					Sem vložte název registrované právnické osoby							
Číslo dokumentu: P30					Název dokumentu: **Politika reakce na incidenty**							
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 8.1, Kapitola 9	Strukturované procesy pro řízení rizik a reakci na incidenty
ISO/IEC 27002:2022	Opatření 5.25–5.27	Role, hlášení, reakce a zlepšování v oblasti incidentů
NIST SP 800-53 Rev.5	IR-1 až IR-9	Komplexní životní cyklus reakce na incidenty
GDPR	Článek 33(1), 33(3)(a)–(d), 34(1), 34(2)(a)–(c)	Lhůty pro oznamování porušení zabezpečení, hlášení a komunikace vůči subjektům údajů
směrnice NIS2	Článek 23(1)–(4)	Oznamování vnitrostátním orgánům a strukturované hlášení
nařízení DORA	Článek 17(1)–(3)	Hlášení závažných incidentů souvisejících s ICT pro finanční subjekty
COBIT 2019	DSS02, DSS04, MEA	Definuje, monitoruje a posuzuje řízení incidentů, kontinuitu činností a vyhodnocování

1. Účel

1.1 Tato politika stanoví formální rámec pro identifikaci, hlášení, analýzu, omezení dopadů, reakci, obnovu a přezkoumání po incidentu v oblasti bezpečnostních incidentů informací, které mají dopad na organizaci.

1.2 Zajišťuje včasnou, koordinovanou a účinnou reakci s cílem minimalizovat provozní narušení, finanční ztráty, poškození dobré pověsti a nesoulad s právními předpisy.

1.3 Politika dále podporuje průběžné zlepšování postoje organizace ke kybernetické odolnosti a riziku prostřednictvím získaných poznatků a začlenění zjištění z přezkoumání po incidentu do správy a řízení, nástrojů a vzdělávacích programů.

2. Rozsah

2.1 Tato politika se vztahuje na:

2.1.1 veškerý personál, včetně zaměstnanců, dodavatelů, konzultantů a externích poskytovatelů služeb

2.1.2 všechny informační systémy, aplikace, infrastrukturu, sítě a data bez ohledu na to, zda jsou provozovány on-premise, v cloudu nebo v hybridním režimu

2.1.3 všechny typy bezpečnostních incidentů, mimo jiné včetně:

2.1.3.1 neoprávněného přístupu nebo eskalace oprávnění

2.1.3.2 útoků škodlivým kódem a ransomwarem

2.1.3.3 útoků typu odmítnutí služby (DoS/DDoS)

2.1.3.4 ztráty dat, úniku dat nebo exfiltrace dat

2.1.3.5 zneužití ze strany interních osob nebo porušení politiky

2.1.3.6 narušení fyzické bezpečnosti s dopadem na digitální aktiva

2.2 Tato politika zahrnuje detekci, triáž, vyšetřování, eskalaci, omezení dopadů, nakládání s důkazy, oznamování, obnovu a analýzu kořenové příčiny.

3. Cíle

3.1 Zavést opakovatelnou a škálovatelnou schopnost reakce na incidenty, která umožní rychlou detekci, klasifikaci a zmírňování bezpečnostních incidentů.

3.2 Minimalizovat dopad bezpečnostních událostí na obchodní činnost prostřednictvím strukturovaných postupů pro omezení dopadů, odstranění hrozby a obnovu systémů.

3.3 Zajistit, aby hlášení incidentů a reakce na ně byly v souladu s právními, regulačními a smluvními požadavky, zejména pokud jde o lhůty pro oznamování porušení zabezpečení a nakládání s důkazy.

3.4 Podporovat transparentnost a odpovědnost prostřednictvím řádného protokolování, dokumentace a sledování metrik u všech bezpečnostních incidentů.

3.5 Podporovat průběžné zlepšování prostřednictvím přezkoumání po incidentu, nápravných opatření a školení zainteresovaných stran.

4. Role a odpovědnosti

4.1 ředitel informační bezpečnosti (CISO)

4.1.1 Odpovídá za rámec reakce na incidenty, zajišťuje uplatňování této politiky a vykonává dohled nad koordinací incidentů v celé organizaci.

4.1.2 Působí jako hlavní kontaktní osoba pro regulační orgány, vrcholové vedení a externí právní poradce při závažných incidentech.

4.2 Koordinátor reakce na incidenty

4.2.1 Koordinuje meziútvarové týmy reakce na incidenty, řídí pracovní postupy a sleduje stav omezení dopadů a obnovy.

4.2.2 Zahajuje a vede přezkoumání po incidentu (PIR) a zajišťuje, aby byla nápravná opatření zaznamenána a realizována.

[... 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 přezkoumávána nejméně jednou ročně a podle potřeby aktualizována tak, aby zahrnovala:

9.1.1 změny v prostředí hrozeb, typech incidentů nebo vektorech útoku

9.1.2 poznatky získané ze závažných incidentů, incidentů, ke kterým málem došlo, nebo regulačních zjištění

9.1.3 aktualizace příslušných právních a regulačních požadavků (např. GDPR, DORA, NIS2)

9.1.4 zpětnou vazbu z cvičení reakce na incidenty a z přezkoumání po incidentu

9.2 CISO odpovídá za zahájení a koordinaci procesu přezkumu po konzultaci s:

9.2.1.1 právním poradcem a DPO

9.2.1.2 SOC a IT provozem

9.2.1.3 týmy kontinuity činností a řízení rizik

9.2.1.4 vrcholovým vedením

9.3 Změny politiky musí být:

9.3.1 zdokumentovány v repozitáři se správou verzí

9.3.2 komunikovány všem dotčeným týmům a promítnuty do školení bezpečnostního povědomí

9.3.3 ověřeny prostřednictvím stolních nebo praktických cvičení reakce na incidenty do tří měsíců od schválení

9.4 Naléhavé aktualizace vyvolané nově vznikajícími hrozbami, zjištěními auditu nebo nově vydanými právními povinnostmi musí být zavedeny neprodleně a zaznamenány v historii změn politiky.

10. Související politiky a vazby

10.1 Tato politika je podporována následujícími organizačními politikami a je na nich závislá:

10.1.1 P1 – Politika informační bezpečnosti: Stanoví zastřešující požadavek na provoz založený na rizicích a připravenost na incidenty.

10.1.2 P5 – Politika řízení změn: Zajišťuje, aby činnosti omezení dopadů a obnovy zahrnující infrastrukturu nebo služby probíhaly podle formálních postupů.

10.1.3 P13 – Politika klasifikace dat a označování: Podporuje klasifikaci závažnosti incidentů podle citlivosti dat.

10.1.4 P15 – Politika zálohování a obnovy: Umožňuje obnovu po ransomwaru nebo destruktivních útocích při zachování integrity.

10.1.5 P18 – Politika kryptografických opatření: Definuje opatření šifrování, která snižují dopad incidentu a rizika expozice dat.

10.1.6 P22 – Politika protokolování a monitorování: Poskytuje základní viditelnost událostí, upozorňování a uchovávání logů potřebné pro účinnou detekci a forenzní šetření.

10.1.7 P29 – Politika testovacích dat a testovacího prostředí: Zajišťuje, aby incidenty ovlivňující i neprodukční systémy byly řešeny strukturovaně a bezpečně.

10.1.8 P33 – Politika monitorování auditu a souladu: Ověřuje připravenost na incidenty a účinnost reakce prostřednictvím strukturovaných auditů a hodnocení souladu.

11. Referenční normy a rámce

11.1 ISO/IEC 27001: Kapitola 8.1 – Operativní plánování a řízení: Strukturované procesy pro řízení rizik a plánování reakce na incidenty.

11.2 ISO/IEC 27002:2022 – Opatření 5.25–5.27: Odpovědnosti za řízení incidentů, hlášení, reakci, komunikaci a zlepšování.

11.3 NIST SP 800-53 Rev.5: IR-1 až IR-9, AU-6, PL-2: Komplexní požadavky na životní cyklus reakce na incidenty, audit a plánování bezpečnosti.

11.4 GDPR: Článek 33/34: oznamovací povinnosti vůči dozorovým úřadům a požadavky na informování subjektů údajů (s vymezenými výjimkami).

11.5 směrnice EU NIS2 (2022/2555): Článek 23: povinné vnitrostátní hlášení včetně průběžných a závěrečných oznamovacích povinností.

11.6 nařízení EU DORA (2022/2554): Článek 17: požadavky na hlášení ICT incidentů orgánům ze strany finančních institucí.

11.7 COBIT 2019: DSS02, DSS04, MEA01: Řízení servisních incidentů a kontinuity činností a dále monitorování výkonnosti a souladu.