					Sem vložte název registrované právnické osoby						
Číslo dokumentu: P26S					Název dokumentu: **Bezpečnostní politika dodavatelů a poskytovatelů služeb třetích stran**						
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	Provozní opatření pro vztahy s třetími stranami a dodavateli
ISO/IEC 27002:2022	Opatření 5.19–5.22	Bezpečnostní opatření pro dodavatele, smluvní bezpečnostní ustanovení, řízení změn, monitorování a přezkum
NIST SP 800-53 Rev.5	SA-9, SA-10, CA-3, PS-7	Pořizování, konfigurace, dohody o propojení a opatření týkající se externího personálu
GDPR	Články 28, 32	smlouva o zpracování osobních údajů, požadavky na bezpečnost zpracovatele
směrnice NIS2	Články 21(2)(a)(b)(i), 23(1)	Řízení rizik v dodavatelském řetězci, dohled nad službami třetích stran
nařízení DORA	Články 5(1)(2), 28(1)(2)	Řízení rizik v oblasti ICT u poskytovatelů služeb třetích stran
COBIT 2019	APO10, APO12, DSS05	Řízení dodavatelů a integrace rizik

1. Účel

1.1 Tato politika stanoví závazné bezpečnostní požadavky pro navazování, řízení a ukončování vztahů s třetími stranami a dodavateli, kteří přistupují k datům, systémům nebo službám organizace nebo je ovlivňují.

1.2 Zajišťuje, aby externí poskytovatelé, včetně poskytovatelů IT podpory, provozovatelů cloudových služeb, vývojářů softwaru a dodavatelů zajišťujících podnikové procesy, nakládali s aktivy organizace bezpečně a v souladu s příslušnými právními předpisy a normami.

1.3 Tato politika snižuje rizika, jako jsou úniky dat, neoprávněné změny systémů, regulatorní sankce nebo přerušení činností způsobené nezabezpečenými nebo nedostatečně řízenými vztahy s třetími stranami.

2. Rozsah

2.1 Tato politika se vztahuje na všechny třetí strany, které:

2.1.1 poskytují software, infrastrukturu, hosting nebo cloudové služby,

2.1.2 přistupují k interním systémům, zařízením nebo aplikacím nebo je spravují,

2.1.3 nakládají s daty organizace, dokumenty nebo zálohami,

2.1.4 podporují obchodní operace, lidské zdroje, finance nebo zákaznické služby.

2.2 Tato politika se dále vztahuje na:

2.2.1 interní pracovníky podílející se na výběru, pořizování nebo dohledu nad dodavateli,

2.2.2 veškerý personál, který řídí onboarding dodavatelů, smlouvy, přístupy nebo přezkumy,

2.2.3 jakýkoli systém nebo proces závislý na komponentách nebo službách třetích stran.

3. Cíle

3.1 Zajistit, aby všichni dodavatelé splňovali jasně definovaná bezpečnostní očekávání.

3.2 Vyžadovat, aby smlouvy s dodavateli obsahovaly vymahatelné povinnosti v oblasti bezpečnosti, ochrany soukromí a reakce na incidenty.

3.3 Posoudit a zdokumentovat rizika dodavatelů před podpisem smlouvy nebo udělením přístupu.

3.4 Uplatňovat pravidelné přezkumy u vysoce rizikových nebo kritických dodavatelů za účelem potvrzení souladu.

3.5 Zavést formální proces pro výjimky, řízení incidentů a aktualizace smluv.

3.6 Podporovat soulad s povinnostmi podle ISO/IEC 27001:2022, GDPR, NIS2 a DORA vztahujícími se ke správě dodavatelů.

4. Role a odpovědnosti

4.1 generální ředitel (GM)

4.1.1 nese konečnou odpovědnost za výběr dodavatelů a zajištění souladu v oblasti bezpečnosti,

4.1.2 schvaluje smlouvy, výjimky a eskalace týkající se dodavatelů,

4.1.3 vykonává dohled nad reakcí na incidenty a rozhodováním v případech, kdy dodavatelé nesplní své povinnosti.

4.2 externí poskytovatel IT služeb nebo interní bezpečnostní kontakt

4.2.1 posuzuje technický přístup požadovaný dodavateli,

4.2.2 zavádí pravidla řízení přístupu, přezkoumává protokoly a ověřuje bezpečné nakládání s daty,

4.2.3 přezkoumává důkazy o bezpečnostních opatřeních, certifikacích nebo výsledcích auditů, jsou-li k dispozici.

[... 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 za účasti poskytovatele IT podpory nebo manažera dodavatelů.

9.2 Politika musí být dále přezkoumána:

9.2.1 po jakékoli významné změně právních, regulatorních nebo smluvních povinností,

9.2.2 po bezpečnostním incidentu souvisejícím s dodavatelem nebo po zjištění auditu,

9.2.3 při zavedení nových kategorií dodavatelů (např. kritických platforem SaaS).

9.3 Veškeré aktualizace musí být:

9.3.1 zdokumentovány s historií verzí a odůvodněním,

9.3.2 schváleny generálním ředitelem,

9.3.3 oznámeny relevantním interním pracovníkům a manažerům dodavatelů,

9.3.4 uloženy společně s předchozími verzemi podle P14S – Politika uchovávání údajů.

10. Související politiky a vazby

10.1 Účinnost této politiky závisí na koordinaci s následujícími SME politikami informační bezpečnosti:

10.1.1 P2S – Politika rolí a odpovědností v oblasti správy a řízení: přiřazuje odpovědnost za dohled nad dodavateli a uplatňování smluvních podmínek.

10.1.2 P4S – Politika řízení přístupu: stanoví pravidla omezení přístupu, která musí být uplatněna při udělení systémového přístupu dodavatelům.

10.1.3 P17S – Politika ochrany dat a soukromí: zajišťuje, aby dodavatelé zpracovávající osobní údaje dodržovali zásady ochrany dat a právní požadavky.

10.1.4 P14S – Politika uchovávání údajů: vztahuje se na jakákoli data nebo záznamy sdílené s dodavateli nebo jimi ukládané a upravuje bezpečnou likvidaci po ukončení smlouvy.

10.1.5 P30S – Politika reakce na incidenty: stanoví, jak reagovat v případě, že dodavatel způsobí bezpečnostní incident nebo je do něj zapojen, včetně postupů eskalace a nakládání s důkazy.

10.2 Tyto politiky společně zajišťují, že rizika spojená s dodavateli jsou řízena v průběhu celého životního cyklu smlouvy.

11. Referenční normy a rámce

11.1 ISO/IEC 27001

11.1.1 Kapitola 8 – vyžaduje zavedení provozních opatření, včetně těch, která se uplatňují na vztahy s třetími stranami a dodavateli.

11.2 ISO/IEC 27002

11.2.1 Opatření 5.19 – zajišťuje, že bezpečnostní opatření dodavatelů jsou v souladu s požadavky organizace.

11.2.2 Opatření 5.20 – vyžaduje formální dohody zahrnující bezpečnostní podmínky, odpovědnosti a povinnosti při porušení.

11.2.3 Opatření 5.21 – upravuje změny ve službách dodavatelů, které mohou ovlivnit stav bezpečnosti.

11.2.4 Opatření 5.22 – vyžaduje monitorování a přezkum služeb dodavatelů a souladu.

11.3 NIST SP 800-53 Rev.5

11.3.1 SA-9 – upravuje pořizování externích systémů a služeb a vyžaduje hodnocení rizik a jasně stanovená očekávání.

11.3.2 SA-10 – upravuje konfiguraci a postupy změn zahrnující systémy spravované třetími stranami.

11.3.3 CA-3 – vyžaduje dohody o propojení systémů zahrnujících externí subjekty.

11.3.4 PS-7 – stanoví prověřování a odpovědnost externího personálu.

11.4 GDPR (EU) 2016/679

11.4.1 Článek 28 – vyžaduje smlouvy o zpracování osobních údajů s dodavateli vystupujícími jako zpracovatelé.

11.4.2 Článek 32 – ukládá všem zpracovatelům osobních údajů povinnost zavést přiměřená technická a organizační bezpečnostní opatření.

11.5 směrnice EU NIS2 (2022/2555)

11.5.1 Článek 21(2)(a), (b), (i) – ukládá řízení rizik v dodavatelském řetězci ICT a opatření vůči třetím stranám.

11.5.2 Článek 23(1) – vyžaduje zdokumentovaný dohled nad službami třetích stran pro základní a důležité subjekty.

11.6 nařízení EU DORA (2022/2554)

11.6.1 Článek 5(1) – vyžaduje rámec řízení rizik v oblasti ICT pokrývající všechny kritické poskytovatele třetích stran.

11.6.2 Článek 5(2) – stanoví smluvní a provozní opatření pro závislosti na službách ICT.

11.6.3 Článek 28(1), (2) – stanoví pravidla dohledu nad riziky ICT třetích stran ve finančním sektoru.

11.7 COBIT 2019

11.7.1 APO10 – „Manage Suppliers“ vymezuje opatření pro sourcing a očekávání v oblasti řízení vztahů.

11.7.2 APO12 – „Manage Risk“ začleňuje rizika dodavatelů do správy a řízení rizik organizace.

11.7.3 DSS05 – „Manage Security Services“ se vztahuje na řízené dodavatele a outsourcované služby.