					Sem vložte název registrované právnické osoby							
Číslo dokumentu: P30S					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	Kapitoly 6.1, 6.3, 8	řízení incidentů, neustálé zlepšování, provozní řízení
ISO/IEC 27002:2022	Opatření 5.24, 5.25	detekce incidentů, připravenost, získávání poznatků
NIST SP 800-53 Rev.5	IR-4, IR-5, IR-6	zvládání incidentů, monitorování a hlášení
GDPR	Článek 33	požadavky na oznamování porušení zabezpečení
směrnice NIS2	Článek 23	povinné hlášení kybernetických incidentů
nařízení DORA	Článek 17	řízení incidentů v oblasti ICT
COBIT 2019	DSS02, DSS04	řízení služeb a incidentů a kontinuita činností

1. Účel

1.1. Tato politika stanoví, jak organizace detekuje, hlásí a řeší incidenty informační bezpečnosti, které ovlivňují její digitální systémy, data nebo služby.

1.2. Umožňuje organizaci minimalizovat škody, chránit data zákazníků a plnit regulatorní požadavky, jako je například 72hodinová lhůta podle GDPR pro oznámení porušení zabezpečení.

1.3. Tato politika zajišťuje jasné odpovědnosti, komunikační postupy a následné činnosti po incidentu i v malých organizacích bez vyhrazeného bezpečnostního týmu.

2. Rozsah

2.1. Tato politika se vztahuje na:

2.1.1. všechny zaměstnance, smluvní pracovníky a externí poskytovatele IT služeb

2.1.2. všechny systémy a služby spravované společností, včetně webových stránek, cloudových platforem, mobilních zařízení, notebooků a e-mailových účtů

2.1.3. všechny typy incidentů, včetně:

2.1.3.1. neoprávněného přístupu k datům nebo systémům

2.1.3.2. infekce malwarem nebo ransomwarem

2.1.3.3. pokusů o phishing nebo sociální inženýrství

2.1.3.4. výpadků systémů v důsledku kybernetického útoku nebo zneužití

2.1.3.5. náhodného zpřístupnění nebo vymazání citlivých informací

2.1.3.6. ztráty nebo odcizení firemních zařízení nebo paměťových médií

3. Cíle

3.1. Zavést jasný proces pro rozpoznání bezpečnostních incidentů a jejich eskalaci.

3.2. Zajistit, aby incidenty byly hlášeny, zaznamenávány a řešeny ve stanovených lhůtách.

3.3. Umožnit rychlé omezení dopadů, obnovu dat a obnovení služeb.

3.4. Zajistit, aby dotčené strany (např. zákazníci, regulační orgány) byly vyrozuměny, pokud to vyžadují právní předpisy.

3.5. Předcházet opakování prostřednictvím analýzy kořenové příčiny, nápravných opatření a zlepšování politiky.

3.6. Umožnit SME splnit požadavky certifikace ISO 27001 a během auditů doložit odpovědnost.

4. Role a odpovědnosti

4.1. generální ředitel (GM)

4.1.1. Je vlastníkem této politiky a zajišťuje její implementaci.

4.1.2. Dohlíží na činnosti reakce na incidenty a schvaluje oznámení regulačním orgánům nebo zákazníkům.

4.1.3. Přezkoumává zprávy po incidentu a zajišťuje aktualizaci politiky, je-li to nezbytné.

4.1.4. Může delegovat koordinační povinnosti, odpovědnost však zůstává na něm.

4.2. poskytovatel IT podpory / správce systémů (interní nebo externí)

4.2.1. Detekuje a vyšetřuje potenciální bezpečnostní incidenty.

4.2.2. Provádí opatření k omezení dopadů a obnově (např. deaktivaci přístupu, obnovu ze záloh).

4.2.3. Informuje GM o všech potvrzených nebo podezřelých incidentech do 1 hodiny od jejich zjištění.

4.2.4. Vede evidenci incidentů s časovými razítky, posouzením dopadu a přijatými opatřeními reakce.

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

9. Požadavky na přezkoumávání a aktualizaci

9.1. Plánovaný přezkum

9.1.1. Tato politika musí být nejméně jednou za 12 měsíců přezkoumána generálním ředitelem (GM), aby bylo zajištěno:

9.1.1.1. sladění s opatřeními ISO/IEC 27001:2022

9.1.1.2. reakce na nové hrozby, rizika a incidenty

9.1.1.3. trvalý soulad s právními a smluvními povinnostmi (např. GDPR, DORA)

9.2. Spouštěcí události

9.2.1. Politika musí být rovněž přezkoumána a aktualizována po:

9.2.1.1. jakémkoli incidentu s vysokou závažností nebo oznámení regulačnímu orgánu

9.2.1.2. zavedení nové IT infrastruktury nebo změn systému

9.2.1.3. změnách právních požadavků týkajících se porušení bezpečnosti

9.3. Dokumentace přezkumu a distribuce

9.3.1. Všechny přezkumy a změny musí být zdokumentovány v přehledu změn politiky

9.3.2. Aktualizované verze musí být distribuovány všem zaměstnancům, dodavatelům a poskytovatelům IT zapojeným do bezpečnosti nebo provozu systémů

9.3.3. Důkazy o povědomí personálu (např. zápisy z jednání nebo e-mailová potvrzení) musí být uchovávány pro účely připravenosti na audit

10. Související politiky a vazby

10.1. Tato politika musí být uplatňována v koordinaci s následujícími politikami SME:

10.1.1. P1S – Politika informační bezpečnosti: stanoví celková očekávání pro zachování důvěrnosti, integrity a dostupnosti během provozu, včetně zvládání incidentů.

10.1.2. P2S – Politika rolí a odpovědností v oblasti správy a řízení: stanoví struktury pravomocí a odpovědnosti pro detekci incidentů, hlášení a eskalaci.

10.1.3. P4S – Politika řízení přístupu: umožňuje okamžité odebrání přístupových oprávnění během činností reakce na incident.

10.1.4. P8S – Politika povědomí o informační bezpečnosti a školení: zajišťuje, aby všichni zaměstnanci dokázali bezpečnostní incidenty účinně rozpoznat a nahlásit.

10.1.5. P17S – Politika ochrany dat a soukromí: upravuje právní postupy oznamování porušení zabezpečení podle GDPR a podporuje soulad s regulatorními požadavky během incidentů.

10.1.6. P22S – Politika protokolování a monitorování: poskytuje nezbytné nástroje a přehled pro detekci, analýzu a audit bezpečnostních událostí.

10.1.7. P31S – Politika shromažďování důkazů a forenzní analýzy: podporuje vyšetřování a právní obhajitelnost činností souvisejících s incidenty tím, že stanoví správné nakládání s důkazy.

10.2. Tyto politiky společně vytvářejí provozní rámec SME pro detekci incidentů informační bezpečnosti, reakci na ně a obnovu po nich.

11. Referenční normy a rámce

11.1. ISO/IEC 27001

11.1.1. Kapitola 6.1 – Vyžaduje plánování ošetření rizik, včetně přípravy na incidenty.

11.1.2. Kapitola 6.3 – Podporuje neustálé zlepšování prostřednictvím poznatků získaných z bezpečnostních událostí.

11.1.3. Kapitola 8.1 – Zdůrazňuje provozní řízení pro zvládání incidentů a narušení.

11.2. ISO/IEC 27002

11.2.1. Opatření 5.24 – Vyžaduje strukturovaný přístup k hlášení, posuzování a reakci na incidenty informační bezpečnosti.

11.2.2. Opatření 5.25 – Zaměřuje se na získávání poznatků z incidentů za účelem zlepšení budoucí připravenosti a odolnosti systémů.

11.3. NIST SP 800-53 Rev.5

11.3.1. IR-4 – Definuje postupy pro zvládání incidentů, včetně omezení dopadů a obnovy.

11.3.2. IR-5 – Stanoví požadavky na monitorování a analýzu incidentů.

11.3.3. IR-6 – Ukládá interní a externí postupy hlášení incidentů.

11.4. GDPR

11.4.1. Článek 33 – Vyžaduje oznámení porušení zabezpečení osobních údajů regulačním orgánům do 72 hodin, včetně podrobností o rozsahu a zmírnění dopadů.

11.5. směrnice NIS2 (2022/2555)

11.5.1. Článek 23 – Vyžaduje, aby základní a důležité subjekty oznamovaly významné incidenty příslušným orgánům za použití standardizovaných formátů hlášení.

11.6. nařízení DORA (2022/2554)

11.6.1. Článek 17 – Vyžaduje, aby finanční subjekty klasifikovaly, hlásily a sledovaly incidenty a narušení související s ICT.

11.7. COBIT 2019

11.7.1. DSS02 – Řízení požadavků na služby a incidentů: poskytuje vodítko pro účinné zvládání provozních a bezpečnostních incidentů v souladu s cíli správy a řízení.

11.7.2. DSS04 – Řízení kontinuity: propojuje reakci na incidenty s širšími strategiemi kontinuity činností a obnovy.