Backup Policy

Verze dokumentu: 2026-07-25
Kategorie: incidenty

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/backup-policy

Backup 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 Backup Policy stanoví pravidla pro zálohování a obnovu dat v rámci služeb poskytovaných společností Kibios s.r.o. Cílem je zajistit dostupnost dat, minimalizovat ztrátu dat a umožnit obnovu po incidentu, chybě nebo selhání.

Backup Policy se vztahuje na:

- systémy a data klientů, u nichž je zálohování součástí smluvních služeb (MSA/SOW/SLA),
- interní systémy Kibios související s poskytováním služeb klientům,
- konfigurační data (nastavení serverů, sítí, aplikací), pokud jsou v rozsahu služeb.

2. Typy záloh

2.1 Full backup Kompletní záloha vybrané datové sady nebo systému (např. celý server, databáze, úložiště). 2.2 Incremental / differential backup Zálohy změn od poslední full zálohy (incremental) nebo od poslední zálohy daného typu (differential), používané pro efektivnější práci s kapacitou.

2.3 Configuration backup Zálohy konfiguračních souborů a nastavení (např. firewall, router, server, aplikace), zejména před a po významných změnách konfigurace. 2.4 Snapshoty Krátkodobé snapshoty systémů nebo virtuálních strojů pro rychlou obnovu v případě drobných incidentů nebo testovacích změn. Konkrétní typy záloh používané pro daného klienta jsou uvedeny v příslušném SOW/SLA.

3. Frekvence záloh

3.1 Produkční systémy klientů

- full backup minimálně 1× týdně,
- incremental/differential backups podle kritičnosti systému (např. denně nebo několikrát denně u vysoce kritických systémů).

3.2 Konfigurační data

- záloha při každé významné změně konfigurace,
- pravidelné zálohy v definovaných intervalech (např. 1× týdně) pro kritické prvky infrastruktury.

3.3 Interní systémy Kibios

- zálohování podle interního risk-based posouzení, s ohledem na dopad na poskytování služeb klientům.

Přesné parametry frekvence záloh pro jednotlivé systémy jsou definovány v SOW/SLA nebo interní dokumentaci Kibios.

4. Ukládání záloh

- Zálohy jsou ukládány na oddělené úložiště od produkčního prostředí (např.

dedikované backup servery, cloudové úložiště).

- Preferuje se víceúrovňové řešení (např. primární zálohy + offsite/geo-redundant zálohy).
- Zálohy jsou šifrovány (např. AES-256) a přístup k nim je řízen rolovým řízením přístupu (RBAC) a vícefaktorovou autentizací.
- Fyzické médium (pokud se používá) je ukládáno v zabezpečených prostorách s omezeným přístupem.

5. Doba uchování záloh

- Standardní retenční doba pro běžné provozní zálohy je typicky v rozmezí 30– 90 dní (dle SOW/SLA a požadavků klienta).
- Pro specifické systémy nebo typy dat (např. účetní data, logy) může být retenční doba delší podle právních předpisů nebo požadavků klienta.
- Po uplynutí retenční doby jsou zálohy bezpečně mazány nebo anonymizovány, v souladu s Data Retention Policy a právními požadavky (např. GDPR).

6. Testování obnovy

- Obnova ze záloh je pravidelně testována, minimálně 1× za definované období (např. 6–12 měsíců) pro kritické systémy.
- Test obnovy zahrnuje ověření, že záloha je použitelná, kompletní a že obnova proběhne v akceptovatelném čase (RTO).
- O testech obnovy se vede záznam (datum, systém, typ zálohy, výsledek, zjištěné problémy).

7. Přístup a bezpečnost

- K zálohám mají přístup pouze oprávněné osoby podle RBAC, a to v rozsahu nezbytném pro jejich práci (princip least privilege).
- Všechny přístupy k zálohám (prohlížení, stažení, obnova) jsou logovány.
- Přenos záloh mezi lokalitami nebo do cloudového úložiště probíhá výhradně šifrovaným kanálem (např. TLS, IPSec VPN).

8. Obnova po incidentu

- Při incidentu (např. ransomware, selhání hardware, chybná aktualizace) Incident Response tým ve spolupráci se správcem záloh:
  - posoudí rozsah poškození a určí vhodný časový bod zálohy pro obnovu,
  - ověří, že zvolená záloha neobsahuje kompromitované prvky (např.

malware), o provede obnovu v souladu s Incident Response Policy, s cílem minimalizovat downtimes a ztrátu dat (RTO/RPO dle SLA/SOW).

9. Vztah ke smluvním dokumentům

- Konkrétní parametry zálohování (frekvence, typy záloh, retenční doby, RPO/RTO) jsou stanoveny v Master Service Agreement (MSA), Service Level Agreement (SLA) a příslušném Statement of Work (SOW).
- Klient je informován o limitech zálohování (např. maximální možná ztráta dat mezi dvěma zálohami, RPO, RTO) a tyto limity jsou zohledněny v SLA.

10. GDPR a ochrana osobních údajů

- Pokud zálohy obsahují osobní údaje, zpracování těchto záloh a jejich ochrana se řídí Data Processing Agreement (DPA) a platnými právními předpisy (GDPR, zákon č. 110/2019 Sb.).
- Při mazání záloh je dbáno na bezpečné odstranění dat, aby nedošlo k neoprávněnému přístupu k osobním údajům.

11. Závěrečná ustanovení

- Backup Policy může být aktualizována podle změn technologií, právních předpisů, požadavků klientů nebo výsledků testů obnovy.
- Aktuální verze Backup Policy je dostupná klientům na vyžádání nebo prostřednictvím klientského portálu Kibios.
- Backup Policy je vyhotovena v českém jazyce; v případě překladu je rozhodující české znění.