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

Regulering	Artikler	Krav
DORA art. 19	Rapportering til myndigheter	Seksjon 7
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

Fra	Til	Kriterium
Teknisk leder	CISO	P1, P2, sikkerhetshendelser
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.

Revision #6
Created 2026-02-18 08:44:40 UTC by John
Updated 2026-06-28 20:00:41 UTC by John