					Sem zadajte názov registrovanej právnickej osoby							
Číslo dokumentu: P30					Názov dokumentu: **Politika reakcie na incidenty**							
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 predpismi

Norma/predpis	Kapitola/článok	Poznámka
ISO/IEC 27001:2022	Kapitola 8.1, Kapitola 9	Štruktúrované procesy riadenia rizík a reakcie na incidenty
ISO/IEC 27002:2022	Kontroly 5.25–5.27	Roly, nahlasovanie, reakcia a zlepšovanie pri incidentoch
NIST SP 800-53 Rev.5	IR-1 až IR-9	Komplexný životný cyklus reakcie na incidenty
Nariadenie EÚ GDPR	Článok 33(1), 33(3)(a)–(d), 34(1), 34(2)(a)–(c)	Lehoty na oznámenie porušenia ochrany osobných údajov, nahlasovanie a komunikácia s dotknutými osobami
Smernica EÚ NIS2	Článok 23(1)–(4)	Oznámenie vnútroštátnemu orgánu a štruktúrované nahlasovanie
Nariadenie EÚ DORA	Článok 17(1)–(3)	Nahlasovanie závažných incidentov súvisiacich s IKT pre finančné subjekty
COBIT 2019	DSS02, DSS04, MEA	Definuje, monitoruje a posudzuje riadenie incidentov, kontinuitu činností a hodnotenie

1. Účel

1.1 Táto politika stanovuje formálny rámec na identifikáciu, nahlasovanie, analýzu, zamedzenie šírenia, reakciu, obnovu a poincidentné vyhodnotenie bezpečnostných incidentov informačnej bezpečnosti, ktoré majú vplyv na organizáciu.

1.2 Zabezpečuje včasnú, koordinovanú a účinnú reakciu s cieľom minimalizovať prevádzkové narušenie, finančné straty, reputačnú ujmu a regulačný nesúlad.

1.3 Politika zároveň podporuje nepretržité zlepšovanie odolnosti organizácie voči kybernetickým hrozbám prostredníctvom získaných poznatkov a integrácie poincidentných zistení do správy a riadenia, nástrojov a školiacich programov.

2. Rozsah

2.1 Táto politika sa vzťahuje na:

2.1.1 všetkých pracovníkov vrátane zamestnancov, zmluvných pracovníkov, konzultantov a poskytovateľov služieb tretích strán,

2.1.2 všetky informačné systémy, aplikácie, infraštruktúru, siete a údaje bez ohľadu na to, či sú prevádzkované on-premises, v cloudovom prostredí alebo v hybridnom režime,

2.1.3 všetky typy bezpečnostných incidentov vrátane okrem iného:

2.1.3.1 neoprávneného prístupu alebo eskalácie oprávnení,

2.1.3.2 útokov malvérom a ransomvérom,

2.1.3.3 útokov typu odmietnutie služby (DoS/DDoS),

2.1.3.4 straty údajov, úniku údajov alebo exfiltrácie údajov,

2.1.3.5 vnútorného zneužitia alebo porušenia politík,

2.1.3.6 narušenia fyzickej bezpečnosti s dopadom na digitálne aktíva.

2.2 Politika zahŕňa detekciu, triáž, vyšetrovanie, eskaláciu, zamedzenie šírenia, nakladanie s dôkazmi, oznamovanie, obnovu a analýzu hlavnej príčiny.

3. Ciele

3.1 Zaviesť opakovateľnú a škálovateľnú schopnosť reakcie na incidenty, ktorá umožní rýchlu detekciu, klasifikáciu a zmierňovanie bezpečnostných incidentov.

3.2 Minimalizovať dopad bezpečnostných udalostí na organizáciu prostredníctvom štruktúrovaných postupov zamedzenia šírenia, odstránenia a obnovy systémov.

3.3 Zabezpečiť, aby nahlasovanie incidentov a reakcia na ne boli v súlade so zákonnými, regulačnými a zmluvnými požiadavkami, najmä s požiadavkami týkajúcimi sa lehôt na oznamovanie porušenia ochrany osobných údajov a nakladania s dôkazmi.

3.4 Podporiť transparentnosť a zodpovednosť prostredníctvom riadneho logovania, dokumentovania a sledovania metrík pre všetky bezpečnostné incidenty.

3.5 Podporovať nepretržité zlepšovanie prostredníctvom poincidentných revízií, nápravných opatrení a školení zainteresovaných strán.

4. Roly a zodpovednosti

4.1 riaditeľ informačnej bezpečnosti (CISO)

4.1.1 Zodpovedá za rámec reakcie na incidenty, zabezpečuje uplatňovanie tejto politiky a vykonáva dohľad nad koordináciou incidentov v celej organizácii.

4.1.2 Počas závažných incidentov pôsobí ako hlavný kontaktný bod pre regulátorov, vrcholový manažment a externých právnych poradcov.

4.2 koordinátor reakcie na incidenty

4.2.1 Koordinuje medzifunkčné tímy reakcie, riadi pracovné toky a sleduje stav zamedzenia šírenia a obnovy.

4.2.2 Iniciuje a vedie poincidentné revízie (PIR) a zabezpečuje, aby boli nápravné opatrenia zaznamenané a implementované.

[... 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 musí byť preskúmaná najmenej raz ročne a podľa potreby revidovaná tak, aby zohľadnila:

9.1.1 zmeny v prostredí hrozieb, typoch incidentov alebo vektoroch útoku,

9.1.2 poznatky zo závažných incidentov, takmer vzniknutých incidentov alebo regulačných zistení,

9.1.3 aktualizácie príslušných zákonov a predpisov (napr. GDPR, DORA, NIS2),

9.1.4 spätnú väzbu z cvičení reakcie na incidenty a poincidentných revízií.

9.2 CISO zodpovedá za iniciovanie a koordináciu procesu preskúmania po konzultácii s:

9.2.1.1 právnym poradcom a DPO,

9.2.1.2 SOC a IT prevádzkou,

9.2.1.3 tímami kontinuity činností a riadenia rizík,

9.2.1.4 vrcholovým vedením.

9.3 Zmeny politiky musia byť:

9.3.1 zdokumentované v repozitári podliehajúcom riadeniu verzií,

9.3.2 oznámené všetkým dotknutým tímom a zapracované do školení povedomia,

9.3.3 validované prostredníctvom stolových alebo živých cvičení reakcie na incidenty do troch mesiacov od schválenia.

9.4 Naliehavé aktualizácie vyvolané novovznikajúcimi hrozbami, auditnými zisteniami alebo novo vydanými zákonnými povinnosťami musia byť zavedené bezodkladne a zaznamenané v histórii revízií politiky.

10. Súvisiace politiky a väzby

10.1 Túto politiku podporujú a dopĺňajú tieto organizačné politiky:

10.1.1 P1 – Politika informačnej bezpečnosti: stanovuje nadradenú požiadavku na prevádzku pripravenú na incidenty a založenú na rizikách.

10.1.2 P5 – Politika riadenia zmien: zabezpečuje, aby činnosti zamedzenia šírenia a obnovy zahŕňajúce infraštruktúru alebo služby prebiehali podľa formálnych postupov.

10.1.3 P13 – Politika klasifikácie a označovania údajov: podporuje klasifikáciu závažnosti incidentov podľa citlivosti údajov.

10.1.4 P15 – Politika zálohovania a obnovy: umožňuje obnovu po ransomvéri alebo deštruktívnych útokoch pri zachovaní integrity.

10.1.5 P18 – Politika kryptografických kontrol: definuje opatrenia šifrovania, ktoré znižujú dopad incidentov a riziká vystavenia údajov.

10.1.6 P22 – Politika logovania a monitorovania: poskytuje základnú viditeľnosť udalostí, upozorňovanie a uchovávanie logov potrebné na účinnú detekciu a forenznú analýzu.

10.1.7 P29 – Politika testovacích údajov a testovacích prostredí: zabezpečuje, aby boli incidenty ovplyvňujúce aj neprodukčné systémy riešené štruktúrovane a bezpečne.

10.1.8 P33 – Politika monitorovania auditu a súladu: overuje pripravenosť na incidenty a účinnosť reakcie prostredníctvom štruktúrovaných auditov a posúdení súladu.

11. Referenčné normy a rámce

11.1 ISO/IEC 27001: Kapitola 8.1 – Prevádzkové plánovanie a riadenie: štruktúrované procesy na riadenie rizík a plánovanie reakcie na incidenty.

11.2 ISO/IEC 27002:2022 – Kontroly 5.25–5.27: zodpovednosti za riadenie incidentov, nahlasovanie, reakciu, komunikáciu a zlepšovanie.

11.3 NIST SP 800-53 Rev.5: IR-1 až IR-9, AU-6, PL-2: komplexné požiadavky na životný cyklus reakcie na incidenty, audit a bezpečnostné plánovanie.

11.4 Nariadenie EÚ GDPR: Článok 33/34: oznamovacie povinnosti voči dozorným orgánom a požiadavky na oznámenie dotknutým osobám (s definovanými výnimkami).

11.5 Smernica EÚ NIS2 (2022/2555): Článok 23: povinné vnútroštátne nahlasovanie vrátane priebežných a konečných oznamovacích povinností.

11.6 Nariadenie EÚ DORA (2022/2554): Článok 17: požiadavky na nahlasovanie incidentov súvisiacich s IKT príslušným orgánom zo strany finančných inštitúcií.

11.7 COBIT 2019: DSS02, DSS04, MEA01: riadenie servisných incidentov a kontinuity činností spolu s monitorovaním výkonnosti a súladu.