Change Management Policy

Verze dokumentu: 2026-07-25
Kategorie: bezpecnost

Provozovatel: Kibios s.r.o., IČO 29814995, se sídlem Brněnská 305/32, 664 44 Ořechov.
Kontakt: info@kibios.com
Online verze: https://kibios.com/pravni/change-management-policy

Change Management Policy Verze: 1.0 Účinnost od: 4. 8. 2026 Společnost: Kibios s.r.o., Brněnská 305/32, 664 44 Ořechov, IČO 298 14 995

1. Účel a rozsah

Tato Change Management Policy stanoví pravidla pro řízení změn v systémech, konfiguracích, infrastruktuře a službách, které Kibios s.r.o. provozuje nebo spravuje pro sebe a své klienty. Cílem je zajistit, aby změny byly:

- plánované a kontrolované,
- řádně schválené,
- bezpečné z hlediska dostupnosti, integrity a důvěrnosti,
- řádně zdokumentované a auditovatelné.

Policy se vztahuje na:

- produkční systémy a služby klientů spravované Kibios,
- interní systémy Kibios související s poskytováním služeb,
- konfigurace síťových prvků, serverů, aplikací a bezpečnostních technologií.

2. Typy změn

2.1 Standardní změna

- předem definovaná, opakující se změna s nízkým rizikem (např. pravidelné aktualizace, drobné konfigurační změny),
- má schválený postup (runbook) a typicky nevyžaduje individuální schválení pokaždé, jen evidenci.

2.2 Normální (projektová) změna

- změna s potenciálním dopadem na služby nebo architekturu (např. upgrade systému, nasazení nové komponenty),
- vyžaduje analýzu dopadu, plánování, schválení a často maintenance window.

2.3 Urgentní změna

- změna prováděná v reakci na incident nebo kritickou zranitelnost (např.

nouzový patch, dočasná mitigace),

- může být provedena ve zrychleném režimu, ale musí být dodatečně zdokumentována a schválena.

3. Proces řízení změn

Každá významná změna prochází minimálně těmito kroky: 3.1 Návrh změny

- identifikace potřeby změny (bezpečnost, funkčnost, výkon, podpora),
- popis změny, dotčených systémů, očekávaného přínosu a rizik.

3.2 Analýza dopadu

- posouzení dopadu na dostupnost, bezpečnost, integritu dat a klientské služby,
- v případě potřeby konzultace s bezpečnostním nebo infrastrukturním specialistou.

3.3 Schválení změny

- schválení odpovědnou osobou (např. technický lead, bezpečnostní lead, případně vedení),
- u změn s dopadem na klienta může být vyžadováno informování nebo souhlas klienta (dle smlouvy).

3.4 Plánování a provedení

- stanovení termínu (maintenance window),
- přesný postup kroků (implementační plán, možnost rollbacku),
- provedení změny podle plánu a zaznamenání průběhu.

3.5 Kontrola a uzavření

- ověření funkčnosti systémů po změně (testy, monitoring),
- potvrzení, že nedošlo k neplánovanému negativnímu dopadu,
- uzavření změny v evidenci (ticket, change request) a dokumentace výsledku.

4. Evidence změn

- Všechny významné změny jsou evidovány v change/ticket systému (ID změny, datum, autor, popis, dotčené systémy, typ změny, schvalovatel, stav).
- U standardních změn lze vést souhrnnou evidenci podle schválených postupů (např. měsíční aktualizační balíčky).
- U urgentních změn se zaznamenává důvod urgentního režimu, průběh a následné posouzení rizik.

5. Bezpečnostní a provozní zásady

- Změny v produkčních systémech se provádějí primárně v definovaném maintenance window, mimo špičku a po předchozí přípravě.
- Před významnou změnou se doporučuje vytvořit zálohu nebo snapshot, aby byl možný rollback v případě problémů.
- Změny v bezpečnostních mechanismech (firewall, WAF, IAM, MFA) podléhají zvýšené kontrole a schválení.
- Přístup k provádění změn mají pouze oprávněné osoby podle Access Control Policy.

6. Komunikace s klienty

- Změny, které mohou mít dopad na služby klienta (např. krátkodobá nedostupnost, změna konfigurace, upgrade), jsou klientovi oznámeny předem, podle MSA/SLA.
- U větších změn (např. migrace, změna architektury) může být přizván klient k plánování nebo odsouhlasení.
- V případě urgentních změn v reakci na incident je klient informován bez zbytečného odkladu, a následně dostane shrnutí provedených kroků.

7. Vztah k Incident Response a bezpečnosti

- Změny prováděné v rámci Incident Response (např. zablokování účtu, úprava firewall pravidel, nouzový patch) se evidují jako urgentní změny.
- Po stabilizaci situace se provádí jejich revize a případná úprava do standardního režimu (trvalé řešení zranitelnosti, optimalizace konfigurace).
- Change Management Policy je provázána s Incident Response Policy, Backup Policy, Logging & Monitoring Policy a Information Security Policy.

8. Audit a kontrola

- Proces řízení změn může být předmětem interního nebo klientského auditu.
- Z evidence změn musí být zřejmé, kdo změnu navrhl, schválil, provedl a ověřil.
- Nedodržení procesu řízení změn (např. nezdokumentované zásahy do produkce) může být považováno za porušení interních pravidel nebo smluvních ujednání.

9. Závěrečná ustanovení

- Change Management Policy může být aktualizována podle zkušeností z provozu, změn technologií nebo požadavků klientů.
- Aktuální verze této policy je dostupná interně a na vyžádání klientům, zejména v rámci bezpečnostních dotazníků nebo auditů.
- Policy je vyhotovena v českém jazyce; v případě překladu je rozhodující české znění.