Plán kontinuity činností (Business Continuity Plan – BCP)

Verze: 1.1

Platnost od: 27. 01. 2026

Garant procesu: Fleet Manager / CEO

Vazba na ISO/IEC 27001:2022:

- A.5.29 – Informační bezpečnost v rámci řízení kontinuity činností

---

1. Účel

Účelem BCP je zajistit schopnost organizace udržet provoz klíčových činností (monitoring a telemetrie lokomotiv, technická podpora zákazníků) i při závažném narušení běžného provozu, a to s řízeným dopadem na zákazníky a obchodní závazky.

2. Rozsah

BCP se vztahuje na:

- provozní a obchodní činnosti,
- lidské zdroje a organizační strukturu,
- komunikaci se zákazníky a dodavateli.

Vazba na IT: Technická obnova ICT je řešena samostatným *Plánem obnovy po havárii (DRP)*, na který BCP přímo odkazuje.

3. Analýza dopadů na činnosti (BIA)

Na základě BIA byly identifikovány následující kritické procesy:

Kritický proces	**Dopad přerušení**	**MTPD (Max. přípustná doba)**
Příjem telemetrických dat	Ztráta přehledu o poloze a stavu vozidel	4 hodiny
Technická podpora (L1/L2)	Nemožnost řešit provozní poruchy	8 hodin

Kritický proces	Dopad přerušení	MTPD (Max. přípustná doba)
Správa vozového parku	Nemožnost vzdálené konfigurace jednotek	24 hodin
Fakturace a administrativa	Finanční a smluvní dopady	5 pracovních dnů

4. Scénáře narušení a strategie kontinuity

- **Scénář A – Nedostupnost pracoviště (požár, povodeň, výpadek energií):**
  - Okamžitý přechod na práci na dálku (Home Office).
  - Využití cloudových nástrojů dostupných přes VPN.
  - Postup dle *Směrnice pro práci z domova*.
- **Scénář B – Nedostupnost klíčových osob:**
  - Zastupitelnost rolí (multi-skilling).
  - Dokumentované postupy a přístupy uložené v interní znalostní bázi.
  - Omezení závislosti na jedné osobě u kritických procesů.
- **Scénář C – Výpadek klíčového dodavatele (např. gxtdm.eu):**
  - Lokální dostupnost konfiguračních dat a dokumentace.
  - Smluvně definované SLA a eskalační mechanismy.
  - Možnost přechodu na náhradní řešení v přiměřeném čase.

5. Aktivace BCP a krizové řízení

1. **Vyhlášení narušení:** Fleet Manager nebo CEO vyhodnotí situaci a rozhodne o aktivaci BCP.
2. **Svolání krizového řízení:** Zapojení vedení, provozu a IT (včetně vazby na DRP).
3. **Zajištění kontinuity činností:** Aktivace náhradních pracovních režimů, rolí a postupů.
4. **Monitoring stavu:** Pravidelné vyhodnocování stability provozu a dopadů.
5. **Návrat do standardního režimu:** Řízený přechod zpět po odstranění příčiny narušení.

6. Krizová komunikace

- **Interní komunikace:** Fleet Manager informuje zaměstnance prostřednictvím krizového kanálu.
- **Externí komunikace:** CEO nebo Fleet Manager komunikuje se zákazníky. Informace musí být věcné, konzistentní a s realistickým odhadem doby nápravy.

7. Údržba a testování BCP

- **Přezkum:** Minimálně 1× ročně nebo po závažném incidentu.
- **Testování:** Simulace vybraných scénářů (tabletop exercise).
- **Školení:** Zaměstnanci jsou seznámeni se svou rolí v rámci BCP.

8. Odpovědnosti

- **CEO:** Celková odpovědnost za kontinuitu podnikání, schvalování zásadních rozhodnutí a zdrojů.
- **Fleet Manager:** Operativní řízení BCP, komunikace se zákazníky.
- **Vedoucí IT:** Zajištění technické kontinuity, koordinace s DRP.

9. Auditní důkazy

Organizace uchovává:

- dokumentaci BIA,
- záznamy o testování BCP,
- aktuální krizové kontakty,
- záznamy o aktivaci BCP a přijatých opatřeních.