Disaster Recovery Plan

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/disaster-recovery-plan

Disaster Recovery Policy / Plan (DRP) 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

Tento Disaster Recovery Policy / Plan (DRP) stanoví zásady a technické postupy pro obnovu systémů a služeb společnosti Kibios s.r.o. po závažném incidentu nebo katastrofě (výpadek datacentra, zničení infrastruktury, rozsáhlý kybernetický útok).

Cílem je:

- zajistit obnovení klíčových systémů a služeb v definovaných časech,
- minimalizovat dopad na klienty a provoz Kibios,
- koordinovat technickou obnovu v návaznosti na Incident Response a BCP.

DRP se vztahuje na:

- systémy a služby poskytované klientům (monitoring, správa, zálohy, ticketing),
- interní systémy nezbytné pro jejich podporu.

2. Vztah k Business Continuity a Incident Response

- Incident Response Policy řeší identifikaci a řízení incidentu.
- Business Continuity Policy (BCP) řeší kontinuitu provozu a náhradní režimy.
- DRP řeší technickou obnovu systémů po závažném incidentu/katastrofě.

Tyto dokumenty se navzájem doplňují a musí být konzistentní.

3. Kritické systémy a RTO/RPO

Pro každý kritický systém Kibios je interně stanoveno:

- RTO (Recovery Time Objective) – cílový čas, do kdy má být systém po katastrofě znovu funkční (např. 4 h, 24 h),
- RPO (Recovery Point Objective) – maximální tolerovatelná ztráta dat v čase (např. 15 min, 24 h),
- prioritní pořadí obnovy (co se obnovuje jako první).

Mezi kritické systémy patří zejména:

- monitoring platformy,

- ticketing / support systém,
- zálohovací systém a úložiště,
- VPN / remote access,
- interní koordinace (komunikační nástroje).

4. Scénáře katastrof

DRP uvažuje zejména tyto scénáře:

- úplný nebo dlouhodobý výpadek primárního datacentra/cloud lokace,
- rozsáhlý hardware failure (storage, compute cluster),
- závažný kybernetický útok (např. ransomware) postihující více systémů,
- fyzická katastrofa (požár, záplava) ovlivňující infrastrukturu.

Pro každý scénář jsou definovány technické postupy obnovy (runbooky) v interní dokumentaci.

5. Zálohy a replikace

Obnova je založena na:

- zálohách podle Backup Policy (full, incremental, configuration backups),
- případné replikaci dat do sekundární lokace (synchronní/asynchronní replikace),
- snapshot mechanismech.

DRP využívá:

- primární zálohy pro běžnou obnovu,
- offsite/geo-redundant zálohy pro scénáře úplného výpadku primárního prostředí.

6. Postup obnovy po katastrofě

Obecný postup:

1. Posouzení rozsahu škod – které systémy jsou nedostupné, jaký dopad na

klienty.

2. Rozhodnutí o aktivaci DRP a přechodu na obnovu (krizový tým/DRP owner).

3. Výběr vhodného recovery scénáře (obnova z lokálních záloh, obnova v

sekundární lokaci, přepnutí na záložní infrastrukturu).

4. Obnova klíčových systémů v pořadí podle priorit (monitoring, ticketing,

zálohy, VPN atd.).

5. Ověření funkčnosti a integrity po obnově (testy, kontrola dat, bezpečnostní

kontrola).

6. Postupné obnovení méně kritických služeb.

Konkrétní kroky (příkazy, technické detaily) jsou součástí interních DR runbooků.

7. Bezpečnostní aspekty obnovy

Při obnově po kybernetickém incidentu (např. ransomware):

- se volí takové zálohy, které nejsou kompromitované (časový bod před napadením),
- provádí se bezpečnostní kontrola obnovovaného prostředí (antimalware, konfigurace, přístupové údaje),
- mění se kompromitované přístupové údaje (hesla, klíče, certifikáty),
- aktivně se monitoruje obnovené prostředí pro včasné zachycení opakovaného útoku.

8. Testování DRP

- DRP je pravidelně testován (např. 1× ročně) formou:
  - částečných technických testů (obnova vybraného systému),
  - simulací přepnutí na sekundární lokaci,
  - tabletop cvičení pro krizový tým.
- Testy ověřují dosažitelnost RTO/RPO a funkčnost postupů.
- Výsledky testů jsou dokumentovány a využity pro aktualizaci DRP, Backup Policy a BCP.

9. Komunikace s klienty

- Při aktivaci DRP a závažné obnově jsou klienti informováni o:
  - povaze incidentu/katastrofy (v rozsahu vhodném pro sdělení),
  - dopadu na jejich služby,
  - očekávaných časech obnovy (RTO),
  - případných dočasných omezeních po obnově.
- Po dokončení obnovy může být klientům poskytnuto shrnutí (post-disaster / recovery report).

10. Vztah ke smluvním dokumentům

DRP je technickým doplněním smluvních ujednání, zejména:

- Master Service Agreement (MSA),
- Service Level Agreement (SLA) – dostupnost, reakční časy, RTO/RPO,
- Backup Policy, BCP, Incident Response Policy.

Konkrétní garantované úrovně služby (SLA) a limity (RTO/RPO) jsou vždy definovány ve smluvní dokumentaci; DRP popisuje interní postupy, jak těchto úrovní dosahovat.

11. Závěrečná ustanovení

- Disaster Recovery Policy / Plan je interním dokumentem Kibios; jeho shrnutí může být poskytováno klientům pro účely bezpečnostních dotazníků nebo auditů.
- DRP je aktualizován v návaznosti na změny infrastruktury, výsledky testů, zkušenosti z incidentů a regulatorní požadavky.
- Dokument je vyhotoven v českém jazyce; v případě překladu je rozhodující české znění.