
Plán obnovy po havárii (Disaster Recovery Plan – DRP)

Verze: 1.1

Platnost od: 27. 01. 2026

Garant procesu: Vedoucí IT / Fleet Manager

Vazba na ISO/IEC 27001:2022:

- A.5.29 – Informační bezpečnost při přerušení provozu
- A.5.30 – Připravenost ICT pro kontinuitu činností

---

1. Účel

Účelem DRP je zajistit řízenou, opakovatelnou a auditovatelnou obnovu kritických ICT služeb telemetrického systému po závažné havárii. Cílem je minimalizovat dobu nedostupnosti, ztrátu dat a dopad na zákazníky.

2. Rozsah

DRP se vztahuje na:

- backendové aplikační služby (API),
- databáze telemetrických dat,
- autentizační a autorizační služby,
- cloudovou infrastrukturu a síťové komponenty.

Upozornění: DRP se neaktivuje pro běžné incidenty řešitelné standardním Incident Managementem.

3. Cíle obnovy (RTO & RPO)

Pro kritické služby jsou stanoveny následující závazné cíle:

- **RTO (Recovery Time Objective):** Maximální přípustná doba nedostupnosti služby.

Cíl: ≤ 4 hodiny

- **RPO (Recovery Point Objective):** Maximální přípustná ztráta dat.

Cíl: ≤ 15 minut (real-time replikace + log shipping)

4. Klasifikace havárií

- **Úroveň 1 – Lokální výpadek:** Výpadek jednotlivé služby nebo komponenty. Řešeno automatickou redundancí / failoverem, DRP se neaktivuje.
- **Úroveň 2 – Regionální výpadek:** Nedostupnost cloudového regionu, síťového uzlu nebo storage. Aktivace DRP dle rozhodnutí Vedoucího IT.
- **Úroveň 3 – Katastrofická událost:** Masivní kompromitace (ransomware), ztráta kontroly nad prostředím. Okamžitá aktivace DRP + Incident Response.

5. Strategie obnovy

- **Vysoká dostupnost (HA):** Kritické služby běží v režimu Multi-AZ s automatickým failoverem.
- **Zálohování a ochrana dat:** * geograficky oddělené zálohy,
    - imutabilní úložiště (WORM),
    - oddělené zálohovací účty bez admin přístupu k produkci.
- **Infrastruktura jako kód (IaC):** Kompletní infrastruktura je obnovitelná pomocí verzovaných skriptů (Terraform / CloudFormation).

6. Aktivace a postup obnovy

1. **Detekce:** Monitoring (např. Prometheus/Grafana) detekuje kritický stav.
2. **Rozhodnutí o aktivaci:** Vedoucí IT vyhodnotí rozsah a rozhodne o aktivaci DRP.
3. **Svolání DRP týmu:** IT Administrátor, Lead Developer, Fleet Manager.
4. **Volba scénáře obnovy:** Failover / rebuild infrastruktury / obnova dat.
5. **Technická obnova:** Spuštění IaC, obnova databází, kontrola certifikátů a klíčů.
6. **Ověření funkčnosti:** Test integrity dat, dostupnosti API a komunikace s jednotkami.

7. Testování a údržba DRP

DRP je považován za platný pouze při pravidelném testování:

- **Tabletop cvičení:** Simulace scénáře obnovy – 1× za 6 měsíců.
- **Technický test obnovy:** Reálná obnova ze záloh do testovacího prostředí – 1× ročně.

Výsledky testů jsou dokumentovány včetně nápravných opatření.

8. Odpovědnosti

- **Vedoucí IT:** Schvaluje DRP, rozhoduje o aktivaci, odpovídá za splnění RTO/RPO.
- **IT Administrátor:** Provádí technickou obnovu, spravuje zálohy a monitoring.
- **Fleet Manager:** Komunikuje se zákazníky, koordinuje informace o dostupnosti služeb.

9. Auditní důkazy

Organizace uchovává:

- záznamy o testech DRP a jejich výsledcích,
- konfiguraci zálohování a logy úspěšnosti,
- incidentní reporty s vazbou na aktivaci DRP,
- post-mortem analýzy po reálných událostech.