					Sem zadajte názov registrovanej právnickej osoby							
Číslo dokumentu: P30S					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	Kapitoly 6.1, 6.3, 8	Riadenie incidentov, neustále zlepšovanie, prevádzkové riadenie
ISO/IEC 27002:2022	Kontroly 5.24, 5.25	Detekcia incidentov, pripravenosť, poznatky z incidentov
NIST SP 800-53 Rev.5	IR-4, IR-5, IR-6	Riešenie incidentov, monitorovanie a oznamovanie
GDPR EÚ	Článok 33	Požiadavky na oznamovanie porušenia ochrany osobných údajov
Smernica EÚ NIS2	Článok 23	Povinné nahlasovanie kybernetických incidentov
Nariadenie EÚ DORA	Článok 17	Riadenie incidentov súvisiacich so systémami IKT
COBIT 2019	DSS02, DSS04	Riadenie služieb a incidentov a kontinuita činností

1. Účel

1.1. Táto politika stanovuje, ako organizácia deteguje, nahlasuje a rieši incidenty informačnej bezpečnosti, ktoré ovplyvňujú jej digitálne systémy, údaje alebo služby.

1.2. Umožňuje organizácii minimalizovať škody, chrániť údaje zákazníkov a plniť zákonné povinnosti, ako je napríklad 72-hodinová lehota podľa GDPR na oznámenie porušenia ochrany osobných údajov.

1.3. Politika zabezpečuje jednoznačné zodpovednosti, komunikačné postupy a nadväzujúce činnosti po incidente aj v malých organizáciách bez vyhradeného bezpečnostného tímu.

2. Rozsah

2.1. Táto politika sa vzťahuje na:

2.1.1. všetkých zamestnancov, zmluvných pracovníkov a externých poskytovateľov IT služieb,

2.1.2. všetky systémy a služby spravované spoločnosťou vrátane webových sídiel, cloudových platforiem, mobilných zariadení, notebookov a e-mailových účtov,

2.1.3. všetky typy incidentov vrátane:

2.1.3.1. neoprávneného prístupu k údajom alebo systémom,

2.1.3.2. infekcie malvérom alebo ransomvérom,

2.1.3.3. pokusov o phishing alebo sociálne inžinierstvo,

2.1.3.4. výpadkov systémov v dôsledku kybernetického útoku alebo zneužitia,

2.1.3.5. náhodného sprístupnenia alebo vymazania citlivých informácií,

2.1.3.6. straty alebo krádeže zariadení organizácie alebo pamäťových médií.

3. Ciele

3.1. Zaviesť jednoznačný proces na rozpoznanie a eskaláciu bezpečnostných incidentov.

3.2. Zabezpečiť, aby incidenty boli nahlásené, zaznamenané a riešené v rámci vopred definovaných lehôt.

3.3. Umožniť rýchle zamedzenie šírenia, obnovu údajov a obnovenie služieb.

3.4. Zabezpečiť, aby boli dotknuté strany (napr. zákazníci, regulačné orgány) informované, ak to vyžaduje právny predpis.

3.5. Predchádzať opakovaniu prostredníctvom analýzy hlavnej príčiny, nápravných opatrení a zlepšovania politiky.

3.6. Umožniť MSP splniť požiadavky certifikácie ISO/IEC 27001 a preukázať zodpovedný prístup počas auditov.

4. Roly a zodpovednosti

4.1. Generálny manažér (GM)

4.1.1. Zodpovedá za túto politiku a zabezpečuje jej implementáciu.

4.1.2. Dohliada na činnosti reakcie na incidenty a schvaľuje oznámenia regulačným orgánom alebo zákazníkom.

4.1.3. Preskúmava správy po incidente a zabezpečuje aktualizáciu politiky, ak je to potrebné.

4.1.4. Môže delegovať koordinačné úlohy, avšak ponecháva si zodpovednosť za prijaté rozhodnutia.

4.2. Poskytovateľ IT služieb / správca systému (interný alebo externý)

4.2.1. Deteguje a vyšetruje potenciálne bezpečnostné incidenty.

4.2.2. Zavádza opatrenia na zamedzenie šírenia a obnovu (napr. deaktivácia prístupu, obnova zo záloh).

4.2.3. Informuje GM o všetkých potvrdených alebo podozrivých incidentoch do 1 hodiny od ich zistenia.

4.2.4. Vedie záznamy o incidentoch s časovými pečiatkami, posúdením vplyvu a prijatými opatreniami reakcie.

[... 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. Plánované preskúmanie

9.1.1. Túto politiku musí generálny manažér (GM) preskúmať najmenej raz za 12 mesiacov, aby sa zabezpečilo:

9.1.1.1. zosúladenie s kontrolami ISO/IEC 27001:2022,

9.1.1.2. reakcia na nové hrozby, riziká a incidenty,

9.1.1.3. trvalý súlad so zákonnými a zmluvnými povinnosťami (napr. GDPR, DORA).

9.2. Spúšťacie udalosti

9.2.1. Politika sa musí preskúmať a aktualizovať aj po:

9.2.1.1. každom incidente s vysokou závažnosťou alebo regulačnom oznámení,

9.2.1.2. zavedení novej IT infraštruktúry alebo zmenách systémov,

9.2.1.3. zmenách zákonných požiadaviek týkajúcich sa porušení bezpečnosti.

9.3. Dokumentácia preskúmania a distribúcia

9.3.1. Všetky preskúmania a zmeny musia byť zdokumentované v zozname zmien politiky.

9.3.2. Aktualizované verzie musia byť distribuované všetkým zamestnancom, dodávateľom a poskytovateľom IT služieb zapojeným do bezpečnosti alebo prevádzky systémov.

9.3.3. Dôkazy o oboznámení zamestnancov (napr. poznámky zo stretnutí alebo e-mailové potvrdenia) sa musia uchovávať na účely auditnej pripravenosti.

10. Súvisiace politiky a väzby

10.1. Táto politika sa musí uplatňovať v koordinácii s týmito politikami MSP:

10.1.1. P1S – Politika informačnej bezpečnosti: stanovuje celkové požiadavky na zachovanie dôvernosti, integrity a dostupnosti počas prevádzky vrátane riešenia incidentov.

10.1.2. P2S – Politika rolí a zodpovedností v oblasti správy a riadenia: stanovuje štruktúry právomocí a zodpovednosti za detekciu, nahlasovanie a eskaláciu incidentov.

10.1.3. P4S – Politika riadenia prístupu: umožňuje okamžité odňatie prístupových práv počas činností reakcie na incident.

10.1.4. P8S – Politika povedomia a školení v oblasti informačnej bezpečnosti: zabezpečuje, aby všetci zamestnanci vedeli účinne identifikovať a nahlasovať bezpečnostné incidenty.

10.1.5. P17S – Politika ochrany údajov a súkromia: usmerňuje zákonné postupy oznamovania porušenia ochrany osobných údajov podľa GDPR a podporuje súlad počas riešenia incidentov.

10.1.6. P22S – Politika logovania a monitorovania: poskytuje potrebné nástroje a viditeľnosť na detekciu, analýzu a audit bezpečnostných udalostí.

10.1.7. P31S – Politika zberu dôkazov a forenznej analýzy: podporuje vyšetrovanie a právnu obhájiteľnosť činností súvisiacich s incidentmi prostredníctvom správneho nakladania s dôkazmi.

10.2. Tieto politiky spoločne vytvárajú prevádzkový rámec MSP na detekciu, reakciu a obnovu po incidentoch informačnej bezpečnosti.

11. Referenčné normy a rámce

11.1. ISO/IEC 27001

11.1.1. Kapitola 6.1 – Vyžaduje plánovanie ošetrenia rizík vrátane prípravy na incidenty.

11.1.2. Kapitola 6.3 – Podporuje neustále zlepšovanie na základe poznatkov z bezpečnostných udalostí.

11.1.3. Kapitola 8.1 – Zdôrazňuje prevádzkové riadenie na zvládanie incidentov a prerušení.

11.2. ISO/IEC 27002

11.2.1. Kontrola 5.24 – Vyžaduje štruktúrovaný prístup k nahlasovaniu, posudzovaniu a riešeniu incidentov informačnej bezpečnosti.

11.2.2. Kontrola 5.25 – Zameriava sa na poučenie z incidentov s cieľom zlepšiť budúcu pripravenosť a odolnosť systémov.

11.3. NIST SP 800-53 Rev.5

11.3.1. IR-4 – Definuje postupy riešenia incidentov vrátane zamedzenia šírenia a obnovy.

11.3.2. IR-5 – Stanovuje požiadavky na monitorovanie a analýzu incidentov.

11.3.3. IR-6 – Ukladá povinnosť zaviesť protokoly externého a interného nahlasovania incidentov.

11.4. GDPR EÚ

11.4.1. Článok 33 – Vyžaduje oznámiť porušenia ochrany osobných údajov regulačným orgánom do 72 hodín vrátane údajov o rozsahu a zmierňujúcich opatreniach.

11.5. Smernica EÚ NIS2 (2022/2555)

11.5.1. Článok 23 – Vyžaduje, aby základné a dôležité subjekty oznamovali významné incidenty príslušným orgánom pomocou štandardizovaných formátov hlásenia.

11.6. Nariadenie EÚ DORA (2022/2554)

11.6.1. Článok 17 – Vyžaduje, aby finančné subjekty klasifikovali, nahlasovali a sledovali incidenty a prerušenia súvisiace so systémami IKT.

11.7. COBIT 2019

11.7.1. DSS02 – Riadenie servisných požiadaviek a incidentov: poskytuje usmernenie na účinné riešenie prevádzkových a bezpečnostných incidentov v súlade s cieľmi správy a riadenia.

11.7.2. DSS04 – Riadenie kontinuity: prepája reakciu na incidenty so širšími stratégiami kontinuity činností a obnovy.