					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**

V súlade s normami a regulačnými požiadavkami

Norma/predpis	Kapitola/článok	Poznámka
ISO/IEC 27001:2022	Kapitola 8	Prevádzkové plánovanie a riadenie: vyžaduje formálne kontroly nad službami tretích strán, ktoré majú vplyv na systém manažérstva informačnej bezpečnosti (ISMS)
ISO/IEC 27002:2022	Kontroly 5.19–5.22	Politiky a postupy pre vzťahy s dodávateľmi; riadenie rizík dodávateľov; riadenie poskytovania služieb dodávateľmi; monitorovanie a preskúmavanie dodávateľov
NIST SP 800-53 Rev. 5	SA-9, SA-10, CA-3, PS-7	Služby externých systémov; riadenie konfigurácie vývojárom; prepojenia systémov; personálna bezpečnosť tretích strán
GDPR EÚ	Články 28, 32, 33	Povinnosti sprostredkovateľa; bezpečnosť spracúvania; oznamovanie porušenia ochrany osobných údajov
Smernica EÚ NIS2	Článok 21(2)(e–f)	riadenie dodávateľov založené na riziku a bezpečnostný dohľad
Nariadenie EÚ DORA	Články 28, 30	riziko IKT tretích strán, dohľad nad kritickými externými poskytovateľmi IKT
COBIT 2019	BAI05, DSS02, MEA03	Riadenie zavádzania organizačných zmien; riadenie požiadaviek na služby a incidentov; monitorovanie, hodnotenie a posudzovanie súladu

1. Účel

1.1 Táto politika stanovuje požiadavky informačnej bezpečnosti na nadväzovanie, riadenie a udržiavanie bezpečných vzťahov s dodávateľmi a externými poskytovateľmi služieb.

1.2 Zabezpečuje, aby všetci dodávatelia s prístupom k údajom, systémom alebo infraštruktúre organizácie podliehali primeraným bezpečnostným kontrolám, zmluvným ochranným opatreniam a priebežnému dohľadu počas celého životného cyklu služby.

1.3 Politika podporuje kontroly 5.19 až 5.22 prílohy A normy ISO/IEC 27001 tým, že začleňuje bezpečnostné požiadavky do obstarávania, náležitej starostlivosti o dodávateľov, procesu nástupu, due diligence dodávateľov, riadenia zmlúv, monitorovania služieb a procesov ukončenia.

2. Rozsah

2.1 Táto politika sa vzťahuje na:

2.1.1 všetkých dodávateľov, zmluvných pracovníkov, poskytovateľov cloudových služieb a servisné organizácie tretích strán, ktoré spracúvajú informačné aktíva organizácie alebo k nim pristupujú,

2.1.2 všetky interné roly zapojené do hodnotenia dodávateľov, nástupu, uzatvárania zmlúv, riadenia rizík, monitorovania alebo ukončenia vzťahu,

2.1.3 všetky dodávateľské vzťahy, ktoré zahŕňajú prístup k citlivým údajom, integráciu s produkčnými službami alebo podporu kritických funkcií organizácie.

2.2 Zahŕňa priamych dodávateľov aj ich subdodávateľov, ak je to relevantné, a vzťahuje sa na softvér tretích strán, infraštruktúru, podporu a riadené služby.

3. Ciele

3.1 Zabezpečiť, aby sa bezpečnostné riziká dodávateľov konzistentne identifikovali, posudzovali a zmierňovali počas celého životného cyklu vzťahu.

3.2 Zaviesť štandardizované bezpečnostné požiadavky do všetkých zmlúv s dodávateľmi vrátane oznamovacích povinností pri porušení ochrany údajov, ustanovení o práve na audit a zodpovedností v oblasti ochrany údajov.

3.3 Vyžadovať formálne due diligence a zdokumentované posúdenie rizík pred zapojením nových dodávateľov alebo obnovením zmlúv o poskytovaní služieb s vysokým rizikom.

3.4 Zaviesť mechanizmy na priebežné monitorovanie súladu dodávateľov vrátane preskúmaní výkonnosti, auditov a eskalácie incidentov.

3.5 Riadiť zmeny v službách dodávateľov a zabezpečiť bezpečný offboarding a vrátenie alebo likvidáciu údajov pri ukončení zmluvného vzťahu.

3.6 Zosúladiť bezpečnostné kontroly tretích strán s príslušnými regulačnými a zmluvnými povinnosťami vrátane GDPR, NIS2, DORA a normy ISO/IEC 27001.

4. Roly a zodpovednosti

4.1 riaditeľ informačnej bezpečnosti (CISO)

4.1.1 Zodpovedá za túto politiku a zabezpečuje jej súlad s celkovým systémom manažérstva informačnej bezpečnosti (ISMS), stratégiou riadenia rizík a požiadavkami na súlad.

4.1.2 Schvaľuje klasifikačné úrovne dodávateľov, výsledky bezpečnostných preskúmaní a výnimky s vysokým rizikom.

4.1.3 Zúčastňuje sa na eskalácii závažných incidentov dodávateľov a na rokovaniach o zmluvách pre kritické služby.

4.2 útvar obstarávania a riadenia dodávateľov

4.2.1 Zabezpečuje, aby všetky nové a obnovené zmluvy s dodávateľmi obsahovali schválené ustanovenia týkajúce sa bezpečnosti a ochrany údajov.

4.2.2 Vedie centralizovaný register dodávateľov a koordinuje sa s útvarom právnych záležitostí a súladu pri dokumentovaní rizík tretích strán.

4.2.3 Iniciuje procesy nástupu a zabezpečuje vykonanie bezpečnostných posúdení pred uzatvorením zmluvy.

[... 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 Táto politika sa musí preskúmavať minimálne raz ročne alebo skôr v prípade:

9.1.1 významných zmien v stratégii obstarávania alebo ekosystéme dodávateľov,

9.1.2 aktualizácií právnych alebo regulačných rámcov (napr. DORA, GDPR),

9.1.3 závažných incidentov tretích strán, porušenia ochrany údajov alebo zlyhaní auditu,

9.1.4 zistení z posúdení rizík alebo od externých certifikačných orgánov.

9.2 Za proces preskúmania spoločne zodpovedajú funkcie CISO, obstarávania, právneho oddelenia a riadenia rizík.

9.3 Všetky revízie politiky musia byť zdokumentované v registri riadenia dokumentácie ISMS, podliehať riadeniu verzií a byť oznámené príslušným zainteresovaným stranám prostredníctvom kanálov správy a riadenia dodávateľov a programov zvyšovania povedomia zamestnancov.

9.4 Nahradené verzie musia byť archivované minimálne tri roky na účely sledovateľnosti a právneho súladu.

10. Súvisiace politiky a väzby

10.1 P1 – Politika informačnej bezpečnosti. Stanovuje celkový záväzok zabezpečiť všetky činnosti organizácie vrátane závislostí od dodávateľov tretích strán a externých poskytovateľov služieb.

10.2 P6 – Politika riadenia rizík. Usmerňuje identifikáciu rizík, posúdenie rizík a zmierňovanie rizík spojených so vzťahmi s tretími stranami vrátane prenesených alebo systémových rizík vyplývajúcich z ekosystémov dodávateľov.

10.3 P17 – Politika ochrany údajov a súkromia. Vzťahuje sa na všetkých dodávateľov, ktorí nakladajú s osobnými údajmi, a vyžaduje primerané zmluvné podmienky, ochranné opatrenia pri prenose a zásady ochrany súkromia už pri návrhu.

10.4 P4 – Politika riadenia prístupu. Upravuje spôsob, akým personál tretích strán získava prístup do systémov organizácie, pričom uplatňuje oprávnenia na základe rolí, riadenie relácií a postupy odoberania prístupových oprávnení.

10.5 P22 – Politika logovania a monitorovania. Vyžaduje, aby bol prístup dodávateľov do systémov monitorovaný, zaznamenávaný a preskúmavaný, najmä v prostrediach s privilegovanými aktivitami alebo aktivitami zameranými na údaje.

10.6 P30 – Politika reakcie na incidenty (P30). Definuje eskalačné postupy a požiadavky na hlásenie porušení pri bezpečnostných udalostiach pochádzajúcich od dodávateľov alebo pri spoločných vyšetrovaniach zahŕňajúcich systémy tretích strán.

11. Referenčné normy a rámce

11.1 ISO/IEC 27001: Kapitola 8.1 – Prevádzkové plánovanie a riadenie: vyžaduje formálne kontroly nad službami tretích strán, ktoré majú vplyv na ISMS.

11.2 ISO/IEC 27002:2022 – Kontroly 5.19 až 5.22:

11.2.1 Príloha A, kontrola 5.19 – Politiky a postupy pre vzťahy s dodávateľmi: vyžaduje kontroly na riadenie interakcií s dodávateľmi.

11.2.2 Príloha A, kontrola 5.20 – Riadenie rizík dodávateľov: zameriava sa na identifikáciu, posúdenie a priebežný dohľad nad bezpečnostným stavom dodávateľov.

11.2.3 Príloha A, kontrola 5.21 – Riadenie poskytovania služieb dodávateľmi: vyžaduje zosúladenie výkonnosti a bezpečnosti so zmluvnými očakávaniami.

11.2.4 Príloha A, kontrola 5.22 – Monitorovanie a preskúmavanie dodávateľov: zdôrazňuje potrebu priebežného overovania a prehodnocovania súladu tretích strán.

11.3 NIST SP 800-53 Rev. 5:

11.3.1 SA-9 – Služby externých systémov: definuje bezpečnostné a rizikové požiadavky pre systémy prevádzkované externými subjektmi.

11.3.2 SA-10 – Riadenie konfigurácie vývojárom: uplatňuje sa, keď tretie strany dodávajú softvér alebo prostredia.

11.3.3 CA-3 – Prepojenia systémov: vyžaduje dohľad a dohodu o tokoch údajov medzi systémami jednotlivých subjektov.

11.3.4 PS-7 – Personálna bezpečnosť tretích strán: zabezpečuje, aby zmluvní pracovníci a personál dodávateľov boli primerane preverovaní a monitorovaní.

11.4 GDPR EÚ (2016/679):

11.4.1 Článok 28 – Povinnosti sprostredkovateľa: vyžaduje písomné dohody so sprostredkovateľmi vrátane technických a organizačných opatrení (TOM).

11.4.2 Článok 32 – Bezpečnosť spracúvania: ukladá povinnosť primeraných ochranných opatrení prevádzkovateľom aj sprostredkovateľom.

11.4.3 Článok 33 – Oznamovanie porušenia ochrany osobných údajov: vyžaduje promptné oznámenie od dodávateľov v prípade porušenia ochrany údajov.

11.5 Smernica EÚ NIS2 (2022/2555):

11.5.1 Článok 21(2)(e–f): vyžaduje riadenie dodávateľov založené na riziku a bezpečnostný dohľad, najmä v digitálnych dodávateľských reťazcoch základných a dôležitých subjektov.

11.6 Nariadenie EÚ DORA (2022/2554):

11.6.1 Článok 28 – riziko IKT tretích strán: ukladá povinnosti týkajúce sa posúdenia rizík, zmluvných bezpečnostných podmienok a stratégií ukončenia pre poskytovateľov finančných služieb.

11.6.2 Článok 30 – dohľad nad kritickými externými poskytovateľmi IKT: zavádza rozšírené očakávania monitorovania a dohľadu pre kľúčových dodávateľov.

11.7 COBIT 2019:

11.7.1 BAI05 – Riadenie zavádzania organizačných zmien: zabezpečuje, aby prechody medzi dodávateľmi boli riadené bezpečným spôsobom.

11.7.2 DSS02 – Riadenie požiadaviek na služby a incidentov: uplatňuje sa na problémy hlásené dodávateľmi a integráciu riešenia incidentov.

11.7.3 MEA03 – Monitorovanie, hodnotenie a posudzovanie súladu: posilňuje meranie výkonnosti dodávateľov a monitorovanie súladu.