					Sem vložte název registrované právnické osoby							
Číslo dokumentu: P41					Název dokumentu: **Politika řízení rizik závislostí na dodavatelích**							
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	6.1.3, 8.1, 9.1	
ISO/IEC 27002:2022	5.20, 5.21, 5.22, 5.23, 5.30	
NIST SP 800-53 Rev.5	SR-2, SR-3, SR-5, SR-6, SR-11, RA-3	
GDPR	čl. 28, čl. 32 odst. 1 písm. d)	
směrnice NIS2	čl. 21 odst. 2 písm. d), čl. 21 odst. 3, čl. 22	
nařízení DORA	čl. 28–30	
COBIT 2019	APO10.01, APO10.02, APO10.03, APO10.04, DSS04.07, MEA02.03	

1. Účel

1.1 Posílit zabezpečení dodavatelského řetězce organizace zavedením procesu pro identifikaci a řízení kritických závislostí na dodavatelích a poskytovatelích služeb v návaznosti na čl. 21 odst. 3 směrnice NIS2 a hodnocení rizik dodavatelského řetězce na úrovni Unie.

1.2 Zajistit, aby rizika vyplývající z koncentrace nebo závislosti na jednotlivých dodavatelích byla pochopena a zmírňována a aby byla veškerá odvětvově specifická rizika dodavatelského řetězce, na která upozorňují příslušné orgány podle čl. 22 směrnice NIS2, zahrnuta do našeho řízení rizik a plánování kontinuity činností.

2. Rozsah

2.1 Tato politika se vztahuje na všechny klíčové dodavatele a poskytovatele služeb, na nichž je organizace závislá při zajišťování kritických činností, zejména v ICT dodavatelském řetězci (hardware, software, cloudové služby, telekomunikační služby, řízené služby).

2.2 Zahrnuje interní funkce, včetně nákupu, řízení dodavatelů, řízení rizik a příslušných provozních útvarů. V rozsahu nezbytném pro získávání informací o rizicích se vztahuje také na samotné dodavatele. „Kritičtí dodavatelé“ jsou ti, jejichž selhání nebo kompromitace by mohly významně ovlivnit naši schopnost poskytovat služby nebo plnit právní povinnosti.

3. Cíle

3.1 Získat přehled o závislostech v dodavatelském řetězci, zejména identifikovat jednotlivé body selhání nebo vysoké riziko koncentrace v naší dodavatelské základně (např. závislost na jednom poskytovateli cloudových služeb pro všechny služby).

3.2 Zavést opatření ke snižování a řízení rizik souvisejících s dodavateli, jako je diverzifikace, plány pro mimořádné situace nebo požadavek na posílení opatření u dodavatelů, a tím zvýšit odolnost vůči selhání dodavatelů nebo útokům vycházejícím z dodavatelského řetězce.

3.3 Zajistit soulad s požadavky směrnice NIS2 začleněním výsledků koordinovaných hodnocení bezpečnostních rizik kritických dodavatelských řetězců podle čl. 22 do rozhodování organizace v oblasti rizik a současně zajistit, aby náš přístup k řízení rizik dodavatelského řetězce byl zdokumentován a doložitelný.

4. Role a odpovědnosti

4.1 Útvar řízení dodavatelů (VMO): Odpovídá za registr závislostí na dodavatelích a koordinuje hodnocení rizik. Zajišťuje, aby byl každý klíčový dodavatel posouzen z hlediska kritičnosti a úrovně závislosti při zahájení spolupráce a následně v pravidelných intervalech.

4.2 Řízení rizik (výbor pro podniková rizika): Přezkoumává riziko koncentrace a analýzy závislostí, schvaluje strategie ošetření rizik (např. schválení zařazení alternativního dodavatele nebo držení vyšších zásob kritických komponent). Zahrnuje rizika dodavatelského řetězce do registru rizik a podává zprávy vrcholovému vedení.

[... Oddíly 4.3–8 nejsou součástí tohoto náhledu. Pro přístup k úplnému obsahu zakupte celý dokument. ...]

9. Monitorování a audit

9.1 Registr závislostí a hodnocení rizik budou každoročně předmětem interního auditu. Interní audit ověří, že jsou všichni kritičtí dodavatelé evidováni, jejich hodnocení rizik je aktuální a plány zmírnění rizik jsou zavedeny a plněny podle plánu. Současně prověří, že byly řádně zohledněny externí vstupy z hodnocení rizik (zprávy podle čl. 22 apod.).

9.2 Účinnost diverzifikačních opatření a opatření pro mimořádné situace bude pravidelně testována. Může být například provedena plánovaná simulace, při níž se předpokládá selhání významného dodavatele, s cílem otestovat naše plány kontinuity činností a alternativní řešení (obdobně jako cvičení DR, ale pro výpadek dodavatele). Výsledky těchto testů musí být dokumentovány a případné nedostatky odstraněny.

9.3 Metriky: Útvar řízení rizik bude sledovat metriky, jako je „% kritických služeb, pro které je k dispozici alespoň jeden alternativní dodavatel nebo řešení“ nebo „5 nejvýznamnějších závislostí na dodavatelích a jejich trend rizika“. Tyto metriky budou zahrnuty do řídicího panelu rizik pro vedení. Klesající trend rizika závislosti v čase je cílem; pokud metriky ukazují rostoucí závislost, musí to být projednáno vedením.

10. Přezkum a údržba

10.1 Tato politika bude nejméně jednou ročně přezkoumána útvarem řízení dodavatelů a útvarem řízení rizik. Přezkum zohlední všechny změny v prostředí dodavatelů (např. pokud se nový dodavatel stane kritickým nebo je původní dodavatel postupně vyřazen) a jakékoli nové regulační požadavky týkající se outsourcingu nebo rizik třetích stran.

10.2 Pokud odvětvové orgány vydají aktualizované pokyny nebo pokud incident odhalí mezery v kontrolách (například pokud měl výpadek dodavatele větší dopad, než se předpokládalo, což znamená, že naše hodnocení rizik nesprávně posoudilo závislost), politika bude aktualizována za účelem zpřesnění kritérií nebo strategií zmírnění rizik.

10.3 Revidované verze politiky musí schválit vrcholové vedení. Významné změny budou oznámeny všem příslušným útvarům a školicí materiály budou odpovídajícím způsobem aktualizovány tak, aby odrážely nové postupy nebo standardy.

11. Související politiky a vazby

11.1 P01 – P01 Politika informační bezpečnosti. Stanovuje odpovědnost za správu a řízení závislostí na dodavatelích.

11.2 P02 – Politika rolí a odpovědností v oblasti správy a řízení. Upřesňuje vlastnictví rozhodnutí o rizicích souvisejících s dodavateli.

11.3 P06 – Politika řízení rizik. Začleňuje riziko koncentrace do podnikových registrů rizik.

11.4 P26 – Bezpečnostní politika dodavatelů a poskytovatelů služeb třetích stran. Stanovuje základní bezpečnostní opatření; P41 doplňuje opatření pro závislost a koncentraci.

11.5 P27 – Politika používání cloudových služeb. Uplatňuje kritéria závislosti na zavádění cloudových služeb a plány ukončení.

11.6 P28 – Politika outsourcovaného vývoje. Pokrývá rizika závislosti v externím vývoji.

11.7 P32 – Politika kontinuity činností a obnovy po havárii. Plánuje scénáře výpadku nebo náhrady dodavatele.

11.8 P37 – Politika právního a regulačního souladu. Zajišťuje, aby smlouvy a povinnosti odrážely opatření pro řízení závislostí.

12. Reference

12.1 směrnice NIS2 (EU 2022/2555), čl. 21 odst. 3 (vyžadující zohlednění zranitelností specifických pro každého přímého dodavatele/poskytovatele služeb a kvality jejich kybernetické bezpečnosti, včetně výsledků koordinovaných hodnocení rizik dodavatelského řetězce)

12.2 směrnice NIS2, čl. 22 odst. 1 (koordinovaná hodnocení bezpečnostních rizik kritických dodavatelských řetězců na úrovni Unie – informují subjekty o odvětvových rizicích souvisejících s dodavateli)

12.3 prováděcí nařízení Komise (EU) 2024/2690, příloha oddíl 5 (požadavky na bezpečnost dodavatelského řetězce pro subjekty, včetně kritérií pro výběr dodavatelů, diverzifikaci a smluvní povinnosti)

12.4 osvědčené postupy ENISA pro kybernetickou bezpečnost dodavatelského řetězce (2022) – doporučení pro identifikaci kritických dodavatelů a řízení souvisejících rizik

12.5 ISO/IEC 27001:2022 / ISO/IEC 27002:2022