					Sem vložte název registrované právnické osoby							
Číslo dokumentu: P27					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	Článek 8	Požadavky na provozní plánování a řízení v cloudovém prostředí.
ISO/IEC 27002:2022	Opatření 5.23–5.25	Požadavky na používání cloudových služeb, související politiku a jejich zabezpečení.
NIST SP 800-53 Rev.5	AC-20, SA-9(5), SC-12 – SC-28, SR-5	Používání externích systémů, smluvní a technické požadavky, kryptografická ochrana a ochrana dodavatelského řetězce.
GDPR	Články 28, 32, kapitola V	Požadavky na cloudové zpracovatele, zabezpečení zpracování a přenosy dat.
směrnice NIS2	Článek 21(2)(f, i)	Požadavky na řízení rizik třetích stran a dodavatelského řetězce.
nařízení DORA	Články 5(2), 28	Dohled nad ICT a třetími stranami (cloud) u finančních subjektů.
COBIT 2019	BAI04, DSS01, DSS05	Dostupnost cloudových služeb, provoz a řízení bezpečnosti.

1. Účel

1.1 Tato politika stanoví závazné požadavky organizace na bezpečné, souladné a odpovědné používání cloudových služeb napříč modely poskytování Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) a Software-as-a-Service (SaaS).

1.2 Cílem této politiky je zajistit, aby cloudové služby byly zaváděny a spravovány způsobem, který chrání důvěrnost, integritu a dostupnost informačních aktiv a současně zajišťuje plnění regulačních, právních a smluvních povinností.

1.3 Politika vymezuje bezpečnostní opatření pro řízení cloudových rizik, ochranu dat, monitorování souladu poskytovatelů a prevenci neoprávněného používání. Současně podporuje inovace prostřednictvím cloudových platforem sladěním bezpečnosti, provozní spolehlivosti a nákladové efektivity.

2. Rozsah

2.1 Tato politika se vztahuje na všechny zaměstnance, smluvní pracovníky, poskytovatele služeb třetích stran a externí konzultanty, kteří jménem organizace zřizují, konfigurují, používají, spravují nebo jinak využívají cloudové služby.

2.2 Vztahuje se na všechna prostředí, v nichž jsou zpracovávána data nebo provozovány pracovní zátěže organizace, včetně:

2.2.1 veřejných, privátních, hybridních a komunitních cloudových nasazení,

2.2.2 všech modelů cloudových služeb (IaaS, PaaS, SaaS),

2.2.3 multicloudových a federovaných architektur,

2.2.4 používání shadow IT nebo osobních cloudových účtů pro pracovní účely.

2.3 Zahrnuje všechny úrovně klasifikace dat a vztahuje se na interní systémy i platformy hostované dodavateli, na nichž jsou ukládána nebo zpracovávána data vlastněná organizací nebo regulovaná data.

3. Cíle

3.1 Zajistit bezpečné a konzistentní používání cloudových technologií prostřednictvím jasně stanovených pravidel používání, výchozích bezpečnostních opatření a rolí v oblasti správy a řízení.

3.2 Minimalizovat provozní a regulační rizika spojená s cloud computingem, včetně neoprávněného přístupu, narušení bezpečnosti dat, chybné konfigurace, nesouladu a výpadků služeb.

3.3 Prosazovat bezpečnostní požadavky a požadavky na ochranu soukromí u všech cloudových dodavatelů a ověřovat soulad prostřednictvím smluvních ustanovení, posouzení a práv na audit.

3.4 Umožnit škálovatelné a odolné zavádění cloudových služeb bez narušení úrovně bezpečnosti, právních požadavků nebo kontinuity činností.

3.5 Sladit správu a používání cloudových služeb s rámcem ISMS organizace, právními povinnostmi (např. GDPR, DORA), oborově specifickými pokyny a obecně uznávanými osvědčenými postupy (např. NIST, COBIT).

4. Role a odpovědnosti

4.1 Vrcholové vedení

4.1.1 Schvaluje tuto politiku a strategický plán zavádění cloudových služeb.

4.1.2 Přezkoumává a schvaluje výjimky s vysokým rizikem ze standardních požadavků na správu a řízení cloudových služeb.

4.1.3 Zajišťuje, aby cloudové iniciativy měly odpovídající financování, dohled a vazbu na podnikový rámec řízení rizik.

4.2 Ředitel informační bezpečnosti (CISO)

4.2.1 Odpovídá za tuto politiku a za centrální registr cloudových služeb organizace.

4.2.2 Schvaluje zavedení nových cloudových poskytovatelů na základě prověření dodavatele a vyhodnocení rizik.

4.2.3 Přezkoumává dokumentaci poskytovatele k souladu a ověřuje soulad s bezpečnostními požadavky.

[... 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 nejméně jednou ročně a podle potřeby aktualizována tak, aby byl zachován soulad s:

9.1.1 vyvíjejícími se právními a regulačními požadavky (např. GDPR, NIS2, DORA),

9.1.2 změnami norem ISO/IEC 27001 nebo ISO/IEC 27002,

9.1.3 aktualizacemi cloudové architektury organizace, prostředí hrozeb nebo portfolia služeb,

9.1.4 vyšetřováním incidentů, výsledky auditů nebo poznatky z provozního používání.

9.2 CISO odpovídá za zahájení přezkumu a svolání relevantních zainteresovaných stran, včetně:

9.2.1 architekta cloudové bezpečnosti,

9.2.2 týmu právní a compliance,

9.2.3 týmů nákupu a manažerů dodavatelů,

9.2.4 vlastníků služeb a IT provozu.

9.3 Všechny aktualizace musí být:

9.3.1 vedeny v režimu správy verzí a datovány,

9.3.2 schváleny vrcholovým vedením,

9.3.3 oznámeny dotčeným stranám, včetně zaměstnanců, smluvních pracovníků a třetích stran,

9.3.4 archivovány v souladu s interními politikami dokumentace.

9.4 Mimořádné přezkumy mohou být vyvolány:

9.4.1 navázáním nových vztahů s CSP nebo významnými migracemi,

9.4.2 nově vznikajícími hrozbami pro cloudovou infrastrukturu,

9.4.3 významnými změnami smluvních, právních nebo oborově specifických povinností.

10. Související politiky a vazby

10.1 Tato politika úzce souvisí s následujícími interními politikami a je na nich závislá:

10.1.1 P1 – Politika informační bezpečnosti: Stanoví zastřešující principy pro bezpečný provoz systémů a služeb, které tato politika uplatňuje v kontextu cloudových služeb.

10.1.2 P5 – Politika řízení změn: Všechny změny konfigurace cloudových služeb musí probíhat podle postupů řízení změn stanovených v P5.

10.1.3 P13 – Politika klasifikace dat a označování: Určuje, jak jsou data posuzována před přenosem do cloudu a jak se uplatňují bezpečnostní opatření, jako je šifrování a umístění dat.

10.1.4 P18 – Politika kryptografických opatření: Poskytuje standardy pro šifrování, správu klíčů a používání kryptografických algoritmů, které se přímo uplatňují v konfiguracích cloudových služeb.

10.1.5 P22 – Politika protokolování a monitorování: Stanoví požadavky na sběr, uchovávání a analýzu logů, které musí být uplatňovány v cloudových prostředích.

10.1.6 P30 – Politika reakce na incidenty: Definuje eskalační postupy, omezení dopadu a nápravná opatření pro bezpečnostní události související s cloudem.

10.1.7 P33 – Politika monitorování auditu a souladu: Podporuje připravenost na audit a průběžné zajištění, že cloudová opatření jsou uplatňována a monitorována.

11. Referenční normy a rámce

11.1 ISO/IEC 27001: Článek 8.1 – provozní plánování a řízení: Vyžaduje, aby organizace zavedly a řídily procesy potřebné ke splnění požadavků na bezpečnost informací, včetně procesů zahrnujících cloudová prostředí.

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

11.2.1 Příloha A, opatření 5.23 – používání cloudových služeb: Vyžaduje posouzení založené na riziku, formální schválení a dokumentaci používání cloudových služeb.

11.2.2 Příloha A, opatření 5.24 – politika používání cloudových služeb: Vyžaduje zavedení a uplatňování formálních politik používání cloudových služeb v souladu s potřebami a riziky organizace.

11.2.3 Příloha A, opatření 5.25 – bezpečnost cloudových služeb: Vyžaduje integraci bezpečnosti, smluvní ochranu a monitorování cloudově hostovaných pracovních zátěží a dat.

11.3 NIST SP 800-53 Rev.5:

11.3.1 AC-20 – používání externích systémů: Vyžaduje definovaná pravidla a podmínky pro přístup k prostředkům organizace z externích nebo cloudových systémů.

11.3.2 SA-9(5) – služby externích informačních systémů: Vyžaduje smluvní bezpečnostní požadavky, dohled a průběžné monitorování systémů třetích stran v cloudu.

11.3.3 SC-12 až SC-28 – kryptografická ochrana, ochrana perimetru a integrita přenosu: Jsou v souladu s požadavky na šifrování, identitu a přístup pro cloudově hostované služby a data při přenosu.

11.3.4 SR-5 – ochrana dodavatelského řetězce: Podporuje prověřování a smluvní řízení CSP zapojených do poskytování služeb.

11.4 GDPR (2016/679):

11.4.1 Článek 28 – povinnosti zpracovatele: Vyžaduje formální smlouvy s cloudovými poskytovateli k zajištění bezpečnosti, důvěrnosti a auditovatelnosti zpracování osobních údajů.

11.4.2 Článek 32 – zabezpečení zpracování: Podporuje uplatnění šifrování, řízení přístupu, protokolování a dalších ochranných opatření v cloudových prostředích.

11.4.3 Kapitola V – mezinárodní přenosy dat: Vyžaduje zákonný přenos dat mimo EU/EHP s využitím ochranných mechanismů, jako jsou standardní smluvní doložky (SCC) nebo rozhodnutí o odpovídající ochraně.

11.5 směrnice NIS2 (2022/2555):

11.5.1 Článek 21(2)(f, i): Vyžaduje, aby subjekty řídily rizika vyplývající z poskytovatelů cloudových služeb třetích stran a zajišťovaly integritu digitálního dodavatelského řetězce prostřednictvím smluvních a technických opatření.

11.6 nařízení DORA (2022/2554):

11.6.1 Článek 5(2) – správa ICT rizik: Vyžaduje začlenění rizik ICT třetích stran, včetně cloudových služeb, do celkové správy a řízení rizik.

11.6.2 Článek 28 – dohled nad kritickými externími poskytovateli ICT služeb: Vyžaduje, aby finanční subjekty monitorovaly, řídily a vykazovaly závislosti na cloudových poskytovatelích, jejich bezpečnostní stav a odolnost.

11.7 COBIT 2019:

11.7.1 BAI04 – řízení dostupnosti a kapacity: Zajišťuje, aby cloudové služby byly odolné, monitorované a plnily definovaná kritéria výkonnosti.

11.7.2 DSS01 – řízení provozu: Podporuje provozní integraci, zvládání incidentů a výchozí konfigurace napříč cloudově hostovanými platformami.

11.7.3 DSS05 – řízení bezpečnostních služeb: Směřuje implementaci cloudově specifických bezpečnostních opatření, monitorování a prevenci incidentů napříč digitálními službami.