Risiko- og sårbarhetsanalyse (ROS)

Versjon 1.0 · 6. mai 2026 (sist oppdatert 29. mai med MFA-tillegg) · Ansvarlig: Markus Eriksson (Påvakt AS)

> **Scope:** DigiReq (mobil-app + backend + admin-dashboard) i pilot- og tidlig-produksjonsfase. **Vurderings-periode:** Frem til neste vurdering (årlig eller ved vesentlige endringer).

1. Formål

Identifisere og vurdere risiko som DigiReq sin behandling av personopplysninger kan påføre brukerne (ansatte i kommuner og kommunale foretak). Dokumentet er en del av leverandørens internkontroll iht. personopplysningsforskriften, og deles med behandlingsansvarlig (kunden) ved forespørsel.

2. Metodikk

2.1 Sannsynlighet

- **Lav** — mindre enn én forventet hendelse per år
- **Middels** — 1-5 forventede hendelser per år
- **Høy** — mer enn 5 forventede hendelser per år

2.2 Konsekvens

- **Lav** — mindre forstyrrelse, ingen vedvarende skade
- **Middels** — driftsforstyrrelse, kortvarig nedetid eller datatap som kan rekonstrueres
- **Høy** — brudd på personvern eller GDPR; dataeksponering for én kunde; kostbar restitusjon
- **Kritisk** — brudd på flere kunder; varig datatap; vesentlig omdømmeskade

2.3 Risiko-nivå

- 🟢 **Akseptabel** — ingen handling nødvendig utover overvåkning
- 🟡 **Bør reduseres** — skal følges opp innen 6 måneder
- 🔴 **Må reduseres** — skal følges opp umiddelbart

3. Identifiserte trusler

3.1 Uautorisert tilgang via stjålet/kompromittert telefon

- **Sannsynlighet:** Middels · **Konsekvens:** Middels · **Risiko:** 🟡 Bør reduseres
- **Trussel:** Bruker mister telefon med åpen DigiReq-sesjon. Tyv kan opprette eller godkjenne rekvisisjoner inntil sesjonen utløper.
- **Tiltak:** Biometri (Face ID/fingeravtrykk) for å åpne app. Refresh-token utløper etter 30 dager. Brukers admin kan deaktivere konto øyeblikkelig. JWT-tokens lagret i Keychain/Keystore — ikke tilgjengelig uten enhets-passcode.
- **Restrisiko:** Lav. Bruker uten skjermlås er fortsatt en risiko — anbefalt at kunde har MDM-policy som tvinger skjermlås.

3.2 SIM-swap eller OTP-intercept

- **Sannsynlighet:** Lav · **Konsekvens:** Høy (særlig kritisk for admin/godkjenner) · **Risiko:** 🟡 Bør reduseres
- **Trussel:** Angriper får SIM-en til en bruker (SIM-swap-svindel) og kan motta OTP-koder.
- **Tiltak:** OTP utløper etter 5 minutter. Maks 5 feil-forsøk. Audit-logg fanger uvanlig innloggingsmønster (ny IP, ny enhet). Biometri som ekstra lag etter første innlogging. **For admin/godkjenner: anbefalt at kunden slår på `require_oidc_for_admin` slik at SMS-OTP avvises og bare Entra ID-pålogging med MFA tillates** (se 3.2b).
- **Restrisiko:** Lav for employee-rollen. For admin/godkjenner: lav når Entra+MFA er aktivert; ellers middels.

3.2b Admin-konto kompromittert (phishing, gjenbrukt passord, manglende MFA)

- **Sannsynlighet:** Middels uten MFA / Lav med MFA · **Konsekvens:** Høy · **Risiko:** 🔴 uten MFA / 🟢 med MFA
- **Trussel:** Admin- eller godkjenner-konto kompromittert gjennom phishing, gjenbrukt passord på Microsoft-konto, eller fravær av MFA. Angriper kan opprette/godkjenne

rekvisisjoner, endre terskler, invitere falske brukere, eller eksfiltrere audit-data.

- **Tiltak: Anbefalt baseline: alle admin-/godkjenner-roller pålogges via Microsoft Entra ID med Conditional Access som krever MFA**. Kunden slår på `require_oidc_for_admin` i admin-dashbordet → SMS-OTP avvises for privilegerte roller. MFA håndheves i kundens egen Entra-tenant (Authenticator, FIDO2 eller sertifikat). Audit-logg fanger alle privilegerte handlinger med actor + timestamp + IP. Sesjons-TTL 60 min for access, 60 dager for refresh.
- **Restrisiko:** Lav når Entra+MFA er aktivert. Kunder uten Microsoft 365 må bruke SMS-OTP (samme nivå som 3.2).

3.3 Skjermbilde-misbruk av godkjent rekvisisjonsnummer

- **Sannsynlighet:** Lav · **Konsekvens:** Middels · **Risiko:** 🟢 Akseptabel for pilot
- **Trussel:** Ansatt tar skjermbilde av godkjent rekvisisjonsnummer og deler det. Andre bruker det til uautoriserte kjøp.
- **Tiltak:** Faktura-matching mot rekvisisjon i etterkant fanger dobbeltbruk. Audit-logg gir sporbarhet.
- **Restrisiko:** Lav. Vurderes å implementere tids-begrensning på "vis i butikk"-skjerm.

3.4 Insider-misbruk fra admin

- **Sannsynlighet:** Lav · **Konsekvens:** Høy · **Risiko:** 🟡 Bør reduseres
- **Trussel:** Admin i et firma misbruker sin tilgang — endrer roller, sletter brukere, leser data uten saklig grunn.
- **Tiltak:** Alle admin-handlinger logges i `audit_log` med actor_id, IP, tidspunkt. Rolle-endringer og bruker-invitasjoner er sporbare og synlige for andre admins. Audit-logg kan eksporteres for HR/intern-revisjon.
- **Restrisiko:** Lav. Kan styrkes med "to-admin-godkjenning" for kritiske operasjoner — vurderes ved skala.

3.5 Super_admin (plattform-eier) misbruker tilgang til kundedata

- **Sannsynlighet:** Lav · **Konsekvens:** Kritisk · **Risiko:** 🟡 Bør reduseres
- **Trussel:** Plattform-eier (DigiReq/Markus) ser kunders rekvisisjons-data uten saklig grunn.
- **Tiltak:** Super_admin har **kun** tilgang til organisasjons-data via dedikerte `/superadmin/*`-endepunkter. Ingen automatisk tilgang til rekvisisjons-data på tvers av firmaer. Alle

super_admin-handlinger logges som "suspicious" og flagges automatisk i kundens audit-visning.

- **Restrisiko:** Lav. For å støtte/feilsøke må super_admin midlertidig promoteres til admin der — det skaper en audit-rad kunden ser.

3.6 Sub-prosessor-utfall (Hetzner / Cloudflare / Expo / 46elks)

- **Sannsynlighet:** Lav · **Konsekvens:** Middels-Høy · **Risiko:** 🟡 Bør reduseres
- **Trussel:** Kritisk underleverandør har lengre nedetid, datatap eller sikkerhetsbrudd.
- **Tiltak:** Hetzner: daglig kryptert backup, redundans innen Helsinki-datasenter. Cloudflare: tjenesten fungerer ved CF-nedetid. Expo: push-utfall stopper notiser, men ikke kjernefunksjonen. 46elks: utfall stopper innlogging — eneste single-point-of-failure.
- **Restrisiko:** Middels på 46elks. Fallback til alternativ leverandør vurderes når kunde-base er stor nok.

3.7 DDoS / API-misbruk

- **Sannsynlighet:** Lav · **Konsekvens:** Lav-Middels · **Risiko:** 🟢 Akseptabel
- **Trussel:** Angriper sender massive requests for å gjøre tjenesten utilgjengelig eller forbruke SMS-budsjett.
- **Tiltak:** Cloudflare DDoS-beskyttelse. Nginx rate-limit: 10 req/min/IP på autentisering, 300 req/min per JWT på API. OTP-spesifikt rate-limit per telefon per time. Fail2ban på SSH. UFW-firewall — kun port 80/443 åpne.
- **Restrisiko:** Lav.

3.8 Avhengighets-sårbarhet (CVE i bibliotek)

- **Sannsynlighet:** Middels · **Konsekvens:** Varierer · **Risiko:** 🟢 Akseptabel (etter Dependabot-aktivering 29. mai 2026)
- **Trussel:** Sårbarhet i tredjeparts-bibliotek (Flask, Expo SDK, react-native, npm/pip-pakker) utnyttes.
- **Tiltak:** GitHub Dependabot overvåker alle deps kontinuerlig; CVE-er genererer auto-PR-er gruppert per økosystem. Sårbare versjoner oppdateres innen 7 dager (kritiske: 24 timer). `unattended-upgrades` aktiv på VPS for OS-patches. Manuell gjennomgang før hver release.
- **Restrisiko:** Lav.

3.9 Datatap (database-korrupsjon, server-feil, slettings-feil)

- **Sannsynlighet:** Lav · **Konsekvens:** Høy · **Risiko:** 🟡 Bør reduseres
- **Trussel:** Database-korrupsjon, ved-uhell-sletting, eller server-feil fører til tap av kundedata.
- **Tiltak:** Hetzner snapshots: kryptert, daglig, 7 dagers oppbevaring. Backup i samme datasenter (Helsinki). Restore-prosedyre testet ved oppsett. Audit-logg kan brukes til å rekonstruere kritiske handlinger ved delvis tap.
- **Restrisiko:** Lav-Middels. Cross-region backup vurderes når kundebase rettferdiggjør kostnaden.

3.10 GDPR-brudd ved feil retention eller manglende sletting

- **Sannsynlighet:** Lav · **Konsekvens:** Høy · **Risiko:** 🟡 Bør reduseres
- **Trussel:** Personopplysninger oppbevares lenger enn tillatt, eller ikke slettes ved bruker-forespørsel.
- **Tiltak:** Audit-logg slettes automatisk etter 12 mnd via cron. OTP slettes umiddelbart etter consumed/expired. Sletting-forespørsler håndteres innen 30 dager (se /data-rettigheter). Rekvisisjoner beholdes 5 år iht. bokføringsloven.
- **Restrisiko:** Lav. Anbefalt manuell test av sletting-flyt 2× per år.

3.11 Sikkerhetsbrudd hos behandlingsansvarlig (kunden) som påvirker DigiReq

- **Sannsynlighet:** Middels · **Konsekvens:** Middels · **Risiko:** 🟡 Bør reduseres
- **Trussel:** Kunde-admin sin konto blir kompromittert (kommune-IT-brudd, phishing, tap av enhet).
- **Tiltak:** Tenant-isolasjon på `company_id` forhindrer at brudd sprer seg. Audit-logg detekterer uvanlige rolle-endringer. Kompromittert konto kan deaktiveres øyeblikkelig av super_admin eller annen admin. Med `require_oidc_for_admin` + Entra-MFA er admin-rollen MFA-beskyttet.
- **Restrisiko:** Lav når kunden bruker Entra+MFA; ellers middels.

3.12 Sårbarhet i mobilapp (jailbreak, repackaging)

- **Sannsynlighet:** Lav · **Konsekvens:** Middels · **Risiko:** 🟢 Akseptabel for pilot
- **Trussel:** Angriper jailbreaker/rooter telefon og henter ut tokens fra Keychain/Keystore, eller repackager APK-en.

- **Tiltak:** Tokens lagret i platformens sikre lager. Refresh-tokens utløper. Audit-logg ser uvanlig token-bruk. Distribusjon via Apple/Google sine offisielle stores.
- **Restrisiko:** Lav. Jailbreak/root-deteksjon kan vurderes ved kommersiell utrullng.

3.13 Misbruk av super_admin for å opprette firma og klone data

- **Sannsynlighet:** Lav · **Konsekvens:** Lav · **Risiko:** 🟢 Akseptabel
- **Trussel:** Super_admin oppretter ekstra firma-rekord uten saklig grunn.
- **Tiltak:** Alle `superadmin.company.create`-handlinger flagges automatisk i audit-logg. Audit-eksport kan deles med revisor.
- **Restrisiko:** Lav.

3.14 Mistede push-notiser (leverandør-utfall) gir falsk tillit

- **Sannsynlighet:** Middels · **Konsekvens:** Lav · **Risiko:** 🟢 Akseptabel
- **Trussel:** Push-utfall hos Apple/Google/Expo gjør at godkjenning ikke leveres → leder antar "alt godt" mens ansatt venter.
- **Tiltak:** App poller tilstand ved focus + foreground. Pending-listen er primær kilde, push er bare hint. Audit-logg viser når godkjenning faktisk skjedde.
- **Restrisiko:** Lav.

3.15 Plattform-konsentrasjon: Påvakt AS som eneste eier

- **Sannsynlighet:** Lav · **Konsekvens:** Kritisk · **Risiko:** 🟡 Bør reduseres
- **Trussel:** Markus Eriksson (eneste tilgang til produksjon) blir utilgjengelig.
- **Tiltak:** Alt deploy- og konfigurasjons-arbeid er dokumentert i versjonskontrollert driftsinstruks. SSH-tilgang og credentials i Påvakt AS sin sikre dokumentasjon. Beredskapskontakt: Medeier i Påvakt AS – Digireq har instrukser.
- **Restrisiko:** Middels. Akseptert for pilot-fase. Reduseres ved første ansettelse / co-founder.

4. Restrisiko-oppsummering

Etter implementerte tiltak er **alle identifiserte risikoer på akseptabelt nivå** for pilot- og tidlig-produksjonsbruk. Tre områder krever oppmerksomhet i nærmeste framtid:

1. **Avhengighets-skanning** — Dependabot aktivert 29. mai 2026, drift dokumenteres på /sikkerhet § 11
2. **MFA på admin-rolle** — anbefales via Entra+CA (se /sikkerhet § 4.3); kommunikasjon med kunder pågår
3. **Plattform-bus-faktor** — co-founder eller dokumentert beredskap når kundebase vokser

5. Oppfølging

- **Markus Eriksson, hver 6. mnd:** Manuell gjennomgang av alle trusler, justering ved nye funn
- **Markus Eriksson, ved hver vesentlig endring:** Oppdatering når ny funksjonalitet, ny sub-prosessor, eller ny rolle introduseres
- **Kundens admin, ved behov:** Eksport av audit-logg for intern-revisjon
- **Datatilsynet, aldri proaktivt:** ROS deles ved tilsynsforespørsel

6. Referanser

- Personvernerklæring
- Databehandleravtale
- Sikkerhetsoversikt
- Underleverandør-liste
- Personopplysningsloven, GDPR (forordning EU 2016/679)
- Datatilsynets veileder: `datatilsynet.no/personvern-pa-ulike-omrader/internkontroll-og-informasjonssikkerhet`

Dokument-versjon 1.1 · Sist oppdatert 29. mai 2026 (lagt til 3.2b admin-MFA, oppdatert 3.8 etter Dependabot-aktivering, oppdatert 3.11) · sikkerhet@digireq.no

OM LEVERANDØREN

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

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