					Sem zadajte názov registrovanej právnickej osoby							
Číslo dokumentu: P27					Názov dokumentu: **Politika používania cloudových služieb**							
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	Kapitola 8	Požiadavky na prevádzkové plánovanie a riadenie v cloudovom prostredí.
ISO/IEC 27002:2022	Kontroly 5.23 – 5.25	Požiadavky na používanie cloudových služieb, politiku ich používania a ich bezpečnosť.
NIST SP 800-53 Rev. 5	AC-20, SA-9(5), SC-12 – SC-28, SR-5	Používanie externých systémov, zmluvné a technické požiadavky, kryptografické ochranné opatrenia a ochrana dodávateľského reťazca.
GDPR EÚ	Články 28, 32, kapitola V	Požiadavky na cloudových sprostredkovateľov, bezpečnosť spracúvania a prenosy údajov.
NIS2 EÚ	Článok 21(2)(f, i)	Požiadavky na riadenie rizík tretích strán a dodávateľského reťazca.
DORA EÚ	Články 5(2), 28	Dohľad nad IKT a tretími stranami (cloud) pre finančné subjekty.
COBIT 2019	BAI04, DSS01, DSS05	Dostupnosť cloudových služieb, prevádzka a riadenie bezpečnosti.

1. Účel

1.1 Táto politika stanovuje záväzné požiadavky organizácie na bezpečné, súladné a zodpovedné používanie cloudových služieb v modeloch Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) a Software-as-a-Service (SaaS).

1.2 Cieľom tejto politiky je zabezpečiť, aby sa cloudové služby zavádzali a spravovali spôsobom, ktorý chráni dôvernosť, integritu a dostupnosť informačných aktív a zároveň spĺňa regulačné, zákonné a zmluvné povinnosti.

1.3 Politika definuje kontroly na riadenie cloudových rizík, ochranu údajov, monitorovanie súladu poskytovateľov a prevenciu neoprávneného používania. Zároveň podporuje inovácie organizácie prostredníctvom cloudových platforiem zosúladením bezpečnosti, prevádzkovej spoľahlivosti a nákladovej efektívnosti.

2. Rozsah

2.1 Táto politika sa vzťahuje na všetkých zamestnancov, zmluvných pracovníkov, externých poskytovateľov služieb a konzultantov, ktorí v mene organizácie zriaďujú, konfigurujú, pristupujú, spravujú alebo používajú cloudové služby.

2.2 Vzťahuje sa na všetky prostredia, v ktorých sa spracúvajú údaje alebo pracovné záťaže organizácie, vrátane:

2.2.1 verejných, súkromných, hybridných a komunitných cloudových nasadení,

2.2.2 všetkých modelov cloudových služieb (IaaS, PaaS, SaaS),

2.2.3 multicloudových a federovaných architektúr,

2.2.4 používania shadow IT alebo osobných cloudových účtov na pracovné účely.

2.3 Zahŕňa všetky úrovne klasifikácie údajov a vzťahuje sa na interné systémy, ako aj na platformy hostované dodávateľmi, v ktorých sú uložené alebo spracúvané údaje vo vlastníctve organizácie alebo regulované údaje.

3. Ciele

3.1 Zabezpečiť bezpečné a konzistentné používanie cloudových technológií prostredníctvom jasne definovaných pravidiel používania, referenčných bezpečnostných nastavení a rolí v oblasti správy a riadenia.

3.2 Minimalizovať prevádzkové a regulačné riziká spojené s cloudovými službami vrátane neoprávneného prístupu, porušenia ochrany údajov, chybných konfigurácií, nesúladu a prerušenia služieb.

3.3 Uplatňovať požiadavky na bezpečnosť a ochranu súkromia voči všetkým cloudovým poskytovateľom a overovať súlad prostredníctvom zmluvných ustanovení, posúdení a práv na audit.

3.4 Umožniť škálovateľné a odolné zavádzanie cloudových služieb bez oslabenia úrovne bezpečnosti, zákonných požiadaviek alebo kontinuity činností.

3.5 Zosúladiť správu a riadenie cloudových služieb a ich používanie s rámcom ISMS organizácie, zákonnými povinnosťami (napr. GDPR, DORA), odvetvovými usmerneniami a všeobecne uznávanými osvedčenými postupmi (napr. NIST, COBIT).

4. Roly a zodpovednosti

4.1 Vrcholový manažment

4.1.1 Schvaľuje Politiku používania cloudových služieb a strategický plán zavádzania cloudových služieb.

4.1.2 Preskúmava a schvaľuje výnimky s vysokým rizikom zo štandardných požiadaviek na správu a riadenie cloudových služieb.

4.1.3 Zabezpečuje, aby cloudové iniciatívy mali primerané financovanie, dohľad a integráciu s rámcami podnikového riadenia rizík.

4.2 Riaditeľ informačnej bezpečnosti (CISO)

4.2.1 Je vlastníkom tejto politiky a centrálneho registra cloudových služieb organizácie.

4.2.2 Schvaľuje zavedenie nových cloudových poskytovateľov na základe due diligence a vyhodnotenia rizík.

4.2.3 Preskúmava dokumentáciu súladu poskytovateľov a overuje súlad s bezpečnostnými požiadavkami.

[... 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 preskúmavať najmenej raz ročne a podľa potreby aktualizovať tak, aby zostala v súlade s:

9.1.1 vyvíjajúcimi sa zákonnými a regulačnými požiadavkami (napr. GDPR, NIS2, DORA),

9.1.2 zmenami v normách ISO/IEC 27001 alebo ISO/IEC 27002,

9.1.3 aktualizáciami cloudovej architektúry organizácie, prostredia hrozieb alebo portfólia služieb,

9.1.4 vyšetrovaniami incidentov, výsledkami auditov alebo poznatkami z prevádzky.

9.2 CISO je zodpovedný za iniciovanie preskúmania a zvolanie relevantných zainteresovaných strán vrátane:

9.2.1 cloudového bezpečnostného architekta,

9.2.2 tímu pre právne záležitosti a súlad,

9.2.3 obstarávania a manažérov dodávateľov,

9.2.4 vlastníkov služieb a IT prevádzky.

9.3 Všetky aktualizácie musia byť:

9.3.1 riadené verziami a datované,

9.3.2 schválené vrcholovým manažmentom,

9.3.3 oznámené dotknutým stranám vrátane zamestnancov, zmluvných pracovníkov a tretích strán,

9.3.4 archivované v súlade s internými politikami dokumentácie.

9.4 Mimoriadne preskúmania môžu byť vyvolané:

9.4.1 novými zmluvnými vzťahmi s CSP alebo významnými migráciami,

9.4.2 novými hrozbami pre cloudovú infraštruktúru,

9.4.3 podstatnými zmenami zmluvných, zákonných alebo odvetvových povinností.

10. Súvisiace politiky a väzby

10.1 Táto politika úzko súvisí s nasledujúcimi internými politikami a je od nich závislá:

10.1.1 P1 – Politika informačnej bezpečnosti: stanovuje nadradené princípy riadiace bezpečnú prevádzku systémov a služieb, ktoré táto politika uplatňuje v cloudovom kontexte.

10.1.2 P5 – Politika riadenia zmien: všetky zmeny cloudových konfigurácií sa musia riadiť postupmi riadenia zmien definovanými v P5.

10.1.3 P13 – Politika klasifikácie a označovania údajov: určuje, ako sa údaje posudzujú pred prenosom do cloudu a ako sa uplatňujú kontroly, ako sú šifrovanie a lokalizácia údajov.

10.1.4 P18 – Politika kryptografických kontrol: poskytuje štandardy pre šifrovanie, správu kľúčov a používanie kryptografických algoritmov, ktoré sa priamo uplatňujú pri konfiguráciách cloudových služieb.

10.1.5 P22 – Politika logovania a monitorovania: špecifikuje požiadavky na zber, uchovávanie a analýzu logov, ktoré sa musia uplatňovať v cloudových prostrediach.

10.1.6 P30 – Politika reakcie na incidenty: definuje eskaláciu, zamedzenie šírenia a nápravné postupy pre bezpečnostné udalosti súvisiace s cloudom.

10.1.7 P33 – Politika monitorovania auditu a súladu: podporuje pripravenosť na audit a priebežné uisťovanie, že cloudové kontroly sú uplatňované a monitorované.

11. Referenčné normy a rámce

11.1 ISO/IEC 27001: Kapitola 8.1 – Prevádzkové plánovanie a riadenie: vyžaduje, aby organizácie zaviedli a riadili procesy potrebné na splnenie požiadaviek informačnej bezpečnosti vrátane tých, ktoré sa týkajú cloudových prostredí.

11.2 ISO/IEC 27002:2022 – Kontroly 5.23 až 5.25:

11.2.1 Príloha A, kontrola 5.23 – Používanie cloudových služieb: vyžaduje posúdenie založené na riziku, formálne schválenie a dokumentovanie používania cloudových služieb.

11.2.2 Príloha A, kontrola 5.24 – Politika používania cloudových služieb: vyžaduje vytvorenie a uplatňovanie formálnych pravidiel používania cloudových služieb zosúladených s potrebami a rizikami organizácie.

11.2.3 Príloha A, kontrola 5.25 – Bezpečnosť cloudových služieb: vyžaduje integráciu bezpečnosti, zmluvné ochranné opatrenia a monitorovanie pracovných záťaží a údajov prevádzkovaných v cloudovom prostredí.

11.3 NIST SP 800-53 Rev. 5:

11.3.1 AC-20 – Používanie externých systémov: vyžaduje definované pravidlá a podmienky prístupu k zdrojom organizácie z externých systémov alebo systémov v cloudovom prostredí.

11.3.2 SA-9(5) – Externé služby informačných systémov: vyžaduje zmluvné bezpečnostné požiadavky, dohľad a priebežné monitorovanie systémov tretích strán v cloudovom prostredí.

11.3.3 SC-12 až SC-28 – Kryptografické ochranné opatrenia, ochrana hraníc a integrita prenosu: zodpovedajú požiadavkám na šifrovanie, identitu a prístup pri službách prevádzkovaných v cloudovom prostredí a pri údajoch pri prenose.

11.3.4 SR-5 – Ochrana dodávateľského reťazca: podporuje preverovanie a zmluvnú kontrolu nad CSP zapojenými do poskytovania služieb.

11.4 GDPR EÚ (2016/679):

11.4.1 Článok 28 – Povinnosti sprostredkovateľa: vyžaduje formálne zmluvy s cloudovými poskytovateľmi na zabezpečenie bezpečnosti, dôvernosti a auditovateľnosti spracúvania osobných údajov.

11.4.2 Článok 32 – Bezpečnosť spracúvania: podporuje uplatnenie šifrovania, riadenia prístupu, logovania a ďalších ochranných opatrení v cloudových prostrediach.

11.4.3 Kapitola V – Medzinárodné prenosy údajov: vyžaduje zákonný prenos údajov mimo EÚ/EHP s použitím ochranných opatrení, ako sú štandardné zmluvné doložky (SCC) alebo rozhodnutia o primeranosti.

11.5 Smernica EÚ NIS2 (2022/2555):

11.5.1 Článok 21(2)(f, i): vyžaduje, aby subjekty riadili riziká vyplývajúce z cloudových poskytovateľov tretích strán a zabezpečovali integritu digitálneho dodávateľského reťazca prostredníctvom zmluvných a technických opatrení.

11.6 Nariadenie EÚ DORA (2022/2554):

11.6.1 Článok 5(2) – Správa a riadenie rizík IKT: vyžaduje integráciu rizík IKT tretích strán vrátane cloudových služieb do celkového rámca riadenia rizík.

11.6.2 Článok 28 – Dohľad nad kritickými externými poskytovateľmi služieb IKT: vyžaduje, aby finančné subjekty monitorovali, riadili a oznamovali závislosti od cloudových poskytovateľov, ich bezpečnostný stav a odolnosť.

11.7 COBIT 2019:

11.7.1 BAI04 – Riadenie dostupnosti a kapacity: zabezpečuje, aby cloudové služby boli odolné, monitorované a spĺňali definované výkonnostné kritériá.

11.7.2 DSS01 – Riadenie prevádzky: podporuje prevádzkovú integráciu, riešenie incidentov a referenčné konfigurácie naprieč platformami prevádzkovanými v cloudovom prostredí.

11.7.3 DSS05 – Riadenie bezpečnostných služieb: usmerňuje implementáciu cloudovo špecifických bezpečnostných kontrol, monitorovania a prevencie incidentov v digitálnych službách.