					Sem vložte název registrované právnické osoby							
Číslo dokumentu: P05					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**

V souladu s normami a právními předpisy

Norma/právní předpis	Článek/ustanovení	Komentář
ISO/IEC 27001:2022	Články 6.1, 5	Řeší opatření k ošetření rizik, řízení přístupu a řízení změn
ISO/IEC 27002:2022	Opatření 8	Zavádí strukturovaný proces řízení změn
NIST SP 800-53 Rev.5	CM-2 až CM-14	Opatření pro řízení konfigurace
GDPR EU	Články 32(1)(b–d), 25; bod odůvodnění 78	Technická a organizační opatření pro bezpečnost systémů a dat v průběhu změn
směrnice EU NIS2	Článek 21(2)(a, b, d, e)	Stanoví řízení rizik změn ICT
nařízení EU DORA	Články 5, 8, 12	Upravuje provozní rizika, rizika ICT a hlášení incidentů
COBIT 2019	BAI06, BAI02, BAI03, DSS01, MEA01, MEA03	Strukturované řízení IT změn, výkonnost, soulad a související požadavky

1. Účel

1.1. Tato politika stanoví formální rámec pro zahájení, posouzení, schválení, implementaci a přezkum změn informačních systémů, infrastruktury, aplikací a souvisejících procesů organizace.

1.2. Zajišťuje, aby všechny změny byly prováděny řízeným a auditovatelným způsobem s cílem minimalizovat riziko narušení provozu, bezpečnosti nebo regulatorního nesouladu.

1.3. Podporuje opatření 8.32 přílohy A normy ISO/IEC 27001:2022 prosazováním bezpečných, dokumentovaných a s riziky sladěných postupů řízení změn.

1.4. Tato politika dále zajišťuje dohledatelnost rozhodnutí o změnách a podporuje provozní odolnost při plánovaných i nouzových úpravách.

2. Rozsah

2.1. Tato politika se vztahuje na všechny změny ovlivňující systémy, data a prostředí v rozsahu ISMS, včetně:

2.1.1. IT infrastruktury (on-premise, cloud, hybridní prostředí)

2.1.2. Produkčního prostředí, předprodukčních prostředí a prostředí pro obnovu po havárii

2.1.3. Podnikových aplikací, služeb, API a integrací

2.1.4. Konfiguračních nastavení, záplatování systémů, vydání softwaru a migrací systémů

2.1.5. Nouzových oprav a projektových nebo plánovaných změn

2.2. Upravuje změny iniciované:

2.2.1. Interními pracovníky (IT provoz, vývojáři, vlastníci systémů)

2.2.2. Externími dodavateli, poskytovateli řízených služeb (MSP) a dalšími dodavateli a poskytovateli služeb třetích stran

2.2.3. Projektovými týmy při implementaci systémů, upgradech nebo přechodech služeb

2.3. Tato politika se nevztahuje na:

2.3.1. Dočasná testovací a vývojová prostředí bez přístupu k produkčním datům

2.3.2. Osobní konfigurace uživatelů (řešeno v dokumentu Zásady přípustného užívání)

2.3.3. Změny systémů mimo hranice řízení organizace, pokud neovlivňují integrovaná aktiva nebo povinnosti vyplývající ze souladu

3. Cíle

3.1. Zajistit, aby všechny změny byly před provedením přezkoumány, schváleny, otestovány a zdokumentovány.

3.2. Udržet dostupnost systémů, integritu dat a kontinuitu služeb během činností souvisejících se změnou i po jejich dokončení.

3.3. Vyžadovat pro všechny typy změn definovanou klasifikaci změn, plány návratu do původního stavu a hodnocení rizik.

3.4. Umožnit transparentní rozhodování a eskalaci prostřednictvím strukturované správy a řízení.

3.5. Podporovat připravenost na audit prostřednictvím dohledatelných záznamů o změnách a přezkumu po implementaci.

3.6. Prosazovat oddělení povinností a snižovat riziko neoprávněných nebo konfliktních změn v kritických systémech.

4. Role a odpovědnosti

4.1. Vrcholové vedení

4.1.1. Schvaluje Politiku řízení změn a zajišťuje její soulad se strategickými cíli a regulatorními povinnostmi.

4.1.2. Schvaluje programy změn s vysokým dopadem nebo napříč funkcemi v rámci dohledu nad správou a řízením.

4.1.3. Přiděluje nezbytné zdroje a rozpočet na nástroje pro řízení změn a školení pracovníků.

4.2. Poradní výbor pro změny

4.2.1. Přezkoumává a schvaluje standardní a významné změny a zajišťuje odpovídající vyhodnocení rizik, dopadů a závislostí.

4.2.2. Validuje plány návratu do původního stavu, výsledky testů, komunikaci se zainteresovanými stranami a harmonogram.

4.2.3. Je složen z vlastníků systémů, zástupců bezpečnosti, IT provozu, zástupců businessu a zástupců compliance.

4.2.4. Může delegovat rozhodnutí o nízkorizikových nebo nouzových změnách za dokumentovaných podmínek.

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

9. Požadavky na přezkum a aktualizaci

9.1. Spouštěče přezkumu a četnost

9.1.1. Tato politika musí být přezkoumána každoročně nebo při:

9.1.1.1. Významných změnách IT nebo infrastruktury

9.1.1.2. Významných incidentech souvisejících s neúspěšnými nebo neoprávněnými změnami

9.1.1.3. Regulatorních aktualizacích nebo nových právních povinnostech souvisejících se změnami

9.1.1.4. Implementaci nových nástrojů nebo platforem CMS

9.2. Proces přezkumu Politiky řízení změn

9.2.1. Manažer změn povede proces přezkumu ve spolupráci s:

9.2.1.1. IT, bezpečností a provozem

9.2.1.2. Interním auditem a řízením rizik

9.2.1.3. Zástupci Poradního výboru pro změny

9.2.2. Aktualizace musí být přezkoumány a schváleny vrcholovým vedením a Řídicím výborem pro bezpečnost informací.

9.2.3. Znovu vydané verze musí být sledovány v registru dokumentů a oznámeny dotčeným stranám, včetně opětovného potvrzení seznámení podle potřeby.

9.3. Řízení dokumentů a správa verzí

9.3.1. Všechny verze musí obsahovat:

9.3.1.1. ID politiky, název a stupeň klasifikace

9.3.1.2. Vlastníka a historii revizí

9.3.1.3. Přehled změn a datum účinnosti

9.3.1.4. Schvalovací pravomoc

9.3.2. Archivované verze musí být uchovávány v souladu s Politikou uchovávání dokumentů (minimálně 3 roky).

10. Související politiky a vazby

10.1. Tato politika je přímo propojena s následujícími politikami a podporuje jejich uplatňování:

10.1.1. P1 – Politika informační bezpečnosti: Stanoví požadavek na formální bezpečnostní opatření a odpovědnost na úrovni procesů, včetně správy a řízení změn.

10.1.2. P2 – Politika rolí a odpovědností v oblasti správy a řízení: Definuje schvalovací pravomoci a oddělení povinností relevantní pro schvalování změn a dohled.

10.1.3. P4 – Politika řízení přístupu: Zajišťuje, aby přístupová oprávnění osob provádějících změny a osob provádějících jejich přezkum odpovídala zásadě minimálních oprávnění.

10.1.4. P6 – Politika řízení rizik: Zajišťuje, aby všechny změny podléhaly odpovídajícímu vyhodnocení rizik a strategiím zmírnění.

10.1.5. P33 – Politika monitorování auditu a souladu: Upravuje validaci a auditní přezkum záznamů řízení změn a porušení.

10.2. Tyto politiky společně umožňují obhajitelný, dohledatelný a bezpečný životní cyklus řízení změn v rámci ISMS.

11. Referenční normy a rámce

11.1. ISO/IEC 27001:2022

11.1.1. Článek 6.1 – Opatření k řešení rizik a příležitostí: Tato politika podporuje identifikaci, vyhodnocení a řízení rizik souvisejících se změnou.

11.1.2. Článek 5.15 – Řízení přístupu: Zajišťuje, aby přístup během změn byl řízený a dohledatelný.

11.1.3. Opatření 8.32 přílohy A – Řízení změn: Tato politika plně implementuje požadavek na řízení změn zařízení pro zpracování informací a systémů plánovaným a řízeným způsobem.

11.2. ISO/IEC 27002:2022 – Opatření 8

11.2.1. Posiluje implementaci strukturovaného procesu řízení změn včetně klasifikace změn, schvalování, testování, návratu do původního stavu a dokumentace.

11.3. NIST SP 800-53 Rev.5

11.3.1. Rodina CM (CM-1 až CM-14): Tato politika je úzce sladěna s opatřeními řízení konfigurace, včetně výchozích konfigurací (CM-2), řízení změn konfigurace (CM-3), analýzy bezpečnostních dopadů (CM-4) a omezení přístupu (CM-5).

11.3.2. Rodina AU (AU-2, AU-6, AU-12): Mechanismy protokolování a auditu uvedené v této politice podporují dohledatelnost událostí a přezkum souladu u činností souvisejících se změnami.

11.3.3. RA-3, RA-5: Hodnocení rizik vyvolaná změnami a skeny zranitelností jsou začleněny do procesu vyhodnocení změn.

11.3.4. PM-11 (Definice poslání/obchodních procesů): Zajišťuje, aby při změnách byla zachována kontinuita činností a provozní cíle.

11.4. GDPR (2016/679)

11.4.1. Článek 32(1)(b–d): Tato politika podporuje požadavek na přiměřená technická a organizační opatření k zajištění bezpečnosti dat, zejména během systémových změn.

11.4.2. Článek 25 – Ochrana údajů již od návrhu a jako výchozí nastavení: Zajišťuje, aby změny ovlivňující osobní údaje začleňovaly ochranu soukromí a bezpečnost do návrhu i nasazení.

11.4.3. Bod odůvodnění 78: Vyžaduje, aby správci údajů zavedli mechanismy – například politiky řízení změn – k zajištění průběžné důvěrnosti, integrity a odolnosti systémů zpracování.

11.5. směrnice NIS2 (2022/2555)

11.5.1. Článek 21(2)(a, b, d, e): Stanoví technická a organizační opatření pro řízení rizik ICT, včetně rizik vznikajících v důsledku systémových změn, aktualizací softwaru a úprav infrastruktury.

11.6. nařízení DORA (2022/2554)

11.6.1. Článek 5 – Rámec správy a řízení a vnitřních kontrol: Tato politika prosazuje zásady řízení provozních rizik navázané na změny a aktualizace ICT.

11.6.2. Článek 8 – Rámec řízení rizik ICT: Stanoví, že finanční subjekty musí řídit všechny změny ovlivňující systémy ICT v rámci strukturovaných procesů řízení změn – což tato politika odráží svými požadavky na klasifikaci, testování, návrat do původního stavu a dokumentaci.

11.6.3. Článek 12 – Hlášení incidentů: Zajišťuje, že neúspěšné změny vedoucí k narušení ICT jsou dohledatelné, zdokumentované a v relevantních případech oznamované.

11.7. COBIT 2019

11.7.1. BAI06 – Řízené IT změny: Tato politika přímo naplňuje cíle BAI06 tím, že zavádí strukturované workflow pro schvalování změn, posouzení dopadů, komunikaci a testování.

11.7.2. BAI02 – Řízená definice požadavků a BAI03 – Řízená identifikace a tvorba řešení: Zajišťují, aby změny vycházející z obchodních potřeb byly přezkoumány a implementovány bezpečným způsobem.

11.7.3. DSS01 – Řízený provoz: Podporuje průběžnou integritu systémů během provádění změn.

11.7.4. MEA01 a MEA03 – Monitorování, vyhodnocování a posuzování výkonnosti a souladu: Umožňuje průběžný dohled nad účinností Politiky řízení změn a jejím uplatňováním.