Policies & Internal Controls

- ICT Security Policy
- Internal Controls
- Incident Management
- Contingency Plan
- Complaints Handling

ICT Security Policy

IKT-sikkerhetspolicy — Drop

Dokument-ID: IKT-SEC-DROP-001 **Versjon:** 1.0 **Dato:** 12. februar 2026 **Eier:** ALAI Holding AS, org.nr. 932 516 136 **Klassifisering:** Intern **Gjelder for:** Alle systemer, ansatte og leverandører tilknyttet Drop-tjenesten **Regulatorisk grunnlag:** DORA (EU) 2022/2554, IKT-forskriften, GDPR

---

1. Innledning

1.1 Formål

Denne policyen etablerer rammeverket for IKT-sikkerhet i Drop-tjenesten. Policyen sikrer at ALAI Holding AS oppfyller kravene i Digital Operational Resilience Act (DORA), forordning (EU) 2022/2554, samt Finanstilsynets IKT-forskrift og øvrig relevant regulering.

1.2 Virkeområde

Policyen gjelder for:

- Alle IKT-systemer som understøtter Drop-tjenesten
- Alle ansatte, konsulenter og tredjepartsleverandører med tilgang til Drop-systemer
- All behandling av data i Drop-tjenestens infrastruktur
- Open Banking-integrasjoner (PSD2 PISP/AISP)
- BankID-integrasjon

1.3 Regulatorisk bakgrunn

Regulering	Relevante artikler	Beskrivelse
DORA (EU) 2022/2554	Art. 5-16	IKT-risikostyring
DORA (EU) 2022/2554	Art. 17-23	IKT-relaterte hendelser
DORA (EU) 2022/2554	Art. 24-27	Digital operasjonell resiliens-testing
DORA (EU) 2022/2554	Art. 28-30	IKT-tredjepartsrisiko
GDPR (EU) 2016/679	Art. 32	Sikkerhet ved behandling

Regulering	Relevante artikler	Beskrivelse
IKT-forskriften	Hele	Finanstilsynets krav til IKT
PSD2 (EU) 2015/2366	Art. 95-98	Sikkerhet ved betalingstjenester

---

2. IKT-styring og organisering — DORA art. 5

2.1 Ledelsesansvar

Selskapets ledelse har det overordnede ansvaret for IKT-risikostyring, jf. DORA artikkel 5(2). Dette innebærer:

- Godkjenning av IKT-sikkerhetspolicy og vesentlige endringer
- Allokering av tilstrekkelige ressurser til IKT-sikkerhet
- Regelmessig gjennomgang av IKT-risikostatus (minimum kvartalsvis)
- Gjennomføring av opplæring i IKT-sikkerhet (minimum årlig)

2.2 Organisering

Rolle	Ansvar
Daglig leder	Overordnet ansvar for IKT-sikkerhet
IKT-sikkerhetsansvarlig (CISO)	Operativt ansvar for sikkerhetspolicy og -tiltak
Personvernombud (DPO)	Personvernrelatert IKT-sikkerhet
Driftsteam	Implementering og vedlikehold av sikkerhetstiltak
Utviklingsteam	Sikker utvikling (DevSecOps)

2.3 Rapportering

- Kvartalsvis IKT-sikkerhetsrapport til styret
- Umiddelbar eskalering av alvorlige hendelser til daglig leder
- Årlig risikovurdering presentert for styret

---

3. IKT-risikostyringsrammeverk — DORA art. 6

3.1 Rammeverk

IKT-risikostyring følger et strukturert rammeverk basert på:

- **Identifisere:** Kartlegge IKT-eiendeler, trusler og sårbarheter
- **Beskytte:** Implementere tiltak for å redusere risiko
- **Oppdage:** Overvåke og detektere sikkerhetshendelser
- **Reagere:** Håndtere hendelser effektivt
- **Gjenopprette:** Gjenopprette normal drift etter hendelser

3.2 Risikovurdering

- **Frekvens:** Minimum årlig, samt ved vesentlige endringer
- **Metodikk:** Sannsynlighet × konsekvens (4×4-matrise)
- **Omfang:** Alle IKT-systemer, tredjepartsleverandører og prosesser
- **Dokumentasjon:** Risikoregister vedlikeholdes løpende

3.3 Risikoakseptkriterier

Risikonivå	Handling
Lav (1-4)	Aksepteres, overvåkes
Middels (5-8)	Tiltak planlegges innen 90 dager
Høy (9-12)	Tiltak implementeres innen 30 dager
Kritisk (13-16)	Umiddelbar handling, eskalering til ledelse

---

4. IKT-systemer og -eiendeler — DORA art. 7-8

4.1 Eiendelsregister

Vi vedlikeholder et komplett register over alle IKT-eiendeler, jf. DORA artikkel 8, inkludert:

- Programvare og versjoner
- Maskinvare og infrastruktur
- Nettverkskomponenter
- Datalagre og databaser
- Tredjepartssystemer og -integrasjoner

4.2 Klassifisering

Alle IKT-eiendeler klassifiseres etter kritikalitet:

Klasse	Beskrivelse	Eksempler
Kritisk	Tjenesten fungerer ikke uten	Betalingsmotor, BankID-integrasjon, database
Viktig	Vesentlig funksjonalitet påvirkes	Kundeservicesystem, rapportering
Standard	Begrenset påvirkning ved utilgjengelighet	Intern kommunikasjon, utviklingsmiljø

4.3 Konfigurasjons- og endringsstyring

- Alle endringer i produksjonsmiljøet gjennomgår formell endringsprosess
- Endringer risikovurderes og godkjennes før implementering
- Alle konfigurasjoner versjoneres og dokumenteres
- Rollback-plan kreves for alle endringer

---

5. Tilgangskontroll — DORA art. 9(4)

5.1 Tilgangsprinsipper

- **Minste privilegium (Least Privilege):** Brukere tildeles kun nødvendig tilgang
- **Need-to-know:** Tilgang til data begrenses basert på tjenstlig behov
- **Rollebasert tilgangskontroll (RBAC):** Tilgang styres gjennom definerte roller
- **Segregering av oppgaver (SoD):** Kritiske funksjoner fordeles på flere personer

5.2 Brukerkontoer

Type	Krav
Standardbrukere	Unik bruker-ID, MFA påkrevd

Type	Krav
Administratorer	Egen admin-konto, MFA påkrevd, tidsbegrenset tilgang
Systemkontoer	Ingen interaktiv pålogging, API-nøkler med rotasjon
Tredjeparter	Tidsbegrenset tilgang, MFA påkrevd, godkjenning fra CISO

5.3 Multifaktorautentisering (MFA)

MFA er påkrevd for:

- Alle administrative tilganger
- Tilgang til produksjonsdata
- VPN-tilkobling
- Koderepository og CI/CD-pipeline
- Skyinfrastrukturens administrasjonsgrensesnitt

5.4 Tilgangsgjennomgang

- Kvartalsvise gjennomganger av alle tilganger
- Umiddelbar deaktivering ved endret roller eller avsluttet arbeidsforhold
- Årlig resertifisering av alle privilegerte tilganger

---

6. Kryptering — DORA art. 9(4)(d)

6.1 Data i transitt

Protokoll	Minimumskrav	Bruksområde
TLS	Versjon 1.3 (TLS 1.2 kun for legacy-integrasjoner)	All ekstern kommunikasjon
mTLS	TLS 1.3 med gjensidig sertifikatautentisering	Interservice-kommunikasjon
HTTPS	TLS 1.3	Web-API-er og brukergrensesnitt

6.2 Data i hvile

Datakategori	Krypteringsmetode	Nøkkelhåndtering
Personopplysninger	AES-256-GCM	HSM-beskyttede nøkler

Datakategori	Krypteringsmetode	Nøkkelhåndtering
Fødselsnummer	AES-256-GCM + applikasjonsnivå	Separat nøkkelpar, HSM
Transaksjonsdata	AES-256-GCM	HSM-beskyttede nøkler
Logger	AES-256-GCM	Rotasjon hver 90. dag
Sikkerhetskopier	AES-256-GCM	Offline nøkkelkopi i safe

6.3 Nøkkelhåndtering

- Nøkler genereres i Hardware Security Module (HSM)
- Nøkkelrotasjon minimum hver 12. måned (90 dager for logger)
- Separasjon av nøkler per miljø (utvikling, test, produksjon)
- Nøkler for kryptering av fødselsnummer håndteres separat
- Nødprosedyre for nøkkelkompromittering dokumentert

---

7. Applikasjonssikkerhet — OWASP

7.1 Sikker utviklingslivssyklus (SSDLC)

Alle utviklingsaktiviteter følger en sikker utviklingslivssyklus:

1. **Kravfase:** Sikkerhets- og personvernkrav defineres
2. **Design:** Trusselmodellering (STRIDE) gjennomføres
3. **Implementering:** Sikre kodestandarder, code review
4. **Testing:** Sikkerhetstesting (SAST, DAST, avhengighetsskanning)
5. **Lansering:** Penetrasjonstesting før produksjonssetting
6. **Drift:** Løpende overvåking og sårbarhetshåndtering

7.2 OWASP Top 10 — tiltak

OWASP-risiko	Tiltak
A01: Broken Access Control	RBAC, autorisasjonskontroll på API-nivå, funksjonsnivåtesting
A02: Cryptographic Failures	TLS 1.3, AES-256, HSM, ingen hardkodede hemmeligheter
A03: Injection	Parametriserte SQL-spørringer, input-validering, ORM
A04: Insecure Design	Trusselmodellering, sikre designmønstre, minste privilegium

OWASP-risiko	Tiltak
A05: Security Misconfiguration	Automatisert konfigurasjonskontroll, hardening, ingen standardpassord
A06: Vulnerable Components	Avhengighetsskanning (SCA), automatiserte oppdateringer, SBOM
A07: Authentication Failures	BankID (brukere), MFA (ansatte), kontosperring ved mislykkede forsøk
A08: Software and Data Integrity	Signerte builds, CI/CD-integritetskontroll, code review
A09: Logging and Monitoring Failures	Sentralisert logging, SIEM, varsling, revisjonslogger
A10: Server-Side Request Forgery	Input-validering, nettverkssegmentering, egress-filtrering

7.3 API-sikkerhet

Gitt at Drop er en API-drevet tjeneste med Open Banking-integrasjoner:

- OAuth 2.0 / OpenID Connect for autentisering og autorisasjon
- Rate limiting per bruker og per IP
- Input-validering og schema-verifisering på alle endepunkter
- API-versjonering med deprekeringspolicy
- API-gateway med WAF-funksjonalitet

---

8. Nettverkssikkerhet

8.1 Nettverksarkitektur

- **Segmentering:** Produksjon, test og utvikling er fullstendig isolert
- **DMZ:** Offentlig tilgjengelige tjenester plasseres i DMZ
- **Mikrosegmentering:** Tjenester kommuniserer kun med autoriserte tjenester
- **Egress-filtrering:** Utgående trafikk begrenses til godkjente destinasjoner

8.2 Brannmur og filtrering

- Web Application Firewall (WAF) foran alle offentlige endepunkter
- Nettverksbrannmur med default-deny-policy
- IDS/IPS for deteksjon og forebygging av inntrengning
- DDoS-beskyttelse på infrastrukturnivå

8.3 Overvåking

- Sentralisert logginnsamling fra alle nettverkskomponenter
- Netflow-analyse for anomalideteksjon
- DNS-overvåking for ondsinnet trafikk

---

9. Hendelsesdeteksjon og -overvåking — DORA art. 10

9.1 Overvåkingssystem

- **SIEM (Security Information and Event Management):** Sentralisert hendelseskorrelasjon
- **Logginnsamling:** All IKT-aktivitet logges sentralt
- **Automatisert varsling:** Definerte terskelverdier for automatisk varsling
- **Anomalideteksjon:** Maskinlæring for identifisering av uvanlig atferd

9.2 Loggkrav

Loggkategori	Oppbevaringstid	Beskyttelse
Autentiseringslogger	12 måneder	Kryptert, skrivebeskyttet
Transaksjonslogger	5 år	Kryptert, skrivebeskyttet
Systemlogger	6 måneder	Kryptert
Sikkerhetslogger	24 måneder	Kryptert, skrivebeskyttet
Tilgangslogger	12 måneder	Kryptert, skrivebeskyttet

9.3 Hendelsesrespons

Se separat dokument: `hendelseshaandtering.md` for fullstendig hendelsesresponsplan.

---

10. Sårbarhetshåndtering — DORA art. 9(4)(e)

10.1 Sårbarhetsskanning

Type	Frekvens	Omfang
Automatisert skanning	Daglig	Alle produksjonssystemer
Avhengighetsskanning (SCA)	Ved hver build	All kildekode
Statisk kodeanalyse (SAST)	Ved hver pull request	All ny kode
Dynamisk analyse (DAST)	Ukentlig	Alle offentlige endepunkter

10.2 Sårbarhetshåndtering

Alvorlighetsgrad (CVSS)	Frist for utbedring
Kritisk (9.0-10.0)	24 timer
Høy (7.0-8.9)	7 dager
Middels (4.0-6.9)	30 dager
Lav (0.1-3.9)	90 dager

10.3 Patchhåndtering

- Sikkerhetsoppdateringer vurderes og implementeres innenfor angitte frister
- Nødpatcher kan deployeres utenfor normal endringsprosess med etterfølgende godkjenning
- All programvare holdes oppdatert med siste stabile versjon
- End-of-life-programvare erstattes innen 6 måneder etter annonsering

---

11. Penetrasjonstesting — DORA art. 24-27

11.1 Testprogram

Testtype	Frekvens	Gjennomfører
Ekstern penetrasjonstest	Årlig	Uavhengig tredjepart
Intern penetrasjonstest	Årlig	Uavhengig tredjepart
Red team-øvelse	Hvert 3. år (TLPT)	Kvalifisert leverandør jf. DORA art. 26
Applikasjonssikkerhetstest	Ved vesentlige endringer	Intern/ekstern
Social engineering-test	Årlig	Uavhengig tredjepart

11.2 TLPT (Threat-Led Penetration Testing) — DORA art. 26

I henhold til DORA artikkel 26 kan Finanstilsynet kreve at vi gjennomfører TLPT. Vi er forberedt på:

- Engasjement av kvalifisert TLPT-leverandør
- Scenariobasert testing basert på reelle trusseletterretninger
- Involvering av kritiske IKT-tredjepartsleverandører
- Rapportering til Finanstilsynet

11.3 Oppfølging av funn

- Alle funn logges i sårbarhetsstyringssystemet
- Funn prioriteres etter alvorlighetsgrad
- Utbedringsplan utarbeides innen 5 virkedager
- Retest gjennomføres etter utbedring
- Ledelsen informeres om kritiske funn umiddelbart

---

12. Sikkerhetskopier og gjenoppretting — DORA art. 12

12.1 Sikkerhetskopieringsstrategi

Dataklasse	Frekvens	Oppbevaring	Lokasjon
Database (produksjon)	Kontinuerlig (WAL) + daglig full	30 dager	Geografisk adskilt, innenfor EØS
Konfigurasjon	Ved endring	90 dager	Versjonskontroll + kryptert backup
Logger	Daglig	Iht. loggpolicy	Separat logginfrastruktur
Krypteringsnøkler	Ved endring	Permanent	Offline, i safe

12.2 Gjenopprettingstesting

- **Frekvens:** Minimum halvårlig
- **Omfang:** Fullstendig gjenoppretting av kritiske systemer
- **Dokumentasjon:** Testresultater dokumenteres og gjennomgås

- **Forbedring:** Funn fra testing fører til oppdatert prosedyre

12.3 RTO og RPO

Se `beredskapsplan.md` for detaljerte RTO/RPO-krav per system.

---

13. Fysisk sikkerhet

13.1 Datasentre

- All infrastruktur er hostet i sertifiserte datasentre (minimum ISO 27001, SOC 2 Type II)
- Datasentre lokalisert innenfor EØS
- Redundant strømforsyning (UPS + dieselgenerator)
- Brannslukkingssystemer
- Adgangskontroll med biometri og logging

13.2 Utviklingsmiljø

- Produksjonsdata benyttes aldri i utviklings- eller testmiljøer
- Syntetiske testdata genereres for testing
- Utviklingsmaskiner har diskkryptering og MFA

---

14. Opplæring og bevissthet — DORA art. 13

14.1 Obligatorisk opplæring

Målgruppe	Innhold	Frekvens
Alle ansatte	Generell IKT-sikkerhet, phishing, passord	Årlig
Utviklere	Sikker koding, OWASP, code review	Halvårlig
Drift	Hendelseshåndtering, herding, overvåking	Halvårlig
Ledelse	IKT-risikostyring, regulatoriske krav	Årlig

14.2 Phishing-simulering

- Kvartalsvise phishing-simuleringer for alle ansatte
- Individuelle resultater brukes til målrettet opplæring
- Resultater rapporteres til ledelsen (aggregert)

---

15. IKT-tredjepartsrisiko — DORA art. 28-30

15.1 Leverandørstyring

Se separat dokument: `utkontraktering-policy.md` for detaljert leverandørstyringspolicy.

15.2 Kritiske IKT-leverandører

Kritiske IKT-tredjepartsleverandører identifiseres og underlegges forsterkede krav, jf. DORA artikkel 28:

- Årlig risikovurdering
- Rett til revisjon og inspeksjon
- Exit-strategi og overgangsplan
- Rapportering av vesentlige hendelser
- Overholdelse av DORA-krav

---

16. Kontinuitetsplanlegging — DORA art. 11

Se separat dokument: `beredskapsplan.md` for detaljert kontinuitetsplan.

Denne IKT-sikkerhetspolicyen understøtter kontinuitetsplanlegging ved å sikre:

- Høy tilgjengelighet gjennom redundans
- Rask gjenoppretting gjennom testede prosedyrer
- Begrenset konsekvens gjennom segmentering og isolasjon

---

17. Revisjon og oppdatering

17.1 Gjennomgang

- **Årlig:** Full gjennomgang av policyen
- **Ved vesentlige endringer:** Endringer i teknologi, tjenester eller regulering
- **Etter hendelser:** Relevant revisjon etter sikkerhetshendelser
- **Etter penetrasjonstesting:** Oppdatering basert på funn

17.2 Godkjenningsprosess

Endring	Godkjenner
Redaksjonell	CISO
Vesentlig	Daglig leder
Prinsipiell	Styret

17.3 Versjonshistorikk

Versjon	Dato	Endring	Godkjent av
1.0	12.02.2026	Opprinnelig dokument	_____

---

18. Referanser

- DORA — Forordning (EU) 2022/2554 om digital operasjonell motstandsdyktighet
- GDPR — Forordning (EU) 2016/679 om personvern
- PSD2 — Direktiv (EU) 2015/2366 om betalingstjenester
- ISO 27001:2022 — Informasjonssikkerhetsstyring
- NIST Cybersecurity Framework 2.0
- OWASP Top 10 (2021)
- Finanstilsynets IKT-forskrift
- Hvitvaskingsloven (LOV-2018-06-01-23)

Denne IKT-sikkerhetspolicyen er eid av CISO og godkjent av styret i ALAI Holding AS.

Internal Controls

Internkontrollrutiner — Drop (ALAI Holding AS)

Dokument: Rammeverk for internkontroll **Hjemmel:** Finansforetaksloven §13-5, hvitvaskingsloven §§7-8 og §37, internkontrollforskriften **Virksomhet:** ALAI Holding AS, org.nr 932 516 136 **Produkt:** Drop — betalingsformidling og pengeoverføringer **Versjon:** 1.0 **Dato:** 2026-02-12 **Godkjent av:** Styre **Neste revisjon:** 2027-02-12

---

1. Formål

Internkontrollrutinene skal sikre at ALAI Holding AS gjennom produktet Drop:

- Overholder gjeldende lovverk, herunder finansforetaksloven, hvitvaskingsloven og personopplysningsloven
- Har effektiv risikostyring og kontroll med virksomheten
- Har klare ansvarslinjer og rapporteringsveier
- Identifiserer, vurderer og håndterer operasjonelle risikoer
- Har en kultur for etterlevelse (compliance)

---

2. Tre forsvarslinjer

Selskapet organiserer sin internkontroll etter prinsippet om tre forsvarslinjer, jf. Finanstilsynets veiledning og internasjonale standarder (COSO/IIA):

2.1 Første forsvarslinje — Operativ drift

Hvem: Alle ansatte i operative roller (utvikling, drift, kundeservice)

Ansvar:

- Daglig etterlevelse av rutiner og policyer
- Identifisere og rapportere avvik til nærmeste leder

- Gjennomføre kontroller integrert i arbeidsprosesser
- Dokumentere egne kontrollhandlinger

Kontrollaktiviteter:

Kontroll	Frekvens	Ansvarlig
KYC-kvalitetskontroll ved onboarding	Hver kunde	Operativ medarbeider
Verifikasjon av transaksjonsdata	Fortløpende	System (automatisk)
Rapportering av hendelser og avvik	Ved forekomst	Alle ansatte
Oppfølging av automatiske varsler	Fortløpende	Operativ medarbeider

2.2 Andre forsvarslinje — Risikostyring og Compliance

Hvem: Hvitvaskingsansvarlig / Compliance-funksjon

Ansvar:

- Overvåke og teste etterlevelse av lover, forskrifter og interne rutiner
- Utarbeide og vedlikeholde policyer og rutiner
- Gjennomføre risikiovurderinger
- Rådgi første forsvarslinje
- Rapportere til daglig leder og styret
- Håndtere forholdet til tilsynsmyndigheter

Kontrollaktiviteter:

Kontroll	Frekvens	Ansvarlig
Stikkprøvekontroll av KYC-dokumentasjon	Månedlig (min. 10% av nye kunder)	Hvitvaskingsansvarlig
Gjennomgang av flaggede transaksjoner	Ukentlig	Hvitvaskingsansvarlig
Testing av transaksjonsovervåkingsregler	Kvartalsvis	Compliance
Oppdatering av risikovurdering	Årlig + ved vesentlige endringer	Hvitvaskingsansvarlig
Regelverksovervåking	Løpende	Compliance
Compliance-rapport til styret	Kvartalsvis	Hvitvaskingsansvarlig

2.3 Tredje forsvarslinje — Uavhengig kontroll

Hvem: Ekstern revisor / Uavhengig internrevisor

Ansvar:

- Uavhengig vurdering av internkontrollens effektivitet
- Vurdering av risikostyringsrammeverket
- Rapportering til styret

Kontrollaktiviteter:

Kontroll	Frekvens	Ansvarlig
Ekstern revisjon av AML-program	Årlig	Ekstern revisor
Revisjon av IT-sikkerhet	Årlig	Ekstern IT-revisor
Uavhengig gjennomgang av internkontroll	Årlig	Ekstern revisor
Rapportering av funn og anbefalinger	Etter hver revisjon	Ekstern revisor

---

3. Governance og organisering

3.1 Styret

Ansvar:

- Fastsette overordnet strategi for risikostyring og internkontroll
- Godkjenne policyer, rutiner og risikoappetitt
- Motta og behandle kvartalsrapporter fra compliance og revisor
- Sikre tilstrekkelige ressurser til internkontroll
- Overordnet ansvar for etterlevelse

Styreaktiviteter:

Aktivitet	Frekvens
Behandle compliance-rapport	Kvartalsvis
Godkjenne oppdatert risikovurdering	Årlig
Godkjenne oppdaterte hvitvaskingsrutiner	Årlig
Behandle revisjonsrapporter	Etter mottakelse
Evaluere internkontrollens effektivitet	Årlig

3.2 Daglig leder

Ansvar:

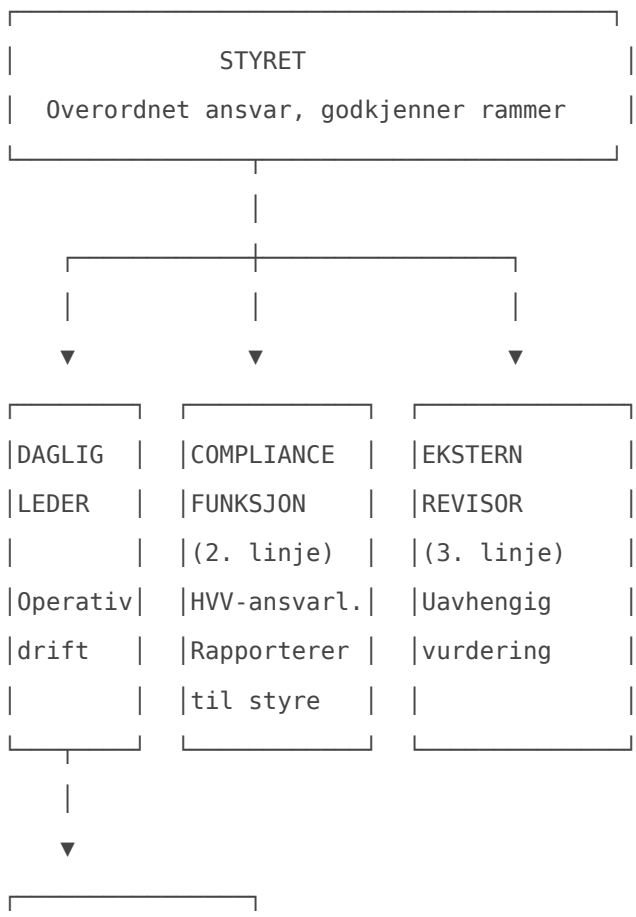
- Operativt ansvar for implementering av styrets vedtak
- Sikre at organisasjonen har nødvendig kompetanse og ressurser
- Godkjenne høyrisiko-kundeforhold (etter anbefaling fra compliance)
- Rapportere til styret om vesentlige risikoforhold

3.3 Hvitvaskingsansvarlig / Chief Compliance Officer

Ansvar:

- Daglig leder for compliance-funksjonen
- Hvitvaskingsansvarlig etter hvitvaskingsloven §8 fjerde ledd
- Rapporterer direkte til daglig leder og styret (uavhengig av operative linjer)
- Har myndighet til å stoppe transaksjoner og avvise kundeforhold

3.4 Organisasjonskart — internkontroll



```
│OPERATIVE       │
│MEDARBEIDERE    │
│(1. linje)      │
│Tech, support,  │
│kundeservice    │
└────────────────┘
```

---

4. Risikostyring

4.1 Risikorammeverk

Selskapet identifiserer og vurderer følgende risikokategorier:

Risikokategori	Beskrivelse	Eier
HV/TF-risiko	Risiko for misbruk til hvitvasking/terrorfinansiering	Hvitvaskingsansvarlig
Operasjonell risiko	Systemfeil, menneskelige feil, prosesssvikt	Daglig leder
IT- og cyberrisiko	Datainnbrudd, tjenestenekt, systemsårbarhet	Tech Lead
Compliance-risiko	Brudd på regelverk, tilsynssanksjoner	Compliance
Omdømmerisiko	Hendelser som skader selskapets omdømme	Daglig leder
Strategisk risiko	Feil forretningsbeslutninger	Styret

4.2 Risikovurderingsprosess

1. **Identifisering:** Kartlegge relevante risikoer per kategori
2. **Vurdering:** Sannsynlighet x konsekvens (skala 1-4)
3. **Tiltak:** Definere risikoreduserende tiltak
4. **Overvåking:** Løpende overvåking av risikoindikatorer
5. **Rapportering:** Kvartalsvise risikorapporter til styret
6. **Revisjon:** Årlig oppdatering av risikovurderingen

4.3 Risikoindikatorer (KRI)

Indikator	Terskel (gul)	Terskel (rød)	Frekvens

Antall flaggede transaksjoner	>50/mnd	>100/mnd	Månedlig
Gjennomsnittlig behandlingstid flagg	>48 timer	>72 timer	Ukentlig
Andel EDD-kunder	>10% av kundebasen	>20%	Kvartalsvis
Antall EFE-rapporter	>2/kvartal	>5/kvartal	Kvartalsvis
KYC-mangler ved stikkprøve	>5%	>10%	Månedlig
Systemnedetid	>99.5% oppetid	<99% oppetid	Daglig
Antall sikkerhetshendelsar	>1/mnd	>3/mnd	Månedlig

---

5. Compliance-overvåking

5.1 Overvåkingsplan

Område	Kontrollhandling	Frekvens	Ansvarlig	Rapporteres til
KYC/CDD	Stikkprøve av onboarding-kvalitet	Månedlig	Compliance	Daglig leder
Transaksjonovervåking	Review av regler og terskler	Kvartalsvis	Compliance	Styret
PEP/sanksjoner	Test av screeningeffektivitet	Halvårlig	Compliance	Styret
Opplæring	Kontroll av gjennomføring	Årlig	Compliance	Daglig leder
Rutiner	Gjennomgang og oppdatering	Årlig	Compliance	Styret
Regelverksendringer	Overvåking av nye krav	Løpende	Compliance	Daglig leder
Hendelseslog	Gjennomgang av logger	Ukentlig	Compliance	Daglig leder
IT-sikkerhet	Penetrasjonstesting	Årlig	Ekstern	Styret
Personvern	DPIA-oppdatering	Årlig	Compliance	Daglig leder

5.2 Rapporteringskalender

Rapport	Mottaker	Frekvens	Innhold

Compliance-statusrapport	Styret	Kvartalsvis	HV/TF-statistikk, avvik, tiltak, regelverksendringer
Risikorapport	Styret	Kvartalsvis	KRI-status, risikoendringer, handlingsplan
AML-årsrapport	Styret	Årlig	Full gjennomgang av AML-programmet
Hendelsesrapport	Daglig leder	Ved hendelse	Beskrivelse, tiltak, læringspunkter
Revisjonsrapport	Styret	Årlig	Ekstern revisors funn og anbefalinger

---

6. Avviksbehandling

6.1 Definisjon

Et avvik er ethvert brudd på, eller manglende etterlevelse av:

- Lover og forskrifter
- Interne rutiner og policyer
- Styrets vedtak og retningslinjer
- Tilsynsmyndighetenes pålegg

6.2 Avviksprosess

```
1. IDENTIFISERING          2. REGISTRERING          3. VURDERING
   Alle ansatte →             Avvikslogg →             Compliance →
   rapporterer                dokumenteres             alvorlighetsgrad

4. TILTAK                  5. OPPFØLGING            6. RAPPORTERING
   Korrigerende →             Verifisere →             Til styre/
   tiltak defineres           effekt                   tilsynsmyndighet
```

6.3 Alvorlighetsgrader

Grad	Beskrivelse	Responstid	Rapporteres til
Kritisk	Lovbrudd, tilsynssanksjon, stor kundeeksponering	Umiddelbart	Styre, Finanstilsynet

Grad	Beskrivelse	Responstid	Rapporteres til
Høy	Vesentlig rutinebrudd, gjentatte avvik	24 timer	Daglig leder, styre
Middels	Enkeltavvik fra rutiner, forbedringspotensial	1 uke	Daglig leder
Lav	Mindre prosessavvik, ingen kundekonsekvens	30 dager	Compliance-logg

6.4 Avvikslogg

Alle avvik registreres i avviksloggen med:

- Dato og tidspunkt
- Beskrivelse av avviket
- Hvem som oppdaget det
- Alvorlighetsgrad
- Korrigerende tiltak
- Ansvarlig for oppfølging
- Frist for lukking
- Status (åpent/lukket)
- Læringspunkter

---

7. Eskalering

7.1 Eskaleringsprosedyre

Situasjon	Eskaleres til	Tidsfrist
Mistenkelig transaksjon (flagget av system)	Hvitvaskingsansvarlig	24 timer
Bekreftet mistanke om HV/TF	EFE/Økokrim + daglig leder	Uten ugrunnet opphold
Sanksjonstreff (bekreftet)	Daglig leder + UD	Umiddelbart
Kritisk avvik	Styre + eventuelt Finanstilsynet	Umiddelbart
Sikkerhetshendeelse (datainnbrudd)	Daglig leder + Datatilsynet (72t)	Umiddelbart
Tilsynsforespørsel	Daglig leder + compliance	Innen tilsynets frist
Kundeklage (compliance-relatert)	Compliance	5 virkedager

7.2 Varsling (Whistleblowing)

Jf. arbeidsmiljøloven kapittel 2A:

- Alle ansatte har rett til å varsle om kritikkverdige forhold
- Varslingskanal er etablert (direkte til styreleder)
- Varsler beskyttes mot gjengjeldelse
- Alle varsler behandles konfidensielt og dokumenteres

---

8. IT-kontroller

8.1 Tilgangsstyring

Prinsipp	Implementering
Minste privilegium	Brukere får kun tilgang til det de trenger
Rollebasert tilgang (RBAC)	Tilgang basert på rolle, ikke person
Separation of duties	Kritiske funksjoner krever to personers godkjenning
Periodisk tilgangsgjennomgang	Kvartalsvis gjennomgang av alle tilganger
Logging	Alle tilgangsendringer og datautrekk logges

8.2 Systemovervåking

Kontroll	Beskrivelse	Frekvens
Oppetidsovervåking	Automatisk varsling ved nedetid	Kontinuerlig
Ytelsesovervåking	Responstider og feilrater	Kontinuerlig
Sikkerhetslogg-gjennomgang	Analyse av innloggingsforsøk og anomalier	Daglig
Sårbarhetsskanning	Automatisk skanning av kjente sårbarheter	Ukentlig
Penetrasjonstesting	Ekstern testing av sikkerhet	Årlig
Backup-verifisering	Test av gjenoppretting fra backup	Månedlig

8.3 Endringsstyring

Alle endringer i produksjonssystemer skal:

1. Dokumenteres med beskrivelse og begrunnelse
2. Testes i staging-miljø

3. Godkjennes av tech lead og compliance (ved regelverksrelevante endringer)
4. Rulles ut med rollback-plan
5. Overvåkes etter utrulling

---

9. Opplæring og kompetanse

9.1 Opplæringsprogram

Kurs	Målgruppe	Frekvens	Innhold
Grunnkurs HV/TF	Alle ansatte	Ved ansettelse + årlig	Lovverk, rutiner, gjenkjennelse
Avansert AML	Compliance, operativ	Årlig	Typologier, caseøvelser, EDD
PEP og sanksjoner	Compliance, operativ	Årlig	PEP-definisjoner, screeningprosess
IT-sikkerhet	Alle ansatte	Årlig	Phishing, passord, hendelsesrapportering
GDPR	Alle ansatte	Ved ansettelse + årlig	Personvern, behandlingsgrunnlag
Etikk og varsling	Alle ansatte	Årlig	Etiske retningslinjer, varslingskanal

9.2 Kompetansekrav

Rolle	Minimumskompetanse
Hvitvaskingsansvarlig	Sertifisering (f.eks. CAMS), min. 3 års erfaring
Compliance-medarbeider	Relevant utdanning, opplæring i HV/TF
Daglig leder	Egnethetsvurdering, grunnleggende HV/TF-forståelse
Styremedlemmer	Egnethetsvurdering, forstå regulatorisk rammeverk
Tech Lead	IT-sikkerhetskompetanse, forståelse av compliance-krav

---

10. Beredskapsplan

10.1 Scenarioer

Scenario	Alvorlighet	Umiddelbare tiltak
Datainnbrudd / personopplysninger kompromittert	Kritisk	Isolere system, varsle Datatilsynet (72t), varsle berørte kunder
Sanksjonert transaksjon gjennomført ved feil	Kritisk	Fryse midler, varsle UD, rapportere til EFE
Systemnedetid > 4 timer	Høy	Aktivere failover, informere kunder, loggføre
Tjenestenektangrep (DDoS)	Høy	Aktivere DDoS-beskyttelse, eskalere til hosting-partner
Mistanke om intern svindel	Kritisk	Fryse tilganger, undersøke, varsle styre og evt. politi

10.2 Kommunikasjonsplan ved hendelse

Interessent	Tidsfrist	Kanal	Ansvarlig
Finanstilsynet	Uten ugrunnet opphold	Altinn / epost	Daglig leder
Datatilsynet	72 timer (datainnbrudd)	Altinn	Daglig leder
Berørte kunder	Uten ugrunnet opphold	App + epost	Kundeservice
Styret	Umiddelbart	Epost + telefon	Daglig leder
Ansatte	Umiddelbart	Intern kanal	Daglig leder

---

11. Endringslogg

Versjon	Dato	Endring	Godkjent av
1.0	2026-02-12	Førstegangs utarbeidelse	Styre

Dokumentet er utarbeidet i henhold til finansforetaksloven §13-5, hvitvaskingsloven §§7-8 og §37, og Finanstilsynets veiledninger om internkontroll i betalingsforetak.

Incident Management

Hendelseshåndteringsplan — Drop

Dokument-ID: IRP-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. 17-23, GDPR art. 33-34, Finanstilsynets IKT-forskrift

---

1. Innledning

1.1 Formål

Denne hendelseshåndteringsplanen definerer prosesser for å oppdage, klassifisere, håndtere og rapportere IKT-relaterte hendelser i Drop-tjenesten. Planen sikrer effektiv respons i samsvar med DORA og øvrig regulering.

1.2 Virkeområde

Planen dekker:

- Alle IKT-sikkerhetshendelser som påvirker Drop-tjenesten
- Personvernbrudd (GDPR art. 4 nr. 12)
- Driftshendelser som påvirker tjenestetilgjengelighet
- Hendelser hos tredjepartsleverandører som påvirker Drop
- Cyberangrep og forsøk på uautorisert tilgang

1.3 Regulatorisk bakgrunn

Regulering	Artikler	Krav
DORA art. 17	IKT-hendelseshåndteringsprosess	Denne planen
DORA art. 18	Klassifisering av hendelser	Seksjon 3
DORA art. 19	Rapportering til myndigheter	Seksjon 7

Regulering	Artikler	Krav
DORA art. 20	Harmonisert rapportering	Seksjon 7
DORA art. 23	Deling av trusseletterretning	Seksjon 9
GDPR art. 33	Varsling til tilsynsmyndighet	Seksjon 7.3
GDPR art. 34	Varsling til registrerte	Seksjon 7.4

---

2. Deteksjon og varsling

2.1 Deteksjonsmekanismer

Kilde	Type	Beskrivelse
SIEM	Automatisert	Korrelasjon av sikkerhetshendelser, regelbaserte og ML-baserte varsler
Overvåking	Automatisert	Ytelse, tilgjengelighet, feilrater
WAF/IDS/IPS	Automatisert	Angrepsdeteksjon, trafikanalyse
Logganalyse	Automatisert/manuell	Anomalideteksjon i applikasjons- og systemlogger
Sårbarhetsskanner	Automatisert	Daglig skanning av kjente sårbarheter
Brukerrapportering	Manuell	Klager eller meldinger fra brukere
Leverandørvarsling	Manuell	Hendelsesrapporter fra tredjeparter
Trusseletterretning	Automatisert/manuell	Feed fra CERT, bransjekilder

2.2 Initialvarsling

Ved deteksjon av potensiell hendelse:

1. Automatisert varsling til vaktteam via definerte kanaler
2. Vaktteamet foretar innledende vurdering innen 15 minutter
3. Hendelsen registreres i hendelseshåndteringssystemet
4. Innledende klassifisering gjennomføres (se seksjon 3)
5. Eskalering iht. klassifisering

---

3. Klassifisering — DORA art. 18

3.1 Alvorlighetsgrader

Hendelser klassifiseres etter alvorlighetsgrad basert på kriteriene i DORA artikkel 18(1):

P1 — Kritisk

Kriterier (ett eller flere):

- Fullstendig tjenestestans for betalingsfunksjoner
- Bekreftet databrudd med personopplysninger eller finansielle data
- Aktivt pågående cyberangrep med vesentlig konsekvens
- Tap eller kompromittering av krypteringsnøkler
- Vesentlig økonomisk tap for brukere
- Hendelse som påvirker mer enn 10% av brukerbasisen

Responstid: Umiddelbart **Rapportering:** Finanstilsynet innen 4 timer (initialrapport)

P2 — Høy

Kriterier (ett eller flere):

- Delvis tjenestestans som påvirker betalinger for en gruppe brukere
- Sikkerhetsbrudd med begrenset omfang
- Kompromittert administratorkonto
- Uautorisert tilgang til produksjonssystemer
- Hendelse hos kritisk leverandør som påvirker tjenesten

Responstid: Innen 30 minutter **Rapportering:** Finanstilsynet innen 4 timer dersom hendelsen anses som vesentlig

P3 — Middels

Kriterier (ett eller flere):

- Degradert tjenestekvalitet (forsinkelser, feil i ikke-kritiske funksjoner)
- Mislykket inntrengningsforsøk med indikasjoner på målrettet angrep
- Sårbarhet med høy CVSS-score oppdaget i produksjon
- Hendelse hos leverandør som kan påvirke tjenesten

Responstid: Innen 2 timer **Rapportering:** Intern rapportering, Finanstilsynet ved behov

P4 — Lav

Kriterier (ett eller flere):

- Mindre tekniske problemer uten brukerpåvirkning
- Automatisk blokkerte angrepsforsøk (WAF, brannmur)

- Sårbarhet med lav/middels CVSS-score
- Informasjonshendelser som krever oppfølging

Responstid: Innen 8 timer **Rapportering:** Intern loggføring

3.2 Klassifiseringskriterier (DORA art. 18(1))

Kriterium	Beskrivelse	Vurdering
Berørte brukere	Antall og andel berørte kunder/transaksjoner	Kvantitativt
Varighet	Faktisk eller forventet varighet	Tidsbasert
Geografisk omfang	Påvirkning i ulike markeder	Geografisk
Datatap	Omfang og sensitivitet av kompromittert data	Kvantitativt
Økonomisk konsekvens	Direkte og indirekte økonomisk påvirkning	Kvantitativt
Tjenestekritikalitet	Påvirkning på kritiske funksjoner	Kvalitativt
Omdømmerisiko	Potensiell påvirkning på tillit	Kvalitativt

3.3 Reklassifisering

Hendelser kan reklassifiseres under håndteringen dersom:

- Omfanget endrer seg (øker eller reduseres)
- Ny informasjon fremkommer
- Konsekvensen viser seg annerledes enn først antatt
- Reklassifisering dokumenteres med begrunnelse

---

4. Respons per alvorlighetsgrad

4.1 P1 — Kritisk hendelsesrespons

```
MINUTT 0-15:    Deteksjon → Innledende vurdering → Klassifisering P1
MINUTT 15-30:   Aktiver hendelsesresponsteam → Isoler berørte systemer
MINUTT 30-60:   Analyse pågår → Kommunikasjon til ledelse og CISO
TIME 1:         Initialrapport til Finanstilsynet (innen 4t)
                Aktivér beredskapsorganisasjon
```

```
                Ekstern kommunikasjon (statusside, push-varsel)
TIME 1-4:       Containment → Eradication → Gjenoppretting pågår
TIME 4:         Statusrapport til Finanstilsynet
                Oppdatering til berørte brukere
TIME 4-24:      Fortsatt gjenoppretting → Overvåking
DAG 1-3:        Intermediær rapport til Finanstilsynet (innen 72t)
                GDPR-varsling til Datatilsynet (innen 72t) ved personvernbrudd
                Kommunikasjon til berørte registrerte ved høy risiko
DAG 3-30:       Endelig rapport til Finanstilsynet (innen 1 måned)
                Post-incident review
```

4.2 P2 — Høy hendelsesrespons

```
MINUTT 0-30:    Deteksjon → Vurdering → Klassifisering P2
MINUTT 30-60:   Hendelsesansvarlig utpekt → Analyse startet
TIME 1-2:       Containment-tiltak implementert
                CISO informert
TIME 2-4:       Eradication og gjenoppretting
                Vurdering av rapporteringsplikt (Finanstilsynet)
TIME 4-8:       Normal drift gjenopprettet
                Intern statusrapport
DAG 1-5:        Rotårsaksanalyse
                Forbedringstiltak identifisert
```

4.3 P3 — Middels hendelsesrespons

```
TIME 0-2:       Deteksjon → Vurdering → Klassifisering P3
TIME 2-4:       Analyse og vurdering av tiltak
TIME 4-8:       Tiltak implementert
DAG 1-3:        Verifisering → Dokumentasjon
DAG 3-5:        Hendelsesrapport ferdigstilt
```

4.4 P4 — Lav hendelsesrespons

```
TIME 0-8:       Deteksjon → Vurdering → Klassifisering P4
DAG 1-5:        Analyse og tiltak ved behov
DAG 5-10:       Dokumentasjon i hendelsesloggen
```

5. Hendelseshåndteringsfaser

5.1 Fase 1: Identifisering

- Bekreft at hendelsen er reell (ikke falsk positiv)
- Kartlegg omfang og berørte systemer
- Identifiser hendelsestypen (angrep, feil, menneskelig feil, leverandør)
- Klassifiser alvorlighetsgrad (P1-P4)
- Dokumenter tidslinje fra deteksjon

5.2 Fase 2: Containment (Inneslutning)

Kortsiktig containment:

- Isoler berørte systemer for å hindre spredning
- Aktiver alternative systemer/failover der mulig
- Bevare bevis (ikke slett logger eller data)
- Blokkér identifiserte angrepsvektor

Langsiktig containment:

- Implementer midlertidige sikkerhetstiltak
- Patch eller oppdater sårbare systemer i isolert miljø
- Verifiser at containment er effektiv

5.3 Fase 3: Eradication (Fjerning)

- Identifiser og fjern rotårsaken
- Fjern skadelig programvare, uautoriserte kontoer, bakdører
- Oppdater/patch alle berørte systemer
- Verifiser at trusselen er eliminert
- Oppdater sikkerhetsregler og blokkérlister

5.4 Fase 4: Recovery (Gjenoppretting)

- Gjenopprett systemer fra kjent god tilstand (backup/clean install)
- Gjenopprett data fra verifiserte sikkerhetskopier
- Implementer forbedrede sikkerhetstiltak før gjenåpning
- Gradvis gjenåpning med forstørket overvåking
- Verifiser tjenestekvalitet

- Overvåk tett de neste 24-72 timene for tilbakefall

5.5 Fase 5: Lessons Learned (Lærdommer)

- Gjennomfør post-incident review innen 5 virkedager (P1/P2) eller 15 virkedager (P3/P4)
- Dokumenter hendelsesforløp, respons og utfall
- Identifiser forbedringstiltak
- Oppdater prosedyrer, deteksjonsregler og sikkerhetstiltak
- Del relevante lærdommer med teamet

---

6. Hendelsesresponsteam

6.1 Sammensetning

Rolle	Ansvar	Aktiveres ved
Hendelsesleder (Incident Commander)	Overordnet koordinering, beslutninger, kommunikasjon	P1, P2
CISO	Sikkerhetsvurdering, myndighetskontakt, strategiske beslutninger	P1, P2
Teknisk leder	Teknisk analyse, containment, gjenoppretting	P1, P2, P3
Driftsingeniør	Systemadministrasjon, failover, gjenoppretting	Alle
Compliance-ansvarlig	Regulatorisk vurdering, rapporteringsplikt	P1, P2
Kommunikasjonsansvarlig	Ekstern/intern kommunikasjon	P1, P2
Daglig leder	Strategiske beslutninger, styrekontakt	P1
Personvernombud (DPO)	Personvernvurdering, Datatilsynet-rapportering	Alle med personvernimplikasjon

6.2 Eskalering

Fra	Til	Kriterium
Vaktteam	Teknisk leder	Alle bekreftede hendelser
Teknisk leder	CISO	P1, P2, sikkerhetshendelser

Fra	Til	Kriterium
CISO	Daglig leder	P1, alle hendelser med regulatorisk rapporteringsplikt
Daglig leder	Styreleder	P1 med vesentlig konsekvens

6.3 Kontaktinformasjon

Oppdatert kontaktliste for hendelsesresponsteamet, inkludert:

- Mobilnummer (primær og sekundær)
- E-post
- Alternativ kontaktmetode
- Stedfortreder per rolle
- Oppdateres minimum kvartalsvis

---

7. Rapportering til myndigheter

7.1 Finanstilsynet — DORA art. 19

Rapporteringsplikt

Vesentlige IKT-relaterte hendelser rapporteres til Finanstilsynet, jf. DORA art. 19(1).

Rapporteringsfrister

Rapport	Frist	Innhold
Initialrapport	Innen 4 timer etter klassifisering som vesentlig	Hendelsestype, berørte tjenester, innledende konsekvens, iverksatte tiltak
Intermediær rapport	Innen 72 timer	Oppdatert omfang, rotårsak (foreløpig), status for containment/gjenoppretting
Endelig rapport	Innen 1 måned	Fullstendig beskrivelse, rotårsak, konsekvenser, lærdommer, forbedringstiltak

Kriterier for «vesentlig hendelse» (DORA art. 18(1))

En hendelse er vesentlig dersom den:

- Berører kritiske betalingstjenester

- Påvirker et betydelig antall brukere
- Medfører eller kan medføre vesentlig økonomisk tap
- Medfører tap av data eller kompromittering av konfidensialitet
- Har eller kan ha betydelig omdømmekonsekvens
- Har varighet som overstiger terskelverdier satt av Finanstilsynet

7.2 DORA art. 20 — Harmonisert rapportering

Vi følger rapporteringsformatet definert av de europeiske tilsynsmyndighetene (ESAs) i henhold til DORA art. 20, når dette er implementert av Finanstilsynet.

7.3 Datatilsynet — GDPR art. 33

Ved brudd på personopplysningssikkerheten:

Handling	Frist	Kriterium
Vurdering av rapporteringsplikt	Umiddelbart etter deteksjon	Alle personvernbrudd
Melding til Datatilsynet	Innen 72 timer	Med mindre bruddet sannsynligvis ikke medfører risiko for registrertes rettigheter
Informasjon til berørte registrerte	Uten ugrunnet opphold	Dersom bruddet sannsynligvis medfører høy risiko (GDPR art. 34)

Innhold i melding til Datatilsynet (GDPR art. 33(3)):

- Bruddets art, inkludert kategorier og antall berørte registrerte
- Navn og kontaktinformasjon til personvernombudet
- Sannsynlige konsekvenser
- Tiltak som er iverksatt eller planlagt

7.4 Varsling til berørte registrerte — GDPR art. 34

Berørte registrerte varsles uten ugrunnet opphold dersom personvernbruddet sannsynligvis medfører høy risiko for deres rettigheter og friheter.

Unntak (GDPR art. 34(3)):

- Data var kryptert og nøkler ikke kompromittert
- Tiltak er truffet som gjør at høy risiko ikke lenger er sannsynlig
- Individuell varsling krever uforholdsmessig innsats (offentlig kommunikasjon brukes)

Varsling inneholder:

- Klar og tydelig beskrivelse av bruddet
- Kontaktinformasjon til personvernombudet
- Sannsynlige konsekvenser
- Tiltak iverksatt og anbefalt egenhandling

Varsling skjer via:

- Push-varsling i appen
- E-post til registrert e-postadresse
- Ved behov: SMS og statusside

---

8. Dokumentasjon

8.1 Hendelseslogg

Alle hendelser dokumenteres med:

- Unikt hendelses-ID
- Dato og tidspunkt for deteksjon
- Kilde for deteksjon
- Klassifisering (P1-P4)
- Hendelsestype (sikkerhet, drift, personvern, leverandør)
- Beskrivelse
- Berørte systemer og brukere
- Tidslinje for håndtering
- Iverksatte tiltak
- Rotårsak
- Rapportering til myndigheter (ja/nei, dato)
- Forbedringstiltak
- Status (åpen, under håndtering, lukket)

8.2 Bevissikring

Ved sikkerhetshendelser (P1/P2):

- Sikre logger og bevis før containment
- Forensisk kopi av berørte systemer der relevant
- Kjede av bevis (chain of custody) dokumenteres
- Bevis oppbevares sikkert og skrivebeskyttet
- Bevisene kan overleveres til politi/påtalemyndighet ved behov

8.3 Oppbevaring

Dokumenttype	Oppbevaringstid
P1-hendelser	5 år
P2-hendelser	3 år
P3/P4-hendelser	2 år
Rapporter til myndigheter	5 år
Personvernbrudd (alle)	5 år
Forensisk bevis	Til saken er avsluttet + 3 år

---

9. Trusseletterretning — DORA art. 23

9.1 Kilder

Vi mottar og vurderer trusseletterretning fra:

- Norsk nasjonalt cybersikkerhetssenter (NCSC/NorCERT)
- FinansCERT (Nordic Financial CERT)
- Kommersielle trusseletterretningsfeeder
- Open-source trusseletterretning (OSINT)
- Bransjesamarbeid og informasjonsdeling

9.2 Deling

I henhold til DORA art. 23 deltar vi i informasjonsdeling om cybertrusler:

- Anonymiserte indikatorer deles med relevante bransjefellesskap
- Vi bidrar til FinansCERT med hendelsesdata
- Vi mottar og implementerer varsler fra myndigheter

9.3 Bruk

Trusseletterretning brukes til å:

- Oppdatere deteksjonsregler i SIEM
- Blokkere kjente ondsinnede IP-adresser og domener
- Prioritere sårbarhetshåndtering
- Informere risikost vurderinger

- Forbedre hendelsesresponsprosedyrer

---

10. Post-Incident Review

10.1 Gjennomføring

Post-incident review gjennomføres etter alle P1- og P2-hendelser, samt utvalgte P3-hendelser:

Alvorlighetsgrad	Frist for review	Deltakere
P1	Innen 5 virkedager	Hele hendelsesresponsteamet + ledelse
P2	Innen 10 virkedager	Hendelsesresponsteam
P3	Innen 15 virkedager	Teknisk leder + relevante ressurser

10.2 Innhold i post-incident review

- **Hendelsesforløp:** Kronologisk gjennomgang av hendelsen
- **Deteksjon:** Ble hendelsen oppdaget raskt nok? Hva kan forbedres?
- **Respons:** Var responsen effektiv? Ble prosedyrer fulgt?
- **Kommunikasjon:** Fungerte intern og ekstern kommunikasjon?
- **Rotårsak:** Hva var den underliggende årsaken?
- **Konsekvens:** Faktisk konsekvens for brukere, tjeneste, økonomi og omdømme
- **Forbedringstiltak:** Konkrete tiltak med ansvarlig og frist

10.3 Oppfølging av forbedringstiltak

- Alle forbedringstiltak registreres med ansvarlig, frist og status
- Statusgjennomgang i månedlig sikkerhetsmøte
- Tiltak verifiseres før lukking

---

11. Øvelser og testing

11.1 Øvelsesprogram

Øvelsestype	Frekvens	Beskrivelse

Tabletop	Kvartalsvis	Scenariobasert gjennomgang med hendelsesresponsteam
Simulering	Halvårlig	Teknisk simulering av hendelse (kontrollert)
Full øvelse	Årlig	Ende-til-ende simulering inkl. kommunikasjon og rapportering
Red team	Hvert 3. år	Realistisk angrepssimulering (jf. DORA TLPT)

11.2 Scenarioer for øvelser

- Ransomware-angrep mot produksjonsserver
- Databasekompromittering med datatap
- DDoS-angrep mot betalingsmotor
- Insider-trussel (kompromittert ansattekonto)
- Leverandørhendelse (Open Banking-leverandør nede)
- Kombinert hendelse (cybersikkerhet + bortfall av leverandør)

11.3 Evaluering

Alle øvelser evalueres med:

- Hva fungerte godt
- Hva kan forbedres
- Konkrete forbedringstiltak
- Dato for neste øvelse

---

12. Revisjon og oppdatering

12.1 Gjennomgang

- **Årlig:** Full gjennomgang av planen
- **Etter P1/P2-hendelser:** Revisjon basert på lærdommer
- **Etter øvelser:** Oppdatering basert på funn
- **Ved regulatoriske endringer:** Tilpasning til nye krav
- **Ved vesentlige endringer:** Ny teknologi, nye leverandører, organisasjonsendring

12.2 Godkjenning

Endring	Godkjenner
Redaksjonell	CISO
Vesentlig	Daglig leder
Prinsipiell	Styret

12.3 Versjonshistorikk

Versjon	Dato	Endring	Godkjent av
1.0	12.02.2026	Opprinnelig dokument	_____

Vedlegg

Vedlegg A: Kontaktliste hendelsesresponsteam

Separat dokument — fortrolig.

Vedlegg B: Maler for rapportering

- Mal for initialrapport til Finanstilsynet
- Mal for intermediær rapport
- Mal for endelig rapport
- Mal for GDPR-bruddmelding til Datatilsynet
- Mal for varsling til berørte registrerte

Vedlegg C: Sjekklister per hendelsestype

- Sjekkliste: Ransomware
- Sjekkliste: DDoS
- Sjekkliste: Databrudd
- Sjekkliste: Leverandørhendelse
- Sjekkliste: Insider-trussel

Vedlegg D: Eskaleringstrinn visuelt

```
P4 (Lav)     → Driftsingeniør
P3 (Middels)  → Driftsingeniør → Teknisk leder
```

```
P2 (Høy)      → Driftsingeniør → Teknisk leder → CISO → Daglig leder
P1 (Kritisk)  → Hele hendelsesresponsteamet → Styreleder
```

Denne hendelseshåndteringsplanen er eid av CISO og godkjent av styret i ALAI Holding AS. Planen testes og revideres minimum årlig.

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.

Complaints Handling

Klagebehandlingsprosedyre — Drop

Dokument-ID: KLAGE-DROP-001 **Versjon:** 1.0 **Dato:** 12. februar 2026 **Eier:** ALAI Holding AS, org.nr. 932 516 136 **Regulatorisk grunnlag:** PSD2 (EU) 2015/2366 art. 101, betalingstjenesteloven, finansforetaksloven

---

1. Innledning

1.1 Formål

Denne prosedyren beskriver hvordan ALAI Holding AS håndterer klager fra brukere av Drop-tjenesten. Prosedyren sikrer at klager behandles effektivt, rettferdig og i samsvar med gjeldende regelverk.

1.2 Virkeområde

Prosedyren gjelder for alle klager som gjelder Drop-tjenesten, inkludert:

- Betalingstransaksjoner (QR-betaling og utenlandsoverføring)
- Gebyrer og prising
- Tilgjengelighet og tekniske problemer
- Personvern og datasikkerhet
- Kundekontroll og verifisering
- Kundeservice
- Andre forhold knyttet til tjenesteleveransen

1.3 Definisjon av klage

En klage er enhver formell uttrykt misnøye fra en bruker vedrørende Drop-tjenesten, der brukeren forventer et svar eller en løsning.

Generelle henvendelser, spørsmål og tilbakemeldinger som ikke uttrykker misnøye, behandles som ordinære kundeservicehenvendelser og faller utenfor denne prosedyren.

---

2. Klagekanaler

2.1 Tilgjengelige kanaler

Kanal	Kontaktinformasjon	Tilgjengelighet
E-post	klage@getdrop.no	24/7 (mottatt)
I appen	Hjelp > Send klage	24/7
Post	ALAI Holding AS, [adresse], Norge	Postgang
Kundeservice	support@getdrop.no	Man-fre 08:00-20:00, lør 10:00-16:00

2.2 Krav til klage

For effektiv behandling bør klagen inneholde:

- Ditt fulle navn og registrerte e-postadresse eller mobilnummer
- Beskrivelse av forholdet du klager på
- Dato og eventuelt transaksjonsreferanse
- Hva du forventer som utfall
- Relevante vedlegg (skjermbilder, kvitteringer)

2.3 Tilgjengelighet

Klagekanaler er tilgjengelige:

- På norsk og engelsk
- Uten kostnad for brukeren
- Uten krav om spesiell programvare eller utstyr utover det som kreves for å bruke Drop

---

3. Behandlingsprosess

3.1 Mottak og registrering

1. Alle klager registreres i klagehåndteringssystemet ved mottak
2. Klager tildeles unikt referansenummer
3. Mottaksbekreftelse sendes til klager innen 1 virkedag
4. Mottaksbekreftelsen inneholder:
   - Referansenummer
   - Forventet behandlingstid
   - Kontaktinformasjon for oppfølging

3.2 Kategorisering

Klager kategoriseres etter type og alvorlighetsgrad:

Kategori	Beskrivelse	Prioritet
K1: Transaksjonsfeil	Feilbelastet, dobbeltbelastet, manglende overføring	Høy
K2: Gebyrtvist	Uenighet om gebyrer eller valutakurs	Middels
K3: Tilgjengelighet	Tjeneste utilgjengelig, tekniske feil	Middels
K4: Kundeservice	Misnøye med servicenivå	Standard
K5: Personvern	Bekymring om datahåndtering	Høy
K6: Kundekontroll	Klage på KYC-prosesser eller avvisning	Middels
K7: Sperring	Konto- eller transaksjonssperring	Høy
K8: Annet	Øvrige klager	Standard

3.3 Behandling

1. Klagen tildeles saksbehandler basert på kategori og kompetanse
2. Saksbehandler gjennomgår klagen, innhenter nødvendig informasjon
3. Saksbehandler kan kontakte klager for avklaring
4. Saksbehandler utarbeider forslag til løsning
5. Ved K1 og K7: Saksbehandler kan iverksette umiddelbare tiltak (f.eks. midlertidig tilbakeføring)

3.4 Svarfrister

I henhold til PSD2 artikkel 101 og betalingstjenesteloven:

Frist	Beskrivelse
1 virkedag	Mottaksbekreftelse

Frist	Beskrivelse
15 virkedager	Endelig svar på klagen
35 virkedager	Maksimal forlenget frist ved ekstraordinære omstendigheter

Ved behov for forlenget frist (utover 15 virkedager) skal klager motta:

- Skriftlig informasjon om forsinkelsen
- Begrunnelse for hvorfor mer tid er nødvendig
- Forventet ny svardato
- Ny frist kan ikke overstige 35 virkedager totalt

3.5 Innhold i svarbrev

Svaret til klager skal inneholde:

- Referanse til klagen
- Oppsummering av forholdet som er klaget inn
- Vår vurdering og begrunnelse
- Eventuell løsning eller kompensasjon
- Informasjon om videre klageadgang (Finansklagenemnda)
- Kontaktinformasjon for oppfølging

---

4. Eskalering

4.1 Intern eskalering

Nivå	Beslutningstaker	Kriterium
Nivå 1	Saksbehandler (kundeservice)	Standard klager
Nivå 2	Teamleder kundeservice	Komplekse klager, kompensasjon > 1 000 kr
Nivå 3	Compliance-ansvarlig	Regulatoriske klager, personvern, gjentatte klager
Nivå 4	Daglig leder	Vesentlige klager, kompensasjon > 10 000 kr, systemiske problemer

4.2 Ekstern eskalering

Dersom klager ikke er tilfreds med vårt svar, informerer vi om retten til å bringe saken inn for:

Finansklagenemnda (FinKN)

- Postboks 53 Skøyen, 0212 Oslo
- Telefon: 23 13 19 60
- Nettsted: https://www.finansklagenemnda.no
- Behandling er kostnadsfri for forbrukere
- Klage til FinKN må fremsettes innen 3 år etter at klager først klaget til oss

Finanstilsynet

- For klager på selve tjenesteleverandøren eller brudd på regulatoriske krav
- Revierstredet 3, 0151 Oslo
- Telefon: 22 93 98 00
- Nettsted: https://www.finanstilsynet.no

Forbrukerrådet

- Generell forbrukerveiledning
- Sandakerveien 138, 0484 Oslo
- Telefon: 23 400 500
- Nettsted: https://www.forbrukerradet.no

4.3 Rettslig tvisteløsning

Dersom saken ikke løses gjennom nemndbehandling, kan tvisten bringes inn for norske domstoler, jf. brukervilkårene punkt 13.

---

5. Kompensasjon

5.1 Prinsipper

- Kompensasjon vurderes individuelt for hver klage
- Målet er å sette klager i den posisjonen vedkommende ville vært i uten feilen
- Kompensasjon kan inkludere tilbakeføring, gebyrfritak, eller annen godtgjørelse

5.2 Automatisk kompensasjon

Følgende utløser automatisk kompensasjon:

- Dobbeltbelastning: Umiddelbar tilbakeføring av overskytende beløp
- Feilsendt overføring (vår feil): Full tilbakeføring

- Gebyr trukket i strid med prisliste: Gebyrrefusjon

5.3 Skjønnsmessig kompensasjon

Ved forhold som ikke utløser automatisk kompensasjon, kan vi tilby:

- Gebyrfritak for fremtidige transaksjoner
- Økonomisk kompensasjon der det er rimelig
- Forbedret servicenivå (f.eks. prioritert kundeservice)

---

6. Dokumentasjon og oppbevaring

6.1 Klageregister

Alle klager dokumenteres i klageregisteret med:

- Unikt referansenummer
- Dato for mottak
- Klagers identifikasjon (anonymisert i rapporter)
- Klagekategori
- Beskrivelse av klagen
- Dato og innhold i svar
- Eventuell kompensasjon
- Status (mottatt, under behandling, besvart, avsluttet, eskalert)

6.2 Oppbevaringstid

- Klager og tilhørende dokumentasjon oppbevares i minimum 3 år etter avslutning
- Klager knyttet til transaksjoner oppbevares i henhold til bokføringsloven § 13 (5 år)
- Klager viderebrakt til Finansklagenemnda oppbevares til endelig avgjørelse + 3 år

6.3 Personvern

Behandling av personopplysninger i klagebehandlingen skjer i henhold til personvernerklæringen og GDPR. Klager har rett til innsyn i egne opplysninger, jf. GDPR artikkel 15.

---

7. Rapportering

7.1 Intern rapportering

Rapport	Frekvens	Mottaker	Innhold
Klageoversikt	Månedlig	Daglig leder	Antall, kategorier, behandlingstid, løsningsrate
Trendanalyse	Kvartalsvis	Ledelsen	Trender, gjentakende problemer, systemiske svakheter
Årsrapport	Årlig	Styret	Sammendrag, nøkkeltall, tiltak, sammenlikning med foregående år

7.2 Innhold i rapporter

- Antall mottatte klager per kategori
- Gjennomsnittlig og median behandlingstid
- Andel klager besvart innen 15 virkedager
- Antall klager eskalert til ekstern instans
- Total kompensasjon utbetalt
- Identifiserte systemiske problemer og iverksatte tiltak

7.3 Styreorientering

Styret orienteres:

- Kvartalsvis om klagestatistikk og trender
- Umiddelbart ved vesentlige klager som indikerer systemisk svikt
- Umiddelbart ved klager til Finansklagenemnda eller Finanstilsynet
- Årlig med full klageårsrapport

7.4 Rapportering til Finanstilsynet

I henhold til regulatoriske krav rapporteres:

- Vesentlige klagetyper og -trender (som del av periodisk rapportering)
- Klager som indikerer brudd på regulatoriske krav
- Utfall av saker behandlet i Finansklagenemnda

---

8. Forbedring

8.1 Rotårsaksanalyse

For gjentakende klager eller alvorlige enkeltklager gjennomføres rotårsaksanalyse:

1. Identifiser grunnleggende årsak
2. Vurder om problemet er systemisk
3. Utarbeid forbedtringstiltak
4. Implementer tiltak med ansvarlig og frist
5. Verifiser at tiltaket har effekt

8.2 Kontinuerlig forbedring

- Klagedata brukes aktivt til å forbedre tjenesten
- Produktteamet mottar anonymiserte klagerapporter
- Tiltak implementeres og effekt måles
- Forbedringer kommuniseres til brukere der relevant

8.3 Opplæring

- Kundeservicemedarbeidere gjennomgår opplæring i klagebehandling ved ansettelse
- Årlig oppdateringsopplæring for alle som behandler klager
- Casebasert opplæring ved nye typer klager

---

9. Ansvar og organisering

9.1 Roller

Rolle	Ansvar
Kundeservicemedarbeider	Mottak, registrering, behandling av nivå 1-klager
Teamleder kundeservice	Kvalitetskontroll, nivå 2-klager, coaching
Compliance-ansvarlig	Regulatoriske klager, rapportering til myndigheter, nivå 3
Daglig leder	Overordnet ansvar, styreorientering, nivå 4

9.2 Uavhengighet

Klagebehandlingen skal være uavhengig av den operative virksomheten. Compliance-ansvarlig har selvstendig rapporteringsrett til styret.

10. Regulatorisk samsvar

Denne prosedyren er utarbeidet i samsvar med:

Regulering	Krav	Dekning
PSD2 art. 101	Klageprosedyre for betalingstjenestebrukere	Hele dokumentet
PSD2 art. 101(1)	15 virkedagers svarfrist	Punkt 3.4
PSD2 art. 101(2)	Informasjon om ekstern klageadgang	Punkt 4.2
Betalingstjenesteloven kap. 3	Rettigheter og plikter ved betalingstjenester	Punkt 3, 5
Finansforetaksloven § 16-1	Klageordning for finansforetak	Hele dokumentet
GDPR art. 77	Klagerett til tilsynsmyndighet	Personvernerklæring
Angrerettloven § 22	Angrerett og klageadgang	Brukervilkår punkt 9

11. Revisjon

11.1 Gjennomgang

- **Årlig:** Full gjennomgang av prosedyren
- **Ved regulatoriske endringer:** Oppdatering iht. nye krav
- **Ved systemiske klager:** Gjennomgang og tilpasning
- **Etter Finansklagenemnda-avgjørelser:** Vurdering av behov for endringer

11.2 Versjonshistorikk

Versjon	Dato	Endring	Godkjent av
1.0	12.02.2026	Opprinnelig dokument	_____

Denne klagebehandlingsprosedyren er eid av compliance-ansvarlig og godkjent av daglig leder i ALAI Holding AS.