					Sem zadajte názov registrovanej právnickej osoby							
Číslo dokumentu: P05S					Názov dokumentu: **Politika riadenia zmien**							
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 6.1, 8.	
ISO/IEC 27002:2022	Kontrola 8.	
NIST SP 800-53 Rev. 5	CM-2 až CM-5, CM-11	
Smernica EÚ NIS2	Článok 21(2)(b)	
Nariadenie EÚ DORA	Články 6(9), 8(4)(b)	
COBIT 2019	BAI06, DSS	

1. Účel

1.1 Táto politika zabezpečuje, aby všetky zmeny IT systémov, konfigurácií, podnikových aplikácií alebo cloudových služieb boli pred implementáciou naplánované, posúdené z hľadiska rizík, otestované a schválené.

1.2 Cieľom je znížiť prevádzkové narušenia, bezpečnostné riziká a výpadky služieb zavedením zjednodušeného, ale záväzného procesu, ktorý sa uplatňuje aj v malých podnikoch s obmedzenými zdrojmi.

1.3 Táto politika podporuje certifikáciu podľa ISO/IEC 27001:2022 tým, že formalizuje spôsob riadenia a dokumentovania technických a prevádzkových zmien.

2. Rozsah

2.1 Táto politika sa vzťahuje na:

2.1.1 zamestnancov a vedúcich oddelení, ktorí navrhujú alebo vykonávajú zmeny,

2.1.2 externých poskytovateľov IT služieb, ktorí spravujú systémy alebo softvér,

2.1.3 generálneho manažéra (GM), ktorý nesie celkovú zodpovednosť za schvaľovanie zmien.

2.2 Zahŕňa zmeny týkajúce sa:

2.2.1 softvéru (aktualizácie, záplaty, nové aplikácie),

2.2.2 hardvéru (výmeny, modernizácie),

2.2.3 sieťových konfigurácií a konfigurácie firewallov,

2.2.4 cloudových služieb, prístupových oprávnení používateľov alebo integrácií s dodávateľmi,

2.2.5 zmien kritických podnikových procesov zahŕňajúcich informačné systémy.

2.3 Do rozsahu tejto politiky patria plánované aj núdzové zmeny.

3. Ciele

3.1 Zabezpečiť, aby všetky zmeny IT a podnikových systémov boli autorizované, zdokumentované a aby ich bolo možné v prípade problémov vrátiť do pôvodného stavu.

3.2 Predchádzať neplánovaným výpadkom, strate údajov alebo bezpečnostným incidentom spôsobeným nekontrolovanými zmenami.

3.3 Stanoviť jednoduché a opakovateľné postupy pre predkladanie zmien, schvaľovanie, testovanie a návrat do pôvodného stavu.

3.4 Viesť overiteľný register zmien, ktorý podporuje prevádzkovú zodpovednosť a súlad s požiadavkami.

3.5 Umožniť rozhodovanie založené na riziku pri významných alebo citlivých zmenách.

4. Roly a zodpovednosti

4.1 Generálny manažér (GM)

4.1.1 Nesie konečnú zodpovednosť za všetky významné zmeny.

4.1.2 Preskúmava a schvaľuje nerutinné, kritické alebo vysokorizikové zmeny.

4.1.3 Preskúmava register zmien štvrťročne alebo po významných incidentoch.

4.2 IT podpora alebo externý poskytovateľ IT služieb

4.2.1 Implementuje zmeny vrátane aktualizácií konfigurácie, záplatovania a migrácií systémov.

4.2.2 Vedie základný register zmien, v ktorom zaznamenáva dátumy, typy zmien, výsledky a schvaľujúce osoby.

4.2.3 Pred implementáciou testuje zmeny a podľa potreby vykonáva kroky na návrat do pôvodného stavu.

4.2.4 Informuje dotknutých používateľov pred významnými zmenami a po nich.

[... 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 Ročné preskúmanie

9.1.1 Táto politika musí byť každoročne preskúmaná generálnym manažérom (GM) alebo určenou IT kontaktnou osobou s cieľom zabezpečiť súlad s aktuálnymi systémami, pracovnými postupmi a regulačnými požiadavkami.

9.2 Priebežné preskúmania

9.2.1 Preskúmania sa musia vykonať aj v prípade:

9.2.1.1 bezpečnostných incidentov spôsobených nedostatočným riadením zmien,

9.2.1.2 zavedenia nových IT systémov,

9.2.1.3 zmien relevantných noriem, ako sú ISO, NIS2 alebo DORA.

9.3 Dokumentovanie aktualizácií

9.3.1 Zmeny tejto politiky musia podliehať riadeniu verzií a byť schválené generálnym manažérom (GM). Každá verzia musí obsahovať dátum, súhrn zmien a schvaľujúcu osobu.

9.4 Oboznámenie s politikou

9.4.1 O každej aktualizácii musia byť informovaní všetci dotknutí zamestnanci a externí poskytovatelia. Dokumentácia musí byť aktualizovaná na všetkých referenčných miestach (napr. personálny portál, zdieľané úložiská).

10. Súvisiace politiky a väzby

10.1 Táto politika úzko súvisí s nasledujúcimi SME politikami:

10.1.1 P2S – Politika rolí a zodpovedností správy a riadenia: Definuje právomoc schvaľovať zmeny.

10.1.2 P4S – Politika riadenia prístupu: Zabezpečuje, aby zmeny prístupových práv vyplývajúce zo zmien boli správne zdokumentované a implementované.

10.1.3 P7S – Politika nástupu a ukončenia: Koordinuje zmeny súvisiace s prechodmi medzi rolami a zriaďovaním prístupov.

10.1.4 P15S – Politika zálohovania a obnovy: Zabezpečuje, aby bolo možné vykonať návrat do pôvodného stavu a obnovu, ak zmena zlyhá.

10.1.5 P30S – Politika reakcie na incidenty: Upravuje spôsob, akým sa neúspešné alebo neautorizované zmeny riešia ako bezpečnostné incidenty.

11. Referenčné normy a rámce

11.1 ISO/IEC 27001

11.1.1 Kapitola 6.1 – Plánovanie založené na riziku musí zahŕňať činnosti súvisiace so zmenami.

11.1.2 Kapitola 8.1 – Prevádzkové kontroly sa musia pri činnostiach súvisiacich so zmenami uplatňovať konzistentne, aby bola zabezpečená integrita služieb.

11.2 ISO/IEC 27002

11.2.1 Kontrola 8.32 – Poskytuje usmernenie pre procesy bezpečného riadenia zmien vrátane dokumentácie, testovania a schvaľovania.

11.3 NIST SP 800-53 Rev. 5

11.3.1 CM-2 – Referenčná konfigurácia systémov pred zmenou.

11.3.2 CM-3 – Riadenie zmien konfigurácie.

11.3.3 CM-4 – Analýza bezpečnostného dopadu.

11.3.4 CM-5 – Schvaľovanie a dokumentovanie zmien.

11.3.5 CM-11 – Audit a monitorovanie zmien.

11.4 Smernica EÚ NIS2

11.4.1 Článok 21(2)(b) – Vyžaduje formálne postupy pre technické a organizačné bezpečnostné opatrenia vrátane riadenia zmien.

11.5 Nariadenie EÚ DORA

11.5.1 Články 6(9) a 8(4)(b) – Vyžadujú, aby finančné subjekty udržiavali riadenie zmien a riadenie konfigurácie pre systémy IKT.

11.6 COBIT 2019

11.6.1 BAI06 – Riadenie zmien: Zdôrazňuje plánovanie, hodnotenie rizík a schopnosť návratu do pôvodného stavu.

11.6.2 DSS01 – Riadenie prevádzky: Zabezpečuje prevádzkovú integritu počas technických prechodov a zmien.