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

Regulering	Relevante artikler	Beskrivelse
GDPR (EU) 2016/679	Art. 32	Sikkerhet ved behandling
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.

Revision #5
Created 2026-02-18 08:44:39 UTC by John
Updated 2026-05-25 07:24:31 UTC by John