					Sem vložte název registrované právnické osoby							
Číslo dokumentu: P05S					Název dokumentu: **Politika řízení změn**							
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**

Soulad s normami a právními předpisy

Norma/právní předpis	Kapitola/článek	Komentář
ISO/IEC 27001:2022	Kapitola 6.1, 8	
ISO/IEC 27002:2022	Opatření 8	
NIST SP 800-53 Rev.5	CM-2 až CM-5, CM-11	
směrnice NIS2	Článek 21(2)(b)	
nařízení DORA	Články 6(9), 8(4)(b)	
COBIT 2019	BAI06, DSS	

1. Účel

1.1 Tato politika zajišťuje, aby všechny změny IT systémů, konfigurací, podnikových aplikací nebo cloudových služeb byly před implementací naplánovány, posouzeny z hlediska rizik, otestovány a schváleny.

1.2 Cílem je omezit provozní narušení, bezpečnostní rizika a výpadky služeb zavedením zjednodušeného, avšak vymahatelného procesu, který je uplatnitelný i v malých podnicích s omezenými zdroji.

1.3 Tato politika podporuje certifikaci podle ISO/IEC 27001:2022 tím, že formalizuje způsob řízení a dokumentování technických a provozních změn.

2. Rozsah

2.1 Tato politika se vztahuje na:

2.1.1 zaměstnance a vedoucí oddělení, kteří navrhují nebo provádějí změny

2.1.2 externí poskytovatele IT služeb, kteří spravují systémy nebo software

2.1.3 generálního ředitele, který nese celkovou odpovědnost za schvalování změn

2.2 Tato politika zahrnuje změny týkající se:

2.2.1 softwaru (aktualizace, záplaty, nové aplikace)

2.2.2 hardwaru (výměny, upgrady)

2.2.3 konfigurace sítě a firewallů

2.2.4 cloudových služeb, přístupových oprávnění uživatelů nebo integrací s dodavateli

2.2.5 změn kritických obchodních procesů zahrnujících informační systémy

2.3 Do rozsahu této politiky spadají plánované i nouzové změny.

3. Cíle

3.1 Zajistit, aby všechny změny IT a podnikových systémů byly schváleny, zdokumentovány a aby bylo možné je v případě problémů vrátit do původního stavu.

3.2 Předcházet neplánovaným výpadkům, ztrátě dat nebo bezpečnostním incidentům způsobeným neřízenými změnami.

3.3 Stanovit jednoduché a opakovatelné postupy pro podání, schválení, testování a vrácení změn.

3.4 Udržovat auditovatelný Registr změn, který podporuje provozní odpovědnost a soulad s právními předpisy.

3.5 Umožnit rozhodování na základě rizik u významných nebo citlivých změn.

4. Role a odpovědnosti

4.1 Generální ředitel

4.1.1 Nese konečnou odpovědnost za všechny významné změny.

4.1.2 Přezkoumává a schvaluje nerutinní, kritické nebo vysoce rizikové změny.

4.1.3 Přezkoumává Registr změn čtvrtletně nebo po závažných incidentech.

4.2 IT podpora nebo externí poskytovatel IT služeb

4.2.1 Provádí změny, včetně změn konfigurace, záplatování a migrací systémů.

4.2.2 Vede základní Registr změn se záznamem dat, typů změn, výsledků a schvalujících osob.

4.2.3 Před implementací změny provádí testování a podle potřeby uplatňuje postupy pro vrácení změn.

4.2.4 Informuje dotčené uživatele před významnými změnami i po nich.

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

9. Požadavky na přezkum a aktualizaci

9.1 Každoroční přezkum

9.1.1 Tato politika musí být každoročně přezkoumána generálním ředitelem nebo určeným IT kontaktem, aby byl zajištěn soulad s aktuálními systémy, pracovními postupy a regulačními požadavky.

9.2 Mimořádné přezkumy

9.2.1 Přezkum musí být vyvolán také v případě:

9.2.1.1 bezpečnostních incidentů způsobených nedostatečným řízením změn

9.2.1.2 zavedení nových IT systémů

9.2.1.3 změn relevantních norem, jako jsou ISO, NIS2 nebo DORA

9.3 Dokumentování aktualizací

9.3.1 Změny této politiky musí být vedeny v režimu správy verzí a schváleny generálním ředitelem. U každé verze musí být zaznamenáno datum, shrnutí změn a schvalující osoba.

9.4 Komunikace politiky

9.4.1 Veškeré aktualizace musí být sděleny všem dotčeným zaměstnancům a externím poskytovatelům. Dokumentace musí být aktualizována na všech referenčních místech (např. personální portál, sdílené disky).

10. Související politiky a návaznosti

10.1 Tato politika úzce souvisí s následujícími SME politikami:

10.1.1 P2S – Politika rolí a odpovědností v oblasti správy a řízení: Definuje pravomoci ke schvalování změn.

10.1.2 P4S – Politika řízení přístupu: Zajišťuje, aby změny přístupových oprávnění vyplývající ze změn byly řádně zdokumentovány a implementovány.

10.1.3 P7S – Politika nástupu a ukončení: Koordinuje změny související se změnou role a zřizováním přístupových práv.

10.1.4 P15S – Politika zálohování a obnovy: Zajišťuje možnost vrácení změn a obnovy, pokud změna selže.

10.1.5 P30S – Politika reakce na incidenty: Upravuje způsob, jakým jsou neúspěšné nebo neoprávněné změny řešeny jako bezpečnostní incidenty.

11. Referenční normy a rámce

11.1 ISO/IEC 27001

11.1.1 Kapitola 6.1 – Plánování založené na rizicích musí zahrnovat činnosti související se změnami.

11.1.2 Kapitola 8.1 – Provozní opatření musí být při činnostech souvisejících se změnami uplatňována konzistentně, aby byla zajištěna integrita služeb.

11.2 ISO/IEC 27002

11.2.1 Opatření 8.32 – Poskytuje návod pro bezpečné procesy řízení změn, včetně dokumentace, testování a schvalování.

11.3 NIST SP 800-53 Rev.

11.3.1 CM-2 – Základní konfigurace systémů před změnou.

11.3.2 CM-3 – Řízení změn konfigurace.

11.3.3 CM-4 – Analýza bezpečnostních dopadů.

11.3.4 CM-5 – Schvalování a dokumentování změn.

11.3.5 CM-11 – Audit a monitorování změn.

11.4 směrnice NIS2

11.4.1 Článek 21(2)(b) – Vyžaduje formální postupy pro technická a organizační bezpečnostní opatření, včetně řízení změn.

11.5 nařízení DORA

11.5.1 Články 6(9) a 8(4)(b) – Vyžadují, aby finanční subjekty zavedly řízení změn a řízení konfigurace ICT systémů.

11.6 COBIT 2019

11.6.1 BAI06 – Řízení změn: klade důraz na plánování, vyhodnocení rizik a schopnost vrácení změn.

11.6.2 DSS01 – Řízení provozu: zajišťuje provozní integritu při technických přechodech a změnách.