Beredskap og kontinuitet

Versjon 1.0 · 29. mai 2026 · Backup, RTO/RPO, hendelseshåndtering og fallback-prosedyrer

Kort fortalt: Daglig kryptert backup med 7 dagers oppbevaring. Recovery time objective (RTO): 4 timer. Recovery point objective (RPO): 24 timer. Mobil-app fungerer offline for å vise allerede-godkjente rekvisisjoner i butikk.

1. Formål og virkeområde

Beskriver hvordan DigiReq håndterer tap av tilgjengelighet, datatap, og krise-scenarier. Komplementerer sikkerhetsside (tekniske tiltak) og SLA-en (kontraktsmessige mål).

2. Mål for gjenoppretting

MÅL	VERDI	BESKRIVELSE
RTO (Recovery Time Objective)	4 timer	Maks tid fra hendelses-start til tjenesten er operasjonell igjen
RPO (Recovery Point Objective)	24 timer	Maks datatap målt i tid — tilsvarer 1 dags rekvisisjoner i verste fall
MTTR (Mean Time To Repair)	2 timer (mål)	Gjennomsnittlig tid for å rette en feil
MTBF (Mean Time Between Failures)	30 dager (mål)	Forventet tid mellom uventede feil

3. Backup-strategi

3.1 Database (PostgreSQL)

- **Frekvens:** Hetzner-snapshot daglig kl. 03:00 norsk tid
- **Oppbevaring:** 7 dager rullerende
- **Lokasjon:** Hetzner Helsinki-datasenter (samme som produksjon)
- **Kryptering:** Hetzner-snapshots er kryptert i hvile
- **Tilgang:** kun super_admin (Markus) via Hetzner-konto

3.2 Applikasjons-kode

- Versjonskontroll i privat GitHub-repo med 2FA på alle utviklere
- Hver deploy lager git-tag som rollback-punkt
- Eksisterer i minst tre kopier: utvikler-maskin, GitHub, produksjons-VPS

3.3 Konfigurasjon og secrets

- `.env`-fil på VPS sikkerhetskopieres ved hver endring til kryptert offsite-lagring
- SSH-nøkler og API-tokens dokumentert i Påvakt AS' sikre dokumentasjon

3.4 Audit-logg

- Append-only i database (overlever sammen med database-backup)
- Brukes ved delvis datatap for å rekonstruere kritiske handlinger

3.5 Hva som IKKE backes opp

- OTP-koder (TTL 5 min, ikke vits)
- Session-tokens (regenereres ved pålogging)
- Push-notifikasjons-payload (ikke persistent stat)

4. Gjenopprettingsprosedyrer

4.1 Database-korrupsjon eller -tap

1. Hent siste gode Hetzner-snapshot (≤ 24 t gammel)
2. Opprett ny PostgreSQL-instans fra snapshot
3. Pek `DATABASE_URL` i `.env` mot ny instans
4. Restart `digireq-api.service`

5. Valider med `/health`-endepunkt (skal returnere `db: true`)
6. Manuell sanity-sjekk: telle requisitions for 3-5 kunder mot deres egen statistikk

Estimat: 1-2 timer til funksjonell tjeneste; opp til 4 timer ved store data-volum.

4.2 VPS-utfall (Hetzner Helsinki nede)

1. Vurder om utfallet er forventet kort (< 1 t) — vent ut
2. Ved lengre utfall: provisjoner ny Hetzner-VPS i annet datasenter (typisk Nürnberg)
3. Kjør `deploy/install.sh` med Postgres-passord
4. Restore fra siste tilgjengelige database-snapshot
5. Oppdater DNS (Cloudflare) for `api.digireq.no` til ny IP
6. Vente på DNS-propagering (TTL 5 min)

Estimat: 3-4 timer; lengre hvis Hetzner-API selv er nede.

4.3 Domain/DNS-utfall (Cloudflare)

- Cloudflare er sjelden nede; ved utfall mister vi DDoS-beskyttelse, men tjenesten fungerer hvis vi peker direkte til VPS-IP
- Fallback-prosedyre: bytte til alternativ DNS-leverandør (one.com eller manuell `A`-record)

4.4 SMS-leverandør-utfall (46elks)

- Brukere kan ikke logge inn med OTP under utfallet
- Allerede-pålogde brukere fortsetter å fungere (JWT-tokens varer 60 min)
- Admins med Entra ID-pålogging kan logge inn uavhengig av 46elks
- Mobil-appen viser allerede-godkjente rekvisisjoner offline (cached) — handelen i butikk kan fullføres
- Fallback til alternativ SMS-leverandør vurderes når kunde-base rettferdiggjør kompleksiteten

4.5 Push-utfall (Apple APNs / Google FCM / Expo)

- Push-notifikasjoner ikke leveres — godkjenner ser ikke ny rekvisisjon før app åpnes
- App poller tilstand ved focus + foreground; pending-listen er primær kilde
- Tjenesten fungerer ellers som normalt

5. Hendelseshåndtering

5.1 Klassifisering

Hendelser klassifiseres etter samme skala som SLA §4:

- **Alvorlighet 1 — Kritisk:** komplett produksjonsstopp, brudd på data, sikkerhets-insident
- **Alvorlighet 2 — Alvorlig:** kjernefunksjon utilgjengelig
- **Alvorlighet 3 — Moderat:** degradering, ikke-blokkerende
- **Alvorlighet 4 — Lav:** kosmetiske feil

5.2 Respons-prosedyre (Alvorlighet 1)

1. **0-15 min:** deteksjon (UptimeRobot-varsel eller kundetilbakemelding)
2. **15-30 min:** verifikasjon — sjekk `/health`, logger, gjennomgå nylige deploys
3. **30-60 min:** aktiv arbeids-start, kommunikasjon til pågående kunder via e-post
4. **60-240 min:** løsning eller workaround
5. **+24 t:** sikkerhetsbrudd-varsel sendes hvis personopplysninger er eksponert (per DPA §10)
6. **+7 d:** post-mortem-rapport leveres berørte kunder

5.3 Sikkerhetsbrudd

Ved mistanke om sikkerhetsbrudd følges sikkerhetsbrudd-prosedyren beskrevet i /sikkerhet § 10. Datatilsynet varsles innen 72 timer hvis personopplysninger er eksponert.

6. Kommunikasjon under hendelser

6.1 Kanaler

- **E-post til kundens kontaktperson** ved Alvorlighet 1-2
- **Status-side** oppdateres med pågående hendelser (kommer)
- **Sikkerhets-kontakt:** sikkerhet@digireq.no (24/7 monitorert)

6.2 Stakeholder-matriks

STAKEHOLDER	NÅR VARSLES	KANAL
Kundens kontaktperson	Alvorlighet 1-2 ved start + ved løsning	E-post
Kundens sikkerhets-team	Sikkerhets-insident	E-post + telefon hvis tilgjengelig
Datatilsynet	Personopplysnings-brudd	Online-skjema, innen 72 t
Sub-prosessorer	Bare hvis deres tjeneste er årsaken	E-post/portal
Offentligheten	Sjelden — bare ved store, langvarige hendelser	digireq.no/status

7. Forretningskontinuitet (BCP)

7.1 Plattform-konsentrasjon (bus-faktor)

I dag har én person (Markus Eriksson) operativ tilgang til produksjon. Dette er en kjent risiko (ROS §3.15). Beredskap:

- Komplett dokumentasjon i versjonskontrollert driftsinstruks (deploy-skript, infrastruktur-config)
- SSH-nøkler og credentials lagret i Påvakt AS' sikre dokumentasjon
- Beredskapskontakt: Medeier i Påvakt AS – Digireq har instrukser
- Reduseres ved første ansettelse / co-founder

7.2 Konkurs-scenario (Påvakt AS)

Ved Påvakt AS' konkurs eller rekonstruksjon har kunden rett til:

- Eksport av all data i CSV/JSON innen 30 dager (jf. SaaS-avtale §15)
- Oppsigelse uten oppsigelsestid (jf. SaaS-avtale §5.4)
- Eskaleringsvei via bostyrer hvis driften er overtatt

Source-escrow er ikke etablert i dag, men kan diskuteres ved store kommersielle avtaler.

8. Testing

- **Backup-restore-test:** kvartalsvis manuell restore til staging-miljø
- **Failover-test:** ad-hoc når større endringer skjer
- **Beredskaps-øvelse:** årlig table-top-øvelse av Alvorlighet 1-scenario
- **Tester logges** i intern test-rapport, tilgjengelig for kunde-revisjon på forespørsel

9. Endringer og oppdateringer

Beredskapsplanen revideres minst årlig og ved vesentlige endringer i infrastruktur eller arkitektur. Endringer logges nedenfor.

Endringslogg

- **1.0 (29. mai 2026):** Første publiserte versjon. RTO 4 t, RPO 24 t. Daglig Hetzner-snapshot, 7 d retention.

Dokument-versjon 1.0 · Sist oppdatert 29. mai 2026 · sikkerhet@digireq.no

OM LEVERANDØREN

Tjenesten DigiReq leveres av **Påvakt AS** (org.nr. **937 620 187**), heretter omtalt som «Leverandør». DigiReq er registrert som virksomhet under Påvakt AS (**Digireq**, org.nr. **937 700 539**). Avtaler signeres med Påvakt AS som juridisk enhet; EHF-fakturaer fra DigiReq utstedes på Digireqs virksomhets-org-nr.

Kontakt: info@digireq.no · Sikkerhet: sikkerhet@digireq.no · Personvern: personvern@digireq.no