					Sem vložte název registrované právnické osoby							
Číslo dokumentu: P26					Název dokumentu: **Politika bezpečnosti třetích stran a dodavatelů**							
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 plánování a řízení: Vyžaduje formální opatření pro služby třetích stran, které mají dopad na systém řízení bezpečnosti informací (ISMS)
ISO/IEC 27002:2022	Opatření 5.19–5.22	politiky a postupy pro vztahy s dodavateli; řízení rizik dodavatelů; řízení poskytování služeb dodavateli; monitorování a přezkum dodavatelů
NIST SP 800-53 Rev.5	SA-9, SA-10, CA-3, PS-7	služby externích systémů; řízení konfigurace ze strany vývojáře; propojení systémů; bezpečnost personálu třetích stran
GDPR	Články 28, 32, 33	povinnosti zpracovatele; zabezpečení zpracování; oznámení porušení zabezpečení osobních údajů
směrnice NIS2	Článek 21(2)(e–f)	řízení dodavatelů založené na riziku a dohled nad bezpečností
nařízení DORA	Články 28, 30	rizika ICT třetích stran; dohled nad kritickými poskytovateli ICT služeb třetích stran
COBIT 2019	BAI05, DSS02, MEA03	řídit umožnění organizační změny; řídit požadavky na služby a incidenty; monitorovat, vyhodnocovat a posuzovat soulad

1. Účel

1.1 Tato politika stanoví požadavky na bezpečnost informací pro navazování, řízení a udržování bezpečných vztahů s dodavateli a poskytovateli služeb třetích stran.

1.2 Zajišťuje, aby všichni dodavatelé s přístupem k datům, systémům nebo infrastruktuře organizace podléhali přísným bezpečnostním opatřením, smluvním zárukám a průběžnému dohledu po celý životní cyklus služby.

1.3 Tato politika podporuje opatření 5.19 až 5.22 přílohy A normy ISO/IEC 27001 tím, že začleňuje bezpečnostní požadavky do procesů nákupu, onboardingu, náležité péče, řízení smluv, monitorování služeb a ukončení spolupráce.

2. Rozsah

2.1 Tato politika se vztahuje na:

2.1.1 všechny dodavatele třetích stran, smluvní pracovníky, poskytovatele cloudových služeb a servisní organizace, které zpracovávají informační aktiva organizace nebo k nim přistupují,

2.1.2 všechny interní role zapojené do hodnocení dodavatelů, onboardingu, uzavírání smluv, řízení rizik, monitorování nebo ukončení spolupráce,

2.1.3 všechny vztahy s dodavateli, které zahrnují přístup k citlivým datům, integraci s produkčními službami nebo podporu funkcí kritických pro podnikání.

2.2 Zahrnuje jak přímé dodavatele, tak jejich dílčí zpracovatele nebo subdodavatele, je-li to relevantní, a vztahuje se na software třetích stran, infrastrukturu, podporu i outsourcované služby.

3. Cíle

3.1 Zajistit, aby byla bezpečnostní rizika dodavatelů v průběhu celého životního cyklu vztahu konzistentně identifikována, posuzována a zmírňována.

3.2 Začlenit standardizované bezpečnostní požadavky do všech smluv s dodavateli, včetně oznamovacích povinností při porušení zabezpečení, smluvních ustanovení o právu auditu a odpovědností v oblasti ochrany dat.

3.3 Vyžadovat formální náležitou péči a dokumentovaná hodnocení rizik před zapojením nových dodavatelů nebo obnovením smluv o službách s vysokým rizikem.

3.4 Zavést mechanismy pro průběžné monitorování souladu dodavatelů, včetně hodnocení výkonnosti, auditů a eskalace incidentů.

3.5 Řídit změny dodavatelských služeb a zajistit bezpečný offboarding a vrácení nebo zničení dat při ukončení spolupráce.

3.6 Uvést bezpečnostní opatření třetích stran do souladu s příslušnými regulatorními požadavky a smluvními povinnostmi, včetně GDPR, směrnice NIS2, nařízení DORA a normy ISO/IEC 27001.

4. Role a odpovědnosti

4.1 ředitel informační bezpečnosti (CISO)

4.1.1 Odpovídá za tuto politiku a zajišťuje její soulad s celkovou strategií ISMS, řízením rizik a zajištěním souladu.

4.1.2 Schvaluje klasifikační stupně dodavatelů, výsledky bezpečnostních přezkumů a výjimky s vysokým rizikem.

4.1.3 Účastní se eskalace závažných incidentů dodavatelů a jednání o smlouvách pro kritické služby.

4.2 nákup a řízení dodavatelů

4.2.1 Zajišťuje, aby všechny nové i obnovované smlouvy s dodavateli obsahovaly schválená bezpečnostní ustanovení a ustanovení o ochraně dat.

4.2.2 Udržuje centralizovaný registr dodavatelů a koordinuje činnost s útvarem Právní a compliance při vedení dokumentace rizik třetích stran.

4.2.3 Zahajuje procesy onboardingu a zajišťuje jejich soulad s bezpečnostními posouzeními před uzavřením smlouvy.

[... 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 přezkoumána nejméně jednou ročně nebo dříve v případě:

9.1.1 významných změn ve strategii nákupu nebo ekosystému dodavatelů,

9.1.2 aktualizací právních nebo regulatorních rámců (např. nařízení DORA, GDPR),

9.1.3 závažných incidentů třetích stran, porušení zabezpečení dat nebo selhání auditu,

9.1.4 zjištění z hodnocení rizik nebo od externích certifikačních orgánů.

9.2 Za proces přezkumu společně odpovídají funkce CISO, nákup, Právní a řízení rizik.

9.3 Všechny změny politiky musí být zdokumentovány v registru řízení dokumentace ISMS, vedeny v režimu správy verzí a sděleny příslušným zainteresovaným stranám prostřednictvím kanálů řízení dodavatelů a programů bezpečnostního povědomí zaměstnanců.

9.4 Nahrazené verze musí být archivovány po dobu nejméně tří let pro účely dohledatelnosti a souladu s právními požadavky.

10. Související politiky a vazby

10.1 P1 – Politika informační bezpečnosti. Stanoví zastřešující závazek bezpečně zajišťovat všechny činnosti organizace, včetně závislosti na dodavatelích třetích stran a externích poskytovatelích služeb.

10.2 P6 – Politika řízení rizik. Upravuje identifikaci, hodnocení a zmírňování rizik spojených se vztahy s třetími stranami, včetně zděděných nebo systémových rizik vyplývajících z ekosystémů dodavatelů.

10.3 P17 – Politika ochrany dat a soukromí. Vztahuje se na všechny dodavatele, kteří nakládají s osobními údaji, a vyžaduje odpovídající smluvní podmínky, záruky při přenosu a zásady ochrany osobních údajů již od návrhu.

10.4 P4 – Politika řízení přístupu. Upravuje, jak personál třetích stran získává přístup k systémům organizace, a vynucuje oprávnění podle rolí, řízení relací a postupy odebrání přístupu.

10.5 P22 – Politika protokolování a monitorování. Vyžaduje, aby byl přístup dodavatelů k systémům monitorován, protokolován a přezkoumáván, zejména v prostředích, kde dochází k privilegovaným činnostem nebo činnostem zaměřeným na data.

10.6 P30 – Politika reakce na incidenty. Vymezuje eskalační postupy a požadavky na hlášení porušení zabezpečení pro bezpečnostní události pocházející od dodavatelů nebo společná vyšetřování zahrnující systémy třetích stran.

11. Referenční normy a rámce

11.1 ISO/IEC 27001: Kapitola 8.1 – provozní plánování a řízení: Vyžaduje formální opatření pro služby třetích stran, které mají dopad na ISMS.

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

11.2.1 Opatření 5.19 přílohy A – politiky a postupy pro vztahy s dodavateli: Ukládá zavedení opatření pro řízení interakcí s dodavateli.

11.2.2 Opatření 5.20 přílohy A – řízení rizik dodavatelů: Zaměřuje se na identifikaci, hodnocení a průběžný dohled nad bezpečnostním stavem dodavatelů.

11.2.3 Opatření 5.21 přílohy A – řízení poskytování služeb dodavateli: Vyžaduje soulad výkonnosti a bezpečnosti se smluvními očekáváními.

11.2.4 Opatření 5.22 přílohy A – monitorování a přezkum dodavatelů: Zdůrazňuje potřebu průběžného ověřování a opětovného posuzování souladu třetích stran.

11.3 NIST SP 800-53 Rev.5:

11.3.1 SA-9 – služby externích systémů: Vymezuje požadavky na bezpečnost a rizika systémů provozovaných externími subjekty.

11.3.2 SA-10 – řízení konfigurace ze strany vývojáře: Uplatní se, pokud třetí strany dodávají software nebo prostředí.

11.3.3 CA-3 – propojení systémů: Vyžaduje dohled a dohodu o tocích dat mezi systémy jednotlivých subjektů.

11.3.4 PS-7 – bezpečnost personálu třetích stran: Zajišťuje, aby smluvní pracovníci a personál dodavatelů byli přiměřeně prověřováni a monitorováni.

11.4 GDPR (2016/679):

11.4.1 Článek 28 – povinnosti zpracovatele: Vyžaduje písemné dohody se zpracovateli osobních údajů, včetně technických a organizačních opatření (TOM).

11.4.2 Článek 32 – zabezpečení zpracování: Ukládá správcům i zpracovatelům povinnost zavést přiměřená ochranná opatření.

11.4.3 Článek 33 – oznámení porušení zabezpečení osobních údajů: Vyžaduje v případě porušení zabezpečení včasné oznámení ze strany dodavatelů.

11.5 směrnice NIS2 (2022/2555):

11.5.1 Článek 21(2)(e–f): Vyžaduje řízení dodavatelů založené na riziku a dohled nad bezpečností, zejména v digitálních dodavatelských řetězcích základních a důležitých subjektů.

11.6 nařízení DORA (2022/2554):

11.6.1 Článek 28 – rizika ICT třetích stran: Ukládá poskytovatelům finančních služeb povinnosti týkající se hodnocení rizik, smluvních bezpečnostních podmínek a strategií ukončení.

11.6.2 Článek 30 – dohled nad kritickými poskytovateli ICT služeb třetích stran: Stanoví zvýšené požadavky na monitorování a dohled nad klíčovými dodavateli.

11.7 COBIT 2019:

11.7.1 BAI05 – řídit umožnění organizační změny: Zajišťuje, aby přechody mezi dodavateli byly řízeny bezpečným způsobem.

11.7.2 DSS02 – řídit požadavky na služby a incidenty: Vztahuje se na problémy hlášené dodavateli a integraci zvládání incidentů.

11.7.3 MEA03 – monitorovat, vyhodnocovat a posuzovat soulad: Posiluje měření výkonnosti dodavatelů a monitorování souladu.