklus od pořízení po zničení.

10.1.3 P13 - Politika klasifikace dat a označování: Určuje klasifikační rozhodnutí, která přímo ovlivňují dobu uchovávání dat a požadovanou metodu likvidace.

10.1.4 P15 - Politika zálohování a obnovy: Definuje retenční lhůty a postupy likvidace pro záložní média a replikovaná datová aktiva.

10.1.5 P18 - Politika kryptografických opatření: Podporuje kryptografické vymazání při likvidaci a prosazuje šifrování během ukládání dat až do jejich zničení.

10.1.6 P30 - Politika reakce na incidenty: Aktivuje se v případech, kdy nesprávná likvidace vede k potenciální ztrátě dat, porušení zabezpečení dat nebo regulatornímu porušení.

10.2 Každá navázaná politika plní úlohu při prosazování uceleného modelu správy dat napříč klasifikací, řízením životního cyklu, přístupem a připraveností na audit.

11. Referenční normy a rámce

11.1 Tato politika je v souladu s celosvětově uznávanými normami a regulačními rámci, které vymezují bezpečné, souladné a účinné postupy pro životní cyklus dat.

11.2 ISO/IEC 27001:

11.2.1 Kapitola 6.1.3 - Plán ošetření rizik: Podporuje zmírňování rizik spojených s nadměrně dlouhým uchováváním, porušením zabezpečení dat nebo selháním likvidace.

11.2.2 Kapitola 8.1 - Provozní plánování a řízení: Zavádí kontroly životního cyklu, které upravují ukládání, archivaci a ničení.

11.3 ISO/IEC 27002:2022 - Opatření 5.10, 5.12, 5.30, 5: Poskytují praktické pokyny k přípustnému využívání dat, odůvodnění uchovávání, řízenému mazání a obhajitelnému vedení záznamů v souladu s tolerancí rizika organizace.

11.4 NIST SP 800-53 Rev. 5:

11.4.1 AU-11 - Uchovávání auditních záznamů: Zajišťuje dostatečné uchovávání auditních protokolů a důkazů o souladu.

11.4.2 MP-6 - Sanitizace médií: Vyžaduje bezpečné a zdokumentované metody ničení fyzických a elektronických médií.

11.4.3 SI-12 - Nakládání s informacemi: Prosazuje vhodné nakládání s daty v souladu s kontrolami uchovávání a likvidace.

11.4.4 PL-2 - Plán bezpečnosti systému a ochrany soukromí: Vyžaduje systémově specifickou dokumentaci nakládání s životním cyklem dat a opatření pro bezpečnou likvidaci.

11.5 GDPR (2016/679):

11.5.1 Článek 5 odst. 1 písm. e) - Minimalizace údajů a omezení uložení: Vyžaduje, aby data nebyla uchovávána déle, než je nezbytné.

11.5.2 Článek 17 - Právo na výmaz („právo být zapomenut“): Vyžaduje bezodkladné a trvalé vymazání osobních údajů na základě oprávněné žádosti.

11.5.3 Článek 32 - Zabezpečení zpracování: Posiluje ochranu dat během uchovávání a vyžaduje bezpečné zničení záznamů po uplynutí jejich retenční lhůty.

11.6 Směrnice NIS2 (2022/2555):

11.6.1 Článek 21(2)(a-e): Vyžaduje, aby subjekty přijaly politiky a technická opatření pro bezpečné nakládání s daty, včetně omezení doby uložení a metod likvidace.

11.7 Nařízení DORA (2022/2554):

11.7.1 Článek 5 - Správa a řízení a kontrola: Ukládá strukturované řízení rizik v oblasti ICT, včetně bezpečného řízení životního cyklu informací.

11.7.2 Článek 9 - Rámec řízení rizik v oblasti ICT: Vyžaduje politiky pro uchovávání dat, jejich ničení a soulad digitálních operací s právními a regulačními požadavky.

11.8 COBIT 2019:

11.8.1 DSS01 - Řízený provoz: Podporuje sledování uchovávání a konzistentnost napříč datovými systémy.

11.8.2 DSS05 - Řízené bezpečnostní služby: Zajišťuje ochranu uložených a archivovaných dat až do jejich bezpečné likvidace.

11.8.3 MEA03 - Monitorování, hodnocení a posuzování souladu: Umožňuje audit uplatňování retenčních lhůt, postupů mazání a plnění regulačních požadavků.