					Sem zadajte názov registrovanej právnickej osoby							
Číslo dokumentu: P14					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**

V súlade s normami a predpismi

Norma/predpis	Kapitola/článok	Poznámka
ISO/IEC 27001:2022	Kapitoly 6.1.3, 8.1	
ISO/IEC 27002:2022	Kontroly 5.10, 5.12, 5.30, 5	
NIST SP 800-53 Rev. 5	AU-11, MP-6, SI-12, PL-2	
Nariadenie EÚ GDPR	Články 5(1)(e), 17, 32	
Smernica EÚ NIS2	Článok 21(2)(a-e)	
Nariadenie EÚ DORA	Články 5, 9	
COBIT 2019	DSS01, DSS05, MEA	

1. Účel

1.1 Účelom tejto politiky je stanoviť organizačné požiadavky na uchovávanie údajov a ich bezpečnú likvidáciu vo všetkých fázach životného cyklu informácií. Politika zabezpečuje súlad s platnými právnymi, regulačnými a zmluvnými požiadavkami a predchádza zbytočnému alebo rizikovému hromadeniu údajov.

1.2 Táto politika podporuje implementáciu normy ISO/IEC 27001:2022 tým, že zavádza kontrolu nad dobou uchovávania údajov a postupmi ich nezvratnej likvidácie. Umožňuje sledovateľnú evidenciu záznamov, uplatňuje uchovávanie primerané citlivosti a klasifikácii údajov a zabezpečuje pripravenosť na audit, regulačnú kontrolu a právne zisťovanie.

1.3 Ďalším cieľom tejto politiky je zachovať dôvernosť, integritu a dostupnosť údajov a zároveň minimalizovať riziko pre organizáciu, prevádzkové neefektívnosti a vystavenie incidentom ochrany súkromia vyplývajúcim z nesprávneho uchovávania alebo likvidácie údajov.

2. Rozsah

2.1 Táto politika sa vzťahuje na všetky fyzické a digitálne informačné aktíva, ktoré organizácia vlastní, spracúva alebo uchováva, vrátane aktív spravovaných tretími stranami, dcérskymi spoločnosťami alebo outsourcingovými partnermi.

2.2 Rozsah zahŕňa okrem iného:

2.2.1 dokumenty, súbory a záznamy (digitálne aj v listinnej podobe),

2.2.2 databázy a archívy,

2.2.3 e-maily a záznamy okamžitej komunikácie,

2.2.4 zálohy, systémové logy a auditné stopy,

2.2.5 zdrojový kód, aplikačné údaje a aktíva hostované v cloude,

2.2.6 vymeniteľné médiá a vyradený hardvér obsahujúci údaje.

2.3 Politika upravuje prevádzkové záznamy aj regulované súbory údajov (napr. finančné, právne, HR, zákaznícke údaje a obsah relevantný pre audit) bez ohľadu na umiestnenie úložiska alebo systému.

2.4 Vzťahuje sa na všetky organizačné útvary, zamestnancov, zmluvných pracovníkov a dodávateľov zapojených do vytvárania, uchovávania, správy alebo likvidácie údajov.

3. Ciele

3.1 Zabezpečiť, aby sa údaje uchovávali iba po dobu, počas ktorej je to nevyhnutné z právneho, zmluvného alebo prevádzkového hľadiska, a aby boli po zániku tejto potreby bezpečne zlikvidované.

3.2 Predchádzať predčasnému, neoprávnenému alebo náhodnému výmazu záznamov potrebných na bežnú prevádzku, účely súladu, súdne spory alebo audit.

3.3 Zaviesť a uplatňovať konzistentné lehoty uchovávania založené na klasifikácii informácií, type aktíva, platných právnych predpisoch a úrovni rizika.

3.4 Chrániť súkromie a dôvernosť údajov počas celej doby uchovávania aj pri ich likvidácii vrátane plnenia práv dotknutých osôb (napr. výmaz podľa článku 17 GDPR).

3.5 Zabezpečiť, aby všetky metódy likvidácie údajov boli nezvratné, primerane zdokumentované a v súlade s uznávanými normami, ako je NIST SP 800-88.

3.6 Minimalizovať prevádzkové neefektívnosti, nákladové zaťaženie a právne riziká spôsobené nadmerným uchovávaním alebo nesledovanými historickými údajmi.

3.7 Podporovať ciele kontinuity činností a obnovy po havárii prostredníctvom integrovanej správy uchovávania záloh a obhájiteľných postupov archivácie údajov.

4. Roly a zodpovednosti

4.1 Vrcholový manažment

4.1.1 Schvaľuje túto politiku a zabezpečuje primerané financovanie, personálne kapacity a jej integráciu do programov podnikového riadenia rizík a súladu.

4.1.2 Nesie celkovú zodpovednosť za dodržiavanie právnych a regulačných požiadaviek týkajúcich sa uchovávania údajov a ich bezpečnej likvidácie.

4.2 Riaditeľ informačnej bezpečnosti (CISO)

4.2.1 Je vlastníkom tejto politiky a zodpovedá za definovanie a preskúmavanie riadenia uchovávania a likvidácie údajov v súlade s ISMS.

4.2.2 Zabezpečuje implementáciu požiadaviek na uchovávanie a likvidáciu vychádzajúcich z klasifikácie v organizačných útvaroch a technických systémoch.

4.2.3 Monitoruje dodržiavanie tejto politiky a podľa potreby prijíma nápravné opatrenia.

[... 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 sa musí preskúmať najmenej raz ročne alebo vždy, keď nastane niektorá z týchto podmienok:

9.1.1 zmeny platných právnych predpisov alebo regulácií ovplyvňujúcich uchovávanie údajov (napr. aktualizácie GDPR, daňových predpisov, DORA),

9.1.2 revízie klasifikačného rámca alebo procesov organizácie ovplyvňujúce fázy životného cyklu údajov,

9.1.3 zavedenie nových IT systémov, archivačných platforiem alebo technológií likvidácie médií,

9.1.4 auditné zistenia vnútorného auditu alebo odporúčania regulátora upozorňujúce na nedostatky v postupoch uchovávania alebo likvidácie.

9.2 Preskúmanie vedie CISO a zodpovedná osoba za ochranu osobných údajov (DPO) za účasti právneho oddelenia, funkcie compliance, IT a príslušných organizačných útvarov.

9.3 Hlavný harmonogram uchovávania údajov (MDRS) a register likvidácie sa musia preskúmavať súbežne s cieľom zabezpečiť, aby:

9.3.1 harmonogramy zostali presné a odrážali prevádzkové, právne a regulačné potreby,

9.3.2 dokumentácia likvidácie bola úplná a overiteľná,

9.3.3 záznamy o právnom uchovaní boli validované a uvoľnené v primeranom čase.

9.4 Každá aktualizácia politiky musí:

9.4.1 podliehať formálnemu riadeniu verzií a byť uchovávaná v úložisku dokumentov ISMS,

9.4.2 obsahovať históriu revízií a odôvodnenie zmeny,

9.4.3 byť schválená vrcholovým manažmentom,

9.4.4 byť oznámená príslušným pracovníkom spolu s aktualizovanými školiacimi alebo metodickými materiálmi.

9.5 Ak dôjde k významným zmenám politiky, dotknutí zamestnanci musia absolvovať cielené školenie do 30 dní od jej vydania, aby sa zabezpečil trvalý súlad.

9.6 Súvisiace politiky a väzby

10. Súvisiace politiky a väzby

10.1.1 P4 - Politika riadenia prístupu: Zabezpečuje, aby k údajom počas doby ich uchovávania pristupovali iba oprávnené osoby a aby bol po uplynutí lehoty prístup k údajom obmedzený až do ich likvidácie.

10.1.2 P12 - Politika správy aktív: Identifikuje aktíva obsahujúce údaje vyžadujúce plánovanú likvidáciu a sleduje ich životný cyklus od obstarania po zničenie.

10.1.3 P13 - Politika klasifikácie a označovania údajov: Usmerňuje rozhodnutia o klasifikácii, ktoré priamo ovplyvňujú dobu uchovávania údajov a požadovanú metódu likvidácie.

10.1.4 P15 - Politika zálohovania a obnovy: Definuje lehoty uchovávania a postupy likvidácie pre zálohovacie médiá a replikované dátové aktíva.

10.1.5 P18 - Politika kryptografických kontrol: Podporuje kryptografický výmaz pri likvidácii a uplatňuje šifrovanie počas uchovávania údajov až do ich zničenia.

10.1.6 P30 - Politika reakcie na incidenty: Aktivuje sa v prípadoch, keď nesprávna likvidácia vedie k potenciálnej strate údajov, porušeniu ochrany údajov alebo porušeniu regulačných požiadaviek.

10.2 Každá prepojená politika zohráva úlohu pri uplatňovaní konzistentného modelu riadenia údajov naprieč klasifikáciou, riadením životného cyklu, prístupom a pripravenosťou na audit.

11. Referenčné normy a rámce

11.1 Táto politika je v súlade s globálne uznávanými normami a regulačnými rámcami, ktoré definujú bezpečné, súladné a efektívne postupy riadenia životného cyklu údajov.

11.2 ISO/IEC 27001:

11.2.1 Kapitola 6.1.3 - plán ošetrenia rizík: Podporuje zmierňovanie rizík súvisiacich s nadmerným uchovávaním, porušeniami ochrany údajov alebo zlyhaniami likvidácie.

11.2.2 Kapitola 8.1 - prevádzkové plánovanie a riadenie: Zavádza kontroly životného cyklu upravujúce uchovávanie, archiváciu a zničenie.

11.3 ISO/IEC 27002:2022 - Kontroly 5.10, 5.12, 5.30, 5: Poskytujú praktické usmernenia k prípustnému používaniu údajov, odôvodneniu uchovávania, riadenému výmazu a obhájiteľnému vedeniu záznamov v súlade s toleranciou rizika organizácie.

11.4 NIST SP 800-53 Rev. 5:

11.4.1 AU-11 - uchovávanie auditných záznamov: Zabezpečuje dostatočné uchovávanie auditných logov a dôkazov o súlade.

11.4.2 MP-6 - sanitizácia médií: Vyžaduje bezpečné a zdokumentované metódy ničenia fyzických a elektronických médií.

11.4.3 SI-12 - nakladanie s informáciami: Uplatňuje primerané zaobchádzanie s údajmi v súlade s kontrolami uchovávania a likvidácie.

11.4.4 PL-2 - plán bezpečnosti systému a ochrany súkromia: Vyžaduje dokumentáciu nakladania s údajmi počas ich životného cyklu špecifickú pre systém a ustanovenia o bezpečnej likvidácii.

11.5 Nariadenie EÚ GDPR (2016/679):

11.5.1 Článok 5(1)(e) - minimalizácia údajov a obmedzenie uchovávania: Vyžaduje, aby sa údaje neuchovávali dlhšie, než je nevyhnutné.

11.5.2 Článok 17 - právo na výmaz („právo byť zabudnutý“): Vyžaduje bezodkladné a trvalé vymazanie osobných údajov na základe oprávnenej žiadosti.

11.5.3 Článok 32 - bezpečnosť spracúvania: Posilňuje ochranu údajov počas ich uchovávania a vyžaduje bezpečné zničenie záznamov po uplynutí lehoty.

11.6 Smernica EÚ NIS2 (2022/2555):

11.6.1 Článok 21(2)(a-e): Vyžaduje, aby subjekty prijali politiky a technické opatrenia na bezpečné nakladanie s údajmi vrátane obmedzenia uchovávania a metód likvidácie.

11.7 Nariadenie EÚ DORA (2022/2554):

11.7.1 Článok 5 - riadenie a kontrola: Ukladá štruktúrované riadenie rizík IKT vrátane bezpečného nakladania s informáciami počas ich životného cyklu.

11.7.2 Článok 9 - rámec riadenia rizík IKT: Vyžaduje politiky pre uchovávanie údajov, ich zničenie a zákonný/regulačný súlad digitálnych operácií.

11.8 COBIT 2019:

11.8.1 DSS01 - riadené operácie: Podporuje sledovanie uchovávania a konzistentnosť naprieč dátovými systémami.

11.8.2 DSS05 - riadené bezpečnostné služby: Zabezpečuje ochranu uložených a archivovaných údajov až do ich bezpečnej likvidácie.

11.8.3 MEA03 - Monitorovanie, hodnotenie a posudzovanie súladu: Umožňuje audit uplatňovania uchovávania, postupov výmazu a plnenia regulačných požiadaviek.