					Sem zadajte názov registrovanej právnickej osoby							
Číslo dokumentu: P26S					Názov dokumentu: **Politika bezpečnosti tretích strán a dodávateľov**							
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**

Súlad s normami a predpismi

Norma/predpis	Kapitola/článok	Poznámka
ISO/IEC 27001:2022	Kapitola 8	Prevádzkové kontrolné opatrenia pre vzťahy s tretími stranami a dodávateľmi
ISO/IEC 27002:2022	Kontroly 5.19–5.22	Bezpečnostné opatrenia dodávateľov, zmluvné bezpečnostné podmienky, riadenie zmien, monitorovanie a preskúmanie
NIST SP 800-53 Rev.5	SA-9, SA-10, CA-3, PS-7	Obstarávanie, konfigurácia, dohody o prepojení a preverovanie externého personálu
Nariadenie (EÚ) 2016/679 (GDPR)	Články 28, 32	Zmluvy o spracúvaní osobných údajov, bezpečnostné požiadavky na sprostredkovateľov
Smernica (EÚ) 2022/2555 (NIS2)	Články 21(2)(a)(b)(i), 23(1)	Riadenie rizík dodávateľského reťazca, dohľad nad službami tretích strán
Nariadenie (EÚ) 2022/2554 (DORA)	Články 5(1)(2), 28(1)(2)	Riadenie rizík IKT pri poskytovateľoch služieb tretích strán
COBIT 2019	APO10, APO12, DSS05	Riadenie dodávateľov a integrácia rizík

1. Účel

1.1 Táto politika stanovuje povinné bezpečnostné požiadavky na nadväzovanie, riadenie a ukončovanie vzťahov s tretími stranami a dodávateľmi, ktorí pristupujú k údajom, systémom alebo službám organizácie alebo ich ovplyvňujú.

1.2 Zabezpečuje, aby externí poskytovatelia vrátane dodávateľov IT podpory, poskytovateľov cloudových služieb, vývojárov softvéru a zmluvných poskytovateľov podnikových procesov nakladali s aktívami organizácie bezpečným spôsobom a v súlade s uplatniteľnými právnymi predpismi a normami.

1.3 Táto politika znižuje riziká, ako sú úniky údajov, neoprávnené zmeny systémov, regulačné pokuty alebo narušenie prevádzky spôsobené nezabezpečenými alebo nedostatočne riadenými vzťahmi s tretími stranami.

2. Rozsah

2.1 Táto politika sa vzťahuje na všetky tretie strany, ktoré:

2.1.1 poskytujú softvér, infraštruktúru, hostingové služby alebo cloudové služby,

2.1.2 pristupujú k interným systémom, zariadeniam alebo aplikáciám alebo ich spravujú,

2.1.3 nakladajú s údajmi organizácie, dokumentmi alebo zálohami,

2.1.4 podporujú prevádzkové činnosti, ľudské zdroje, financie alebo zákaznícke služby.

2.2 Táto politika sa vzťahuje aj na:

2.2.1 interných zamestnancov zapojených do výberu, obstarávania alebo dohľadu nad dodávateľmi,

2.2.2 všetkých pracovníkov, ktorí riadia začatie spolupráce s dodávateľom, zmluvy, prístupy alebo preskúmania,

2.2.3 akýkoľvek systém alebo proces závislý od komponentov alebo služieb tretích strán.

3. Ciele

3.1 Zabezpečiť, aby všetci dodávatelia spĺňali jasne definované bezpečnostné očakávania.

3.2 Vyžadovať, aby zmluvy s dodávateľmi obsahovali zmluvne vymáhateľné povinnosti v oblasti bezpečnosti, ochrany súkromia a reakcie na incidenty.

3.3 Posúdiť a zdokumentovať riziká dodávateľov pred podpisom dohody alebo udelením prístupu.

3.4 Vykonávať pravidelné preskúmania kritických dodávateľov alebo dodávateľov s vysokým rizikom na overenie súladu.

3.5 Zaviesť formálny proces udeľovania výnimiek, riadenia incidentov a aktualizácie zmlúv.

3.6 Podporovať plnenie povinností podľa ISO/IEC 27001:2022, GDPR, NIS2 a DORA súvisiacich so správou a riadením dodávateľov.

4. Roly a zodpovednosti

4.1 Generálny manažér (GM)

4.1.1 Nesie konečnú zodpovednosť za výber dodávateľov a súlad s bezpečnostnými požiadavkami.

4.1.2 Schvaľuje zmluvy, výnimky a eskalácie súvisiace s dodávateľmi.

4.1.3 Dohliada na reakciu na incidenty a rozhodovanie v prípadoch, keď dodávatelia nesplnia svoje povinnosti.

4.2 Poskytovateľ IT služieb alebo interná kontaktná osoba pre informačnú bezpečnosť

4.2.1 Posudzuje technický rozsah prístupu požadovaný dodávateľmi.

4.2.2 Zavádza pravidlá riadenia prístupu, preskúmava auditné záznamy a overuje bezpečné nakladanie s údajmi.

4.2.3 Preskúmava dôkazy o bezpečnostných kontrolných opatreniach, certifikáciách alebo výsledkoch auditov, ak sú dostupné.

[... 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 za účasti poskytovateľa IT služieb alebo osoby zodpovednej za riadenie dodávateľov.

9.2 Politika sa musí preskúmať aj:

9.2.1 po každej významnej zmene zákonných, regulačných alebo zmluvných povinností,

9.2.2 po bezpečnostnom incidente súvisiacom s dodávateľom alebo po auditnom zistení,

9.2.3 pri zapojení nových kategórií dodávateľov, napr. kritických platforiem SaaS.

9.3 Všetky aktualizácie musia byť:

9.3.1 zdokumentované s evidenciou verzií a odôvodnením,

9.3.2 schválené Generálnym manažérom,

9.3.3 oznámené relevantným interným zamestnancom a osobám zodpovedným za riadenie dodávateľov,

9.3.4 uložené spolu s predchádzajúcimi verziami podľa P14S – Politika uchovávania a likvidácie údajov.

10. Súvisiace politiky a väzby

10.1 Účinnosť tejto politiky závisí od koordinácie s týmito politikami informačnej bezpečnosti pre MSP:

10.1.1 P2S – Politika rolí a zodpovedností v oblasti správy a riadenia: určuje zodpovednosť za dohľad nad dodávateľmi a uplatňovanie zmluvných podmienok.

10.1.2 P4S – Politika riadenia prístupu: stanovuje pravidlá obmedzenia prístupu, ktoré sa musia uplatniť pri udeľovaní prístupu dodávateľom do systémov.

10.1.3 P17S – Politika ochrany údajov a súkromia: zabezpečuje, aby dodávatelia spracúvajúci osobné údaje dodržiavali zásady ochrany údajov a právne požiadavky.

10.1.4 P14S – Politika uchovávania a likvidácie údajov: vzťahuje sa na všetky údaje alebo záznamy zdieľané s dodávateľmi alebo uchovávané dodávateľmi a upravuje bezpečnú likvidáciu po ukončení zmluvy.

10.1.5 P30S – Politika reakcie na incidenty: určuje spôsob reakcie, ak dodávateľ spôsobí bezpečnostný incident alebo je doň zapojený, vrátane eskalácie a postupov nakladania s dôkazmi.

10.2 Tieto politiky spoločne zabezpečujú, že riziko dodávateľov je riadené počas celého životného cyklu zmluvy.

11. Referenčné normy a rámce

11.1 ISO/IEC 27001

11.1.1 Kapitola 8.1 – Vyžaduje zavedenie prevádzkových kontrolných opatrení vrátane tých, ktoré sa uplatňujú na vzťahy s tretími stranami a dodávateľmi.

11.2 ISO/IEC 27002

11.2.1 Kontrola 5.19 – Zabezpečuje, aby bezpečnostné opatrenia dodávateľov boli zosúladené s požiadavkami organizácie.

11.2.2 Kontrola 5.20 – Vyžaduje formálne dohody upravujúce bezpečnostné podmienky, zodpovednosti a povinnosti pri porušení bezpečnosti.

11.2.3 Kontrola 5.21 – Riadi zmeny v službách dodávateľov, ktoré môžu ovplyvniť bezpečnostný stav.

11.2.4 Kontrola 5.22 – Vyžaduje monitorovanie a preskúmanie služieb dodávateľov a ich súladu.

11.3 NIST SP 800-53 Rev.5

11.3.1 SA-9 – Upravuje obstarávanie externých systémov a služieb a vyžaduje posúdenia rizík a definované očakávania.

11.3.2 SA-10 – Upravuje riadenie konfigurácie a postupy zmien pri systémoch spravovaných tretími stranami.

11.3.3 CA-3 – Vyžaduje dohody o prepojení systémov zahŕňajúcich externé subjekty.

11.3.4 PS-7 – Upravuje preverovanie externého personálu a pridelenie zodpovednosti.

11.4 Nariadenie (EÚ) 2016/679 (GDPR)

11.4.1 Článok 28 – Vyžaduje zmluvy o spracúvaní osobných údajov s dodávateľmi vystupujúcimi ako sprostredkovatelia.

11.4.2 Článok 32 – Ukladá povinnosť zaviesť primerané technické a organizačné bezpečnostné opatrenia pre všetkých sprostredkovateľov spracúvania osobných údajov.

11.5 Smernica (EÚ) 2022/2555 (NIS2)

11.5.1 Článok 21(2)(a), (b), (i) – Ukladá riadenie rizík dodávateľského reťazca IKT a kontroly tretích strán.

11.5.2 Článok 23(1) – Vyžaduje zdokumentovaný dohľad nad službami tretích strán pre základné a dôležité subjekty.

11.6 Nariadenie (EÚ) 2022/2554 (DORA)

11.6.1 Článok 5(1) – Vyžaduje rámec riadenia rizík IKT pokrývajúci všetkých kritických externých poskytovateľov služieb IKT.

11.6.2 Článok 5(2) – Stanovuje zmluvné a prevádzkové kontroly pre závislosti od služieb IKT.

11.6.3 Článok 28(1), (2) – Stanovuje pravidlá dohľadu nad rizikami tretích strán v oblasti IKT vo finančnom sektore.

11.7 COBIT 2019

11.7.1 APO10 – „Manage Suppliers“ opisuje obstarávacie kontroly a očakávania pri riadení vzťahov.

11.7.2 APO12 – „Manage Risk“ integruje riziká dodávateľov do správy a riadenia rizík organizácie.

11.7.3 DSS05 – „Manage Security Services“ sa vzťahuje na spravované služby tretích strán a externých poskytovateľov služieb.