Contingency Plan

Beredskapsplan — Drop

Dokument-ID: BCP-DROP-001 **Versjon:** 1.0 **Dato:** 12. februar 2026 **Eier:** ALAI Holding AS, org.nr. 932 516 136 **Klassifisering:** Intern — Fortrolig **Regulatorisk grunnlag:** DORA (EU) 2022/2554 art. 11, Finanstilsynets IKT-forskrift

---

1. Innledning

1.1 Formål

Denne beredskapsplanen sikrer at Drop-tjenesten kan opprettholde eller raskt gjenopprette kritiske funksjoner ved vesentlige forstyrrelser. Planen er utarbeidet i henhold til DORA artikkel 11 om forretningskontinuitet og krisekommunikasjon.

1.2 Virkeområde

Planen dekker:

- Alle IKT-systemer som understøtter Drop-tjenesten
- Alle forretningsprosesser knyttet til betalingsbehandling
- Tredjepartsleverandører som er kritiske for tjenesteleveransen
- Kommunikasjon med berørte parter under og etter hendelser

1.3 Definisjoner

Begrep	Definisjon
RTO (Recovery Time Objective)	Maksimal akseptabel nedetid
RPO (Recovery Point Objective)	Maksimalt akseptabelt datatap (tidsperiode)
MTPD (Maximum Tolerable Period of Disruption)	Maksimal periode tjenesten kan være nede
BIA (Business Impact Analysis)	Analyse av konsekvenser ved bortfall

---

2. Business Impact Analysis (BIA)

2.1 Kritiske forretningsprosesser

Prosess	Kritikalitet	RTO	RPO	MTPD	Konsekvens ved bortfall
Betalingsbehandling (PISP)	Kritisk	1 time	0 (null datatap)	4 timer	Brukere kan ikke gjennomføre betalinger, omdømmetap, regulatorisk risiko
Kontoinformasjon (AISP)	Viktig	4 timer	1 time	8 timer	Brukere kan ikke se saldo, begrenset funksjonalitet
Utenlandsoverføring (remittance)	Kritisk	2 timer	0	8 timer	Forsinkede overføringer, kundetap
QR-betalinger	Kritisk	1 time	0	4 timer	Forhandlere kan ikke motta betaling
Brukerautentisering (BankID)	Kritisk	30 min	N/A	2 timer	Ingen kan logge inn, total tjenestestans
Kundeservice	Viktig	8 timer	4 timer	24 timer	Kunder kan ikke få hjelp, klagebehandling forsinkes
KYC/AML-kontroll	Viktig	4 timer	1 time	12 timer	Nye kunder kan ikke registrere seg
Rapportering og compliance	Standard	24 timer	4 timer	48 timer	Regulatorisk rapportering forsinkes
Push-varsler	Standard	8 timer	N/A	24 timer	Brukere mottar ikke transaksjonsvarsler

2.2 Kritiske IKT-systemer

System	Avhengigheter	Redundans	RTO

Betalingsmotor	Database, Open Banking API	Aktiv-aktiv	1 time
Database (PostgreSQL)	Lagring, nettverk	Replikering, automatisk failover	15 min
Open Banking-gateway	Ekstern leverandør	Sekundær leverandør (varm standby)	2 timer
BankID-integrasjon	BankID Norge AS	BankID HA-oppsett	Avhengig av BankID
API-gateway	CDN, lastbalansering	Multiregion	30 min
Appservere	Container-orkestrator	Autoskalering, multinode	15 min
Meldingskø	Broker-klynge	Klynge med replikering	15 min
Cache	Redis-klynge	Replikering	5 min
Overvåkingssystem	SIEM, logger	Separat infrastruktur	1 time

2.3 Avhengigheter til tredjeparter

Leverandør	Tjeneste	Kritikalitet	Alternativ
Open Banking-leverandør	PSD2 PISP/AISP	Kritisk	Sekundær leverandør med varm standby
BankID Norge AS	Autentisering	Kritisk	Ingen alternativ (nasjonal eID) — degradert modus
Skyinfrastrukturleverandør	Hosting	Kritisk	Multiregion-oppsett, alternativ region
Korrespondentbanker	Remittance	Kritisk	Flere partnere per korridor
CDN-leverandør	Innholdslevering	Viktig	Sekundær CDN konfigurert
E-postleverandør	Transaksjonelle e-poster	Standard	Sekundær leverandør

---

3. Scenarioer og responsstrategier

3.1 Scenario S1: Fullstendig datasentertap

Beskrivelse: Primær hosting-region er utilgjengelig (brann, naturkatastrofe, regionalt strømbrudd).

Responsstrategi:

1. Automatisk failover til sekundær region (konfigurasjon: aktiv-passiv)

2. DNS-oppdatering peker trafikk til sekundær region (TTL: 60 sekunder)
3. Database failover til standby-replikka i sekundær region
4. Verifiser tjenestekvalitet i sekundær region
5. Informer brukere via push-varsling og statusside
6. Initier gjenoppbygging av primær region etter at hendelsen er løst

RTO: 2 timer | **RPO:** 5 minutter (asynkron replikering)

3.2 Scenario S2: Databasekorrupsjon

Beskrivelse: Primær database korruptert (programvarefeil, menneskelig feil, ondsinnet aktivitet).

Responsstrategi:

1. Stopp skriving til korrupt database umiddelbart
2. Aktiver skrivebeskyttet modus (brukere kan se, men ikke utføre transaksjoner)
3. Identifiser tidspunkt for korrupsjon
4. Gjenopprett fra siste gyldige backup + WAL-replay til tidspunkt før korrupsjon
5. Verifiser dataintegritet
6. Gjenoppta normal drift
7. Gjennomfør rotårsaksanalyse

RTO: 1 time | **RPO:** 0 (med WAL-replay)

3.3 Scenario S3: Open Banking-leverandør nede

Beskrivelse: Primær Open Banking-leverandør er utilgjengelig.

Responsstrategi:

1. Automatisk failover til sekundær Open Banking-leverandør
2. Aktiver hurtigbuffer for kontoinformasjon (siste kjente saldo, maks 1 time gammel)
3. Informer brukere om mulig forsinkelse i betalingsbehandling
4. Kontakt primær leverandør for statusoppdatering
5. Logg alle transaksjoner som venter på behandling
6. Gjenoppta mot primær leverandør når tilgjengelig

RTO: 30 minutter (failover) | **RPO:** 0

3.4 Scenario S4: BankID utilgjengelig

Beskrivelse: BankID-infrastrukturen er nede nasjonalt.

Responsstrategi:

1. Aktiver degradert modus: eksisterende innloggede brukere kan fullføre pågående transaksjoner
2. Ny autentisering er ikke mulig — informer brukere via app og statusside
3. Kontakt BankID Norge AS for statusoppdatering
4. Forleng sesjonstimeout midlertidig (fra 15 min til 60 min) for aktive sesjoner
5. Logg alle forsøk på autentisering for senere analyse
6. Gjenoppta normal drift når BankID er tilbake

RTO: Avhengig av BankID | **Mitigering:** Forlengede sesjoner for aktive brukere

3.5 Scenario S5: Cyberangrep (ransomware/DDoS)

Beskrivelse: Målrettet cyberangrep mot Drop-infrastrukturen.

Responsstrategi:

1. Aktiver hendelsesresponsplan (se `hendelseshaandtering.md`)
2. Isoler berørte systemer
3. Aktiver DDoS-mitigering på CDN/WAF-nivå
4. Ved ransomware: gjenopprett fra sikkerhetskopier (ingen betaling)
5. Eskaler til Finanstilsynet innen 4 timer
6. Informer berørte brukere
7. Engasjer ekstern hendelsesresponsteam ved behov

RTO: 4 timer (DDoS), 8 timer (ransomware) | **RPO:** 0 (fra backup)

3.6 Scenario S6: Nøkkelpersonavhengighet

Beskrivelse: Kritisk personell er utilgjengelig (sykdom, fratredelse).

Responsstrategi:

1. Alle kritiske roller har stedfortreder dokumentert
2. Alle prosedyrer er dokumentert og tilgjengelig
3. Alle tilganger er rollebasert (ikke personbasert)
4. Tredjepartsavtaler har kontaktlister med flere kontaktpunkter
5. Eskaleringsmatrisen oppdateres ved personalendringer

---

4. Gjenopprettingsprosedyrer

4.1 Generell gjenopprettingsprosess

```
1. OPPDAGE  → Automatisert overvåking eller manuell varsling
2. VURDERE  → Kategoriser hendelsen (S1-S6), identifiser omfang
3. ESKALER  → Aktiver beredskapsorganisasjon iht. eskaleringstrinn
4. HÅNDTERE → Utfør scenariospesifikk respons
5. VERIFISER → Kontroller at gjenoppretting er vellykket
6. INFORMER → Oppdater berørte parter om status
7. NORMALISER → Gjenoppta normal drift
8. ANALYSER → Rotårsaksanalyse og forbedring
```

4.2 Database-gjenoppretting

Forutsetninger: PostgreSQL med streaming replikering og WAL-arkivering.

1. Identifiser siste gyldige tidspunkt
2. Stopp applikasjonsservere
3. Gjenopprett database fra siste fullsikkerhetskopi
4. Replay WAL-segmenter frem til identifisert tidspunkt (PITR)
5. Verifiser dataintegritet med sjekksumkontroll
6. Kjør integrasjonstester mot gjenopprettet database
7. Start applikasjonsservere i kontrollert rekkefølge
8. Overvåk tett de neste 24 timene

4.3 Infrastruktur-gjenoppretting

1. Verifiser at infrastruktur-som-kode (IaC) er tilgjengelig
2. Provisionér ny infrastruktur i sekundær region/sone
3. Deploy siste gyldige applikasjonsversjon
4. Gjenopprett databaser (se 4.2)
5. Konfigurer nettverksruter og lastbalansering
6. Verifiser tjenestekvalitet
7. Oppdater DNS

---

5. Kommunikasjonsplan

5.1 Intern kommunikasjon

Eskaleringstrinn	Kriterium	Varsler	Metode	Innen
Trinn 1	Degradert tjeneste	Driftsteam	Automatisk varsling	Umiddelbart
Trinn 2	Kritisk tjeneste nede	Driftsteam + CISO	Telefon + e-post	15 min
Trinn 3	Fullstendig tjenestestans > 1 time	+ Daglig leder	Telefon	30 min
Trinn 4	Tjenestestans > 4 timer eller databrudd	+ Styreleder	Telefon	1 time

5.2 Ekstern kommunikasjon

Mottaker	Kriterium	Metode	Innen
Brukere	Tjenestestans > 15 min	Push-varsling, statusside	30 min
Forhandlere	QR-betalinger nede > 15 min	E-post, telefon (store)	30 min
Finanstilsynet	Alvorlig IKT-hendelse (DORA art. 19)	Varslingsskjema	4 timer
Datatilsynet	Personvernbrudd	Avviksskjema	72 timer
Open Banking-leverandør	Integrasjonsproblemer	Avtalt kanal	Umiddelbart
BankID Norge AS	Autentiseringsproblemer	Avtalt kanal	Umiddelbart
Media	Ved offentlig oppmerksomhet	Pressekontakt	Koordinert

5.3 Statusside

- Ekstern statusside oppdateres ved alle hendelser som påvirker brukere
- Automatisert oppdatering fra overvåkingssystem
- Manuell oppdatering ved komplekse hendelser
- Historikk over alle hendelser tilgjengelig

5.4 Maler for kommunikasjon

Ferdigformulerte maler for:

- Planlagt vedlikehold
- Uplanlagt tjenesteavbrudd
- Gjenoppretting bekreftet

- Sikkerhetsbrudd (til brukere)
- Regulatorisk varsling (Finanstilsynet)

---

6. Beredskapsorganisasjon

6.1 Roller og ansvar

Rolle	Ansvar	Stedfortreder
Beredskapsleder (daglig leder)	Overordnet beslutningsansvar, ekstern kommunikasjon	CTO
Teknisk leder (CTO)	Teknisk gjenoppretting, koordinering av driftsteam	Senior utvikler
Kommunikasjonsansvarlig	Intern/ekstern kommunikasjon, statusoppdateringer	Daglig leder
CISO	Sikkerhetsvurdering, koordinering med myndigheter	CTO
Compliance-ansvarlig	Regulatorisk vurdering, varsling til tilsyn	CISO
Driftsleder	Utfører gjenopprettingsprosedyrer	Backup driftsteam

6.2 Kontaktliste

Oppdatert kontaktliste med:

- Mobilnummer (primær og sekundær)
- E-postadresse
- Alternativ kontaktmetode
- Oppdateres minimum kvartalsvis

6.3 Aktivering av beredskap

Beredskap aktiveres når:

- Automatisert overvåking utløser P1- eller P2-alarm
- Manuell vurdering tilsier aktivering
- Finanstilsynet krever det
- Tredjepartsleverandør rapporterer kritisk hendelse

---

7. Testing og øvelser

7.1 Testprogram

Testtype	Frekvens	Omfang	Ansvarlig
Tabletop-øvelse	Kvartalsvis	Gjennomgang av scenarioer med beredskapsorganisasjon	Beredskapsleder
Failover-test	Halvårlig	Teknisk failover til sekundær region	CTO
Database-gjenoppretting	Halvårlig	Full gjenoppretting fra backup	Driftsleder
Kommunikasjonstest	Kvartalsvis	Test av kontaktlister og eskaleringsprosedyrer	Kommunikasjonsansvarlig
Full beredskapsøvelse	Årlig	Ende-til-ende simulering inkl. tredjeparter	Beredskapsleder

7.2 Testdokumentasjon

Alle tester dokumenteres med:

- Dato og deltakere
- Scenario som ble testet
- Faktisk RTO/RPO oppnådd
- Avvik fra planlagte prosedyrer
- Forbedringstiltak med frist og ansvarlig

7.3 Oppdatering etter test

- Beredskapsplanen oppdateres innen 30 dager etter test/øvelse
- Identifiserte svakheter utbedres innen 60 dager
- Neste test planlegges

---

8. Vedlikehold av planen

8.1 Gjennomgangsfrekvens

- **Årlig:** Full gjennomgang av beredskapsplanen
- **Kvartalsvis:** Oppdatering av kontaktlister
- **Ved vesentlige endringer:** Ny leverandør, ny teknologi, organisasjonsendring
- **Etter hendelser:** Revideres basert på lærdommer
- **Etter øvelser:** Oppdateres basert på testresultater

8.2 Ansvar for vedlikehold

Aktivitet	Ansvarlig	Frekvens
Oppdatering av kontaktlister	Alle rolleinnehavere	Kvartalsvis
Teknisk gjennomgang	CTO	Halvårlig
Full plangjennomgang	Beredskapsleder	Årlig
Godkjenning	Daglig leder	Ved endring

8.3 Distribusjon

- Planen distribueres til alle i beredskapsorganisasjonen
- Tilgjengelig offline (utskrift) hos beredskapsleder og CTO
- Lagret i versjonskontroll med endringshistorikk
- Kopier hos tredjepartsleverandører ved behov

---

9. Samsvar med DORA artikkel 11

Denne beredskapsplanen er utarbeidet i henhold til kravene i DORA artikkel 11:

DORA-krav	Dekning i planen
Art. 11(1): IKT-kontinuitetspolicy	Hele dokumentet
Art. 11(2): BIA for kritiske funksjoner	Seksjon 2
Art. 11(3): Responsstrategier	Seksjon 3
Art. 11(4): Gjenopprettingsprosedyrer	Seksjon 4
Art. 11(5): Kommunikasjonsplan	Seksjon 5
Art. 11(6): Testing	Seksjon 7
Art. 11(7): Gjennomgang og oppdatering	Seksjon 8
Art. 11(8): Hendelsesrespons	Ref. hendelseshaandtering.md
Art. 11(9): Tredjepartsavhengigheter	Seksjon 2.3

10. Versjonshistorikk

Versjon	Dato	Endring	Godkjent av
1.0	12.02.2026	Opprinnelig dokument	_____

Vedlegg

Vedlegg A: Kontaktliste beredskapsorganisasjon

Separat dokument — fortrolig.

Vedlegg B: Sjekklister per scenario

Operasjonelle sjekklister — oppbevares hos driftsteam.

Vedlegg C: Oversikt over sikkerhetskopier og gjenopprettingspunkter

Teknisk dokumentasjon — vedlikeholdes av driftsteam.

Beredskapsplanen er eid av beredskapsleder og godkjent av styret i ALAI Holding AS. Planen revideres minimum årlig og etter enhver vesentlig hendelse.

Revision #5
Created 2026-02-18 08:44:40 UTC by John
Updated 2026-05-25 07:24:37 UTC by John