					Sem zadajte názov registrovanej právnickej osoby							
Číslo dokumentu: P27S					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	
ISO/IEC 27002:2022	Kontroly 5.23–5.25	
NIST SP 800-53 Rev.5	AC-20, SC-12, SC-13, SR-5	
Nariadenie EÚ GDPR	Článok 28, 32 a kapitola V	
Smernica EÚ NIS2	Článok 21(2)(f), (i)	
Nariadenie EÚ DORA	Článok 5(2), 28	
COBIT 2019	DSS01, DSS05, BAI	

1. Účel

1.1 Táto politika stanovuje podmienky bezpečného používania cloudových služieb v organizácii. Zabezpečuje, aby údaje spracúvané alebo ukladané v cloude boli chránené, aby bol prístup riadený a aby sa riziká riadili primeraným a zodpovedným spôsobom.

1.2 Pomáha MSP plniť zákonné povinnosti a očakávania zákazníkov pri ochrane citlivých informácií, predchádzaní únikom údajov a účinnom riadení rizík v cloudovom prostredí bez potreby infraštruktúry podnikovej úrovne.

1.3 Táto politika podporuje certifikáciu podľa ISO/IEC 27001, súlad s GDPR a zabezpečenie dodávateľského reťazca prostredníctvom konzistentného riadenia všetkých cloudových služieb tretích strán.

2. Rozsah

2.1 Táto politika sa vzťahuje na:

2.1.1 všetky cloudové služby používané na ukladanie, spracúvanie alebo prenos údajov spoločnosti,

2.1.2 všetkých zamestnancov, zmluvných pracovníkov a poskytovateľov služieb, ktorí používajú cloudové nástroje v mene organizácie,

2.1.3 bezplatné aj platené cloudové riešenia vrátane platforiem elektronickej pošty, zdieľania dokumentov, SaaS nástrojov, zálohovacích platforiem, videokonferenčných riešení a zákazníckych platforiem,

2.1.4 akékoľvek zariadenie (stolový počítač, mobilné zariadenie, tablet), ktoré pristupuje k informáciám spoločnosti prostredníctvom cloudových aplikácií.

2.2 To zahŕňa najmä:

2.2.1 Microsoft 365, Google Workspace, Dropbox Business,

2.2.2 Zoom, Microsoft Teams, Google Meet,

2.2.3 AWS, Azure, GCP,

2.2.4 cloudové nástroje na zálohovanie a obnovu po havárii,

2.2.5 zdieľané priečinky alebo aplikácie používané na fakturáciu, riadenie projektov alebo komunikáciu so zákazníkmi.

3. Ciele

3.1 Predchádzať neoprávnenému alebo vysoko rizikovému používaniu neschválených cloudových služieb.

3.2 Zabezpečiť, aby citlivé alebo regulované údaje uložené v cloude boli chránené primeranými technickými a organizačnými kontrolami.

3.3 Stanoviť jasné roly pri schvaľovaní, konfigurácii, monitorovaní a vyradení cloudových služieb.

3.4 Riadiť toky údajov a zabezpečiť plnenie povinností týkajúcich sa uchovávania, výmazu a ochrany súkromia pri informáciách uložených v cloude.

3.5 Znížiť závislosť od osobných účtov alebo neevidovaných nástrojov tým, že všetky cloudové systémy používané na pracovné účely podliehajú schváleniu.

3.6 Dodržiavať požiadavky ISO/IEC 27001:2022, GDPR, NIS2 a DORA na riadenie externých závislostí od cloudových služieb.

4. Roly a zodpovednosti

4.1 Generálny manažér (GM)

4.1.1 schvaľuje používanie všetkých nových cloudových služieb,

4.1.2 preskúmava riziká súvisiace s cloudovými poskytovateľmi a typmi služieb,

4.1.3 zabezpečuje uplatňovanie tejto politiky a dohliada na rozhodovanie o výnimkách.

4.2 IT provider alebo technická podpora

4.2.1 posudzuje a implementuje bezpečnú konfiguráciu cloudových služieb,

4.2.2 zriaďuje účty, riadenie prístupu a zálohovanie,

4.2.3 monitoruje súlad s požiadavkami na heslá, MFA a bezpečnostné nastavenia.

[... 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 Túto politiku musí najmenej raz ročne preskúmať Generálny manažér v koordinácii s IT providerom.

9.2 Formálne preskúmanie sa musí vykonať aj:

9.2.1 po bezpečnostnom incidente súvisiacom s cloudom (napr. porušenie ochrany údajov, strata údajov),

9.2.2 pri zavedení novej významnej cloudovej platformy,

9.2.3 ak sa zmenia právne alebo regulačné požiadavky (napr. aktualizácie GDPR, NIS2, DORA),

9.2.4 ak monitorovacie činnosti odhalia nesprávne používanie alebo nové riziká.

9.3 GM musí zabezpečiť, aby:

9.3.1 bol register cloudových služieb aktualizovaný o nové alebo vyradené služby,

9.3.2 boli naďalej plnené právne požiadavky a požiadavky na ochranu súkromia,

9.3.3 boli všetky zmeny oznámené relevantným používateľom a zainteresovaným stranám.

9.4 Archivované verzie musia byť bezpečne uchovávané a so starými verziami politiky sa musí nakladať v súlade s politikou organizácie P14S – Politika uchovávania a likvidácie údajov.

10. Súvisiace politiky a väzby

10.1 Táto politika sa musí používať v koordinácii s týmito politikami informačnej bezpečnosti zosúladenými pre MSP:

10.1.1 P2S – Politika rolí a zodpovedností v oblasti správy a riadenia: definuje zodpovednosti za schvaľovanie cloudových služieb a riadenie vzťahov s poskytovateľmi.

10.1.2 P4S – Politika riadenia prístupu: podporuje bezpečné prihlasovanie, riadenie relácií a postupy odoberania prístupu požadované pre cloudové platformy.

10.1.3 P14S – Politika uchovávania a likvidácie údajov: upravuje, ako sa údaje v cloudovom prostredí zálohujú, uchovávajú a vymazávajú v súlade so zákonnými povinnosťami.

10.1.4 P17S – Politika ochrany údajov a súkromia: zabezpečuje, aby sa s akýmikoľvek osobnými údajmi uloženými v cloudových službách nakladalo podľa zásad GDPR.

10.1.5 P30S – Politika reakcie na incidenty: poskytuje štruktúrované postupy reakcie na bezpečnostné incidenty v cloudovom prostredí vrátane zberu dôkazov a externého oznamovania.

10.2 Tieto politiky spoločne zabezpečujú, aby používanie cloudových služieb bolo bezpečné, v súlade s požiadavkami a prevádzkovo odolné.

11. Referenčné normy a rámce

11.1 ISO/IEC 27001

11.1.1 Kapitola 8.1 – vyžaduje, aby organizácie implementovali prevádzkové kontroly nakladania s údajmi vrátane kontrol súvisiacich s cloudovými systémami.

11.2 ISO/IEC 27002

11.2.1 Kontrola 5.23 – vyžaduje riadenie používania cloudových služieb a SaaS nástrojov tretích strán.

11.2.2 Kontrola 5.24 – vyžaduje definovanú politiku používania cloudových služieb zosúladenú s rizikami a regulačnými požiadavkami.

11.2.3 Kontrola 5.25 – vyžaduje, aby organizácie zabezpečili, že bezpečnostné kontroly v cloudovom prostredí zodpovedajú ich potrebám.

11.3 NIST SP 800-53 Rev.

11.3.1 AC-20 – vyžaduje formálne politiky používania externých systémov, ako sú cloudové služby.

11.3.2 SC-12, SC-13 – upravujú šifrovanie údajov pri prenose a údajov v pokoji v cloudovom prostredí.

11.3.3 SR-5 – pokrýva kontroly rizík cloudu a tretích strán v rámci dodávateľského reťazca.

11.4 Nariadenie EÚ GDPR (2016/679)

11.4.1 Článok 28 – vyžaduje, aby poskytovatelia cloudových služieb vystupujúci ako sprostredkovatelia dodržiavali záväzné zmluvné povinnosti.

11.4.2 Článok 32 – vyžaduje technické a organizačné opatrenia na spracúvanie údajov v cloudovom prostredí.

11.4.3 Kapitola V – zakazuje neoprávnené medzinárodné prenosy osobných údajov uložených v cloude.

11.5 Smernica EÚ NIS2 (2022/2555)

11.5.1 Článok 21(2)(f), (i) – vyžaduje, aby základné a dôležité subjekty zaviedli primerané politiky pre bezpečnosť cloudových služieb a riadenie dodávateľského reťazca.

11.6 Nariadenie EÚ DORA (2022/2554)

11.6.1 Článok 5(2) – vyžaduje, aby finančné MSP integrovali bezpečnosť cloudových služieb do svojich rámcov riadenia IKT rizík.

11.6.2 Článok 28 – stanovuje pravidlá dohľadu nad kritickými externými poskytovateľmi služieb IKT vrátane cloudových poskytovateľov.

11.7 COBIT 2019

11.7.1 DSS01 – „Riadenie prevádzky“ sa venuje prevádzkovej integrite cloudových služieb.

11.7.2 DSS05 – „Riadenie bezpečnostných služieb“ zahŕňa ochranné opatrenia a monitorovanie špecifické pre cloudové prostredie.

11.7.3 BAI04 – „Riadenie dostupnosti a kapacity“ zabezpečuje kontinuitu činností a výkonnosť v cloudovom prostredí.