					Sem vložte název registrované právnické osoby							
Číslo dokumentu: P27S					Název dokumentu: **Politika používání cloudových služeb**							
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	Kapitola 8	
ISO/IEC 27002:2022	Opatření 5.23–5.25	
NIST SP 800-53 Rev. 5	AC-20, SC-12, SC-13, SR-5	
GDPR	Článek 28, 32 a kapitola V	
směrnice NIS2	Článek 21 odst. 2 písm. f), i)	
nařízení DORA	Článek 5 odst. 2, 28	
COBIT 2019	DSS01, DSS05, BAI04	

1. Účel

1.1 Tato politika stanoví pravidla pro bezpečné používání cloudových služeb v organizaci. Zajišťuje, aby data zpracovávaná nebo uložená v cloudu byla chráněna, přístup k nim byl řízen a související rizika byla odpovídajícím způsobem řízena.

1.2 Pomáhá SME plnit právní povinnosti a očekávání zákazníků v oblasti ochrany citlivých informací, předcházení únikům dat a účinného řízení rizik spojených s cloudovými službami bez potřeby infrastruktury v rozsahu velkého podniku.

1.3 Tato politika podporuje certifikaci podle ISO/IEC 27001, soulad s GDPR a zabezpečení dodavatelského řetězce prostřednictvím konzistentní správy všech cloudových služeb třetích stran.

2. Rozsah

2.1 Tato politika se vztahuje na:

2.1.1 jakoukoli cloudovou službu používanou k ukládání, zpracování nebo přenosu firemních dat,

2.1.2 veškerý personál, dodavatele nebo poskytovatele služeb používající cloudové nástroje jménem organizace,

2.1.3 placená i bezplatná cloudová řešení, včetně e-mailových platforem, platforem pro sdílení dokumentů, nástrojů SaaS, zálohovacích platforem, videokonferenčních nástrojů a zákaznických platforem,

2.1.4 jakékoli zařízení (stolní počítač, mobilní telefon, tablet) přistupující k firemním informacím prostřednictvím cloudových aplikací.

2.2 To zahrnuje mimo jiné:

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 pro zálohování a obnovu po havárii,

2.2.5 sdílené složky nebo aplikace používané pro fakturaci, řízení projektů nebo komunikaci se zákazníky.

3. Cíle

3.1 Předcházet neoprávněnému nebo vysoce rizikovému používání neschválených cloudových služeb.

3.2 Zajistit, aby citlivá nebo regulovaná data uložená v cloudu byla zabezpečena vhodnými technickými a organizačními opatřeními.

3.3 Vymezit jasné role pro schvalování, konfiguraci, monitorování a vyřazování cloudových služeb z provozu.

3.4 Řídit datové toky a zajistit plnění povinností týkajících se uchovávání, mazání a ochrany soukromí u informací uložených v cloudu.

3.5 Omezit závislost na osobních účtech nebo nespravovaných nástrojích tím, že všechny cloudové systémy používané pro obchodní účely podléhají schválení.

3.6 Zajistit soulad s požadavky ISO/IEC 27001:2022, GDPR, NIS2 a DORA na řízení externích závislostí souvisejících s cloudovými službami.

4. Role a odpovědnosti

4.1 generální ředitel (GM)

4.1.1 schvaluje používání všech nových cloudových služeb,

4.1.2 přezkoumává rizika související s poskytovateli cloudových služeb a typy služeb,

4.1.3 zajišťuje uplatňování této politiky a rozhoduje o výjimkách.

4.2 poskytovatel IT podpory nebo technická podpora

4.2.1 vyhodnocuje a zavádí bezpečnou konfiguraci cloudových služeb,

4.2.2 zřizuje účty, řízení přístupu a zálohování,

4.2.3 monitoruje soulad s požadavky na hesla, vícefaktorovou autentizaci (MFA) a bezpečnostní nastavení.

[... 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 nejméně jednou ročně přezkoumána generálním ředitelem ve spolupráci s poskytovatelem IT podpory.

9.2 Formální přezkum musí proběhnout také:

9.2.1 po bezpečnostním incidentu souvisejícím s cloudem (např. porušení zabezpečení, ztráta dat),

9.2.2 při zavedení nové hlavní cloudové platformy,

9.2.3 pokud dojde ke změně právních nebo regulačních požadavků (např. aktualizace GDPR, NIS2 nebo DORA),

9.2.4 pokud monitorovací činnosti odhalí zneužití nebo nová rizika.

9.3 GM musí zajistit, aby:

9.3.1 byl Registr cloudových služeb aktualizován o nové nebo vyřazené služby,

9.3.2 byly i nadále plněny právní požadavky a požadavky na ochranu soukromí,

9.3.3 všechny změny byly oznámeny relevantním uživatelům a zainteresovaným stranám.

9.4 Archivované verze musí být bezpečně uloženy a se starými verzemi politiky musí být nakládáno v souladu s P14S – Politikou uchovávání údajů.

10. Související politiky a vazby

10.1 Tato politika musí být používána ve spojení s následujícími politikami informační bezpečnosti přizpůsobenými pro SME:

10.1.1 P2S – Politika rolí a odpovědností v oblasti správy a řízení: Vymezuje odpovědnost za schvalování cloudových služeb a řízení vztahů s poskytovateli.

10.1.2 P4S – Politika řízení přístupu: Podporuje bezpečné přihlašování, řízení relací a postupy odebírání přístupu požadované pro cloudové platformy.

10.1.3 P14S – Politika uchovávání údajů: Upravuje, jak jsou data v cloudu zálohována, uchovávána a mazána v souladu s právními povinnostmi.

10.1.4 P17S – Politika ochrany dat a soukromí: Zajišťuje, aby s osobními údaji uloženými v cloudových službách bylo nakládáno v souladu s požadavky GDPR.

10.1.5 P30S – Politika reakce na incidenty: Stanoví strukturované postupy pro reakci na bezpečnostní incidenty v cloudu, včetně shromažďování důkazů a externího oznamování.

10.2 Tyto politiky společně zajišťují, že používání cloudu je bezpečné, v souladu s požadavky a provozně odolné.

11. Referenční normy a rámce

11.1 ISO/IEC 27001

11.1.1 Kapitola 8.1 – Vyžaduje, aby organizace zavedly provozní opatření pro nakládání s daty, včetně opatření vztahujících se ke cloudovým systémům.

11.2 ISO/IEC 27002

11.2.1 Opatření 5.23 – Vyžaduje správu používání cloudových služeb a nástrojů SaaS třetích stran.

11.2.2 Opatření 5.24 – Vyžaduje stanovenou politiku používání cloudu v souladu s riziky a regulačními požadavky.

11.2.3 Opatření 5.25 – Vyžaduje, aby organizace zajistily, že bezpečnostní opatření v cloudových prostředích odpovídají potřebám organizace.

11.3 NIST SP 800-53 Rev. 5

11.3.1 AC-20 – Vyžaduje formální zásady používání externích systémů, jako jsou cloudové služby.

11.3.2 SC-12, SC-13 – Řeší šifrování dat při přenosu a dat v klidu v cloudových prostředích.

11.3.3 SR-5 – Pokrývá opatření pro řízení rizik cloudu a třetích stran v rámci dodavatelského řetězce.

11.4 GDPR (2016/679)

11.4.1 Článek 28 – Vyžaduje, aby poskytovatelé cloudových služeb vystupující jako zpracovatelé dodržovali závazné smluvní povinnosti.

11.4.2 Článek 32 – Vyžaduje technická a organizační opatření pro cloudové zpracování dat.

11.4.3 Kapitola V – Zakazuje neoprávněné mezinárodní přenosy osobních údajů uložených v cloudu.

11.5 směrnice NIS2 (2022/2555)

11.5.1 Článek 21 odst. 2 písm. f), i) – Vyžaduje, aby základní a významné subjekty zavedly odpovídající politiky pro bezpečnost cloudových služeb a řízení dodavatelského řetězce.

11.6 nařízení DORA (2022/2554)

11.6.1 Článek 5 odst. 2 – Vyžaduje, aby finanční SME začlenily bezpečnost cloudu do svých rámců řízení rizik v oblasti ICT.

11.6.2 Článek 28 – Stanoví pravidla dohledu nad kritickými externími poskytovateli služeb ICT, včetně poskytovatelů cloudových služeb.

11.7 COBIT 2019

11.7.1 DSS01 – „Manage Operations“ se zabývá provozní integritou cloudových služeb.

11.7.2 DSS05 – „Manage Security Services“ zahrnuje ochranná opatření a monitorování specifická pro cloud.

11.7.3 BAI04 – „Manage Availability and Capacity“ zajišťuje kontinuitu činností a výkonnost v cloudových prostředích.