Informasjonssikkerhetshåndbok og IKT-reglement for Lillehammer, Gausdal og Øyer

Versjon 0.7

1 Innledning

Informasjonssikkerhetshåndboken beskriver regler og retningslinjer for behandling av informasjon for å ivareta informasjonssikkerheten og personvernet til
våre **samarbeidsparter, innbyggere, ansatte og elever.**

Hva er informasjonssikkerhet?

Informasjonssikkerhet handler om sikring av informasjonsverdier med betydning for både offentlig forvaltning, virksomheter, organisasjoner og enkeltpersoner, derfor angår det oss alle.

Tilgang til informasjon og informasjonssikring skal ikke være to motstridende interesser. Målet med informasjonssikring er å sikre informasjonen mot misbruk.

Kravene til sikring av informasjon bestemmes i hovedsak av to faktorer:

1. informasjonenes innhold
2. hvilken sammenheng den behandles i

Den største trusselen mot informasjonssikkerheten er vår manglende forståelse for behovet for sikring. Det kan handle om manglende sikring eller om manglende kompetanse. Sikringstiltak, systematikk, rutiner og prosedyrer skal ivareta informasjonssikkerheten på en formell, systematisk og etterprøvbar måte.

Informasjonssikkerhet er knyttet til behandling av personopplysninger. Innholdet her gjelder behandling av både sensitive og ikke sensitive personopplysninger om ansatte, elever, barnehagebarn, tjenestemottakere og andre kommunen behandler personopplysninger om.

Personvern

Det er viktig å ha en saklig grunn (begrunnet og lovlig formål) for å behandle personopplysninger. Grunnlag for behandling er normalt basert på lovhjemmel eller samtykke fra den registrerte. Uavhengig av grunnlaget har virksomheten plikt til å informere den registrerte om hvordan den har tenkt å behandle opplysningene. Det betyr at det må informeres om formål, rettigheter og lagringstid for opplysningene.

Bestemmelser

Informasjonssikkerhetshåndboken er vedtatt i kommunedirektørens ledergruppe, og gjelder for alle som skal ha tilgang til våre IT-systemer. Bestemmelsene i håndboken gjelder for all behandling av informasjon i kommunene. Intern informasjon, offentlig informasjon, informasjon unntatt fra offentlighet eller personopplysninger - herunder sensitive personopplysninger.

Mål

All informasjon skal sikres slik at den ikke blir kjent for uvedkommende, misbrukt, manipulert eller unødig går tapt. Informasjon skal fordeles etter tjenstlige behov. Informasjonssikkerhet handler om:

Konfidensialitet

Personopplysninger og annen beskyttelsesverdig informasjon som behandles i *kommunen* skal være beskyttet mot uautorisert tilgang.

Personopplysninger behandles konfidensielt og kan bare deles med andre medarbeidere i den grad det er tjenstlige behov.

Personopplysninger om egne arbeidstakere kan kun behandles av den som har tjenstlig behov.

Integritet

Informasjon som *kommunen* har ansvaret for blir bare produsert og endret av ansatte, eller av eksterne som har fullmakt til dette.
Informasjon skal ikke endres utilsiktet.

Tilgjengelighet

Informasjonssystemet er tilgjengelig for autoriserte brukere ved behov.

Robusthet

Virksomheten og informasjonssystemet er motstandsdyktig og robust.
Når uønskede fysiske eller tekniske hendelser inntreffer, bidrar beredskapstiltak til å begrense skaden og at *kommunen* raskt kommer tilbake til normal drift. Dette inkluderer å gjenopprette tilgjengelighet og tilgang til personopplysninger i rett tid.

I kommunen skal vi beskytte informasjonen og informasjonssystemene slik at informasjon ikke kommer på avveie. Kommunene skal sikre at behandlingen av informasjon oppfyller lovpålagte krav, kontraktsmessige forpliktelser og dekker behovet for personvern og etisk ansvar. Informasjonssikkerhetshåndboken skal til enhver tid være i tråd med Grunnloven, personopplysningsloven, forvaltningsloven, kommuneloven, offentlighetsloven, arkivloven og andre relevante særlover.

Det skal utarbeides og tas i bruk rutinebeskrivelser for behandling av informasjon i systemer og fagområder, som er i tråd med gjeldende lovverk. Alle som benytter kommunens systemer, er forpliktet til å kjenne til og følge informasjonssikkerhetshåndboken.

Målsettinger for å lykkes med informasjonssikkerhet- og personvernarbeidet:

- Det er etablert en sikkerhetsorganisasjon med klare ansvars- og myndighetsforhold (Se punkt om organisering og ansvar)
- Arbeidet med informasjonssikkerhet skal forankres i øverste ledelse og inngå i ansvarsområdet en leder til enhver tid har. (Se punkt om organisering og ansvar).
- Alle behandlinger av personopplysninger skal være registrert i kommunens behandlingsprotokoller.
- Det skal gjennomføres risikovurderinger av systemer hvor det behandles personopplysninger slik at disse er oppdatert til enhver tid.
- IKT-tekniske løsninger skal støtte opp om sikkerhetsmål og strategier gjennom tilfredsstillende forvaltning av utstyr, system og data
- Tilgang til systemer og informasjon gis til ansatte etter tjenesterelaterte behov
- Det skal gis opplæring og informasjon til ansatte som bruker kommunens datasystem for å sikre at gjeldende sikkerhetskrav blir ivaretatt
- Uvedkommende skal hindres tilgang til systemer og informasjon
- Det skal sikres at personopplysninger ikke forandres utilsiktet eller uautorisert
- Det skal være mulig å spore uønskede hendelser knyttet til bruk av kommunens datasystem der dette er hensiktsmessig og/eller lovpålagt
- Fysisk sikring skal hindre at uautoriserte får adgang til lokaler der personopplysninger lagres og behandles
- Det er rutiner og prosesser for å håndtere uønskede hendelser, avvik rapporteres i f.t. TQM
- Det skal gjennomføres tilfredsstillende intern kontroll, herunder sikkerhetsrevisjoner og ledelsens årlige gjennomgang

2 Informasjonssikkerhet for alle ansatte

2.1 Adgangskontroll

- Adgang til lokaler begrenses til autorisert personale.
- Alle medarbeidere skal, der det er hensiktsmessig, bære synlig identifikasjon.
- Besøksregistrering skal benyttes der det er tilgjengelig.

2.2 Tilgang og brukerkontroll

1. Alle ansatte får tildelt brukernavn og passord som oppgis for å autentisere den ansatte og gi tilgang til kommunenes IT-utstyr, systemer og nettverk. Smartkort benyttes i tillegg for tilgang til enkelte pasientjournalsystem. Fellesbrukere skal ikke opprettes i kommunens systemer.
2. Passordet skal holdes hemmelig for andre, og det skal læres utenat eller oppbevares på en sikker måte.
3. Det skal benyttes MFA/2-faktorautentisering alle steder hvor det er støtte for dette.

4. Passordets kompleksitet (lengde/bruk av spesialtegn osv.) skal følge gjeldende anbefalinger fra rådgivende organisasjoner som Nasjonal Sikkerhetsmyndighet (NSM), Kommune CSIRT og andre.
5. Hvis ansatte har glemt passordet, eller mistenker at passordet er blitt kjent for andre, skal den ansatte endre passordet umiddelbart.
6. Det er ikke tiltatt å bruke en annens brukernavn og passord. Passord som benyttes i kommunens systemer skal ikke brukes på dine private apper og tjenester.
7. Adgangskort og Smartkort skal ikke lånes bort.
8. Konsulenter, vikarer og andre som skal ha tilgang til IT-systemene skal ha undertegnet taushetserklæring. Taushetserklæringen inneholder en bestemmelse som forplikter den ansatte til informasjonssikkerhetshåndboken. Ansatte skal ha undertegnet en ansettelseskontrakt der dette er ivaretatt.
9. Når ansatte forlater PC-en, nettbrett, mobiltelefon m.m. skal skjermen låses.

2.3 Bruk av IT-systemer, lagring og behandling av data

Informasjon som lagres på kommunens IT-systemer skal være jobbrelatert.
Det er kun lov til å benytte IT-systemer/skytjenester som er godkjent for bruk i kommunen. All lagring av data skal være i henhold til lovverk. Ansatte skal rapportere forhold som kan ha betydning for informasjonssikkerhet til sin leder så raskt som mulig. Bruk av kommunes systemer og nettverk loggføres. Aktiviteter registreres og kan spores tilbake til den enkelte bruker.

Disse tjenestene skal benyttes:

- Filserver hos Ikomm
- Skylagring og epost hos Microsoft. Se kommunens egne retningslinjer for bruk og lagring i Microsoft 365
- Fagsystem og apper som er anskaffet og risikovurdert.
- Sensitiv og/eller gradert informasjon skal aldri lagres lokalt.
- Unntaksvis kan lagring skje på lokale lagringsmedier (blant annet lokal maskin) under forutsetning av at disse er krypterte og beskyttet med godkjent metode.
- Eksterne lagringsmedier (minnepinner etc.) skal ikke benyttes.

2.3.1 Lagring og behandling av sensitiv informasjon.

- Som sensitiv informasjon regnes f.eks. personopplysninger, sensitive personopplysninger, gradert og virksomhetskritiske data.
- Sensitive personopplysninger skal lagres i egnet fagsystem.
- Sensitiv informasjon skal kun deles elektronisk via godkjente løsninger.
- Papirkopier med sensitiv data skal oppbevares i låsbart rom eller skap og skal makuleres ved avhending.

2.4 Mobile enheter (mobiltelefon, nettbrett, PC)

Følgende gjelder for alle mobile enheter (mobiltelefon, nettbrett, PC) med tilgang til kommunens løsninger, eksempelvis e-post, Teams mm.:

- Leder skal varsles hvis IKT-utstyr eller mobiltelefon blir stjålet eller mistet.
- Kommunens enheter skal ikke lånes bort.
- Enheter brukt i arbeidssammenheng skal ikke etterlates ubevoktet på offentlig sted. De skal alltid fraktes som håndbagasje og låses inn når bruker ikke er til stede.
- Passord eller kode skal benyttes for å komme inn på enheten (kode med minimum 6 tegn for mobil og nettbrett)
- Antivirus/endepunktsikring skal benyttes. Det skal skilles på privat og jobbsone.
- Bruk mobildata, ikke åpne trådløse nett hvor du ikke blir avkrevd eget passord)
- For å ivareta personvernet og taushetsplikten er det ikke lov å bruke mobiltelefon, nettbrett eller andre mobile enheter til å ta bilder, video eller lydopptak av elever, barnehagebarn, pasienter, pårørende eller ansatte. Ved behov for denne type bilder skal kommunens eget egnede utstyr benyttes.
- Hvilke tillatelser skal den enkelte ansatte ha på sine mobile enheter? Applocker/Localadmin? Antivirus/endepunktssikring? Under arbeid.
- Hvilke retningslinjer skal gjelde for synkronisering til lokal disk/enhet? Under arbeid.
- Den ansatte er ansvarlig for å tilbakestille telefonen til fabrikkinnstillingene før den avhendes eller overtas av andre for videre bruk.

2.4.1 Arbeidstakere med stilling som behandler sensitive personopplysninger

Privat/personlig mobiltelefon må ikke benyttes til håndtering av sensitive personopplysninger. Arbeidstakere med stilling som innebærer at hans/hennes mobiltelefon kan inneholde sensitive opplysninger om enkeltpersoner/klienter, f.eks. SMS, skal ha egen mobiltelefon til tjenstlig bruk. Mobilen er knyttet til en bestemt arbeidstaker, benyttes kun til tjenstlig bruk og oppbevares på arbeidsplassen på et sikkert sted.
Det er leder som vurderer om den enkelte stilling er av en slik karakter at den ansattes mobiltelefon skal benyttes i jobbsammenheng eller om den også kan benyttes privat.

2.5 Bruk av e-post og kalender

- Bruk av e-post skal være jobbrelatert.
- Bruk av kommunens e-postadresser til privat kommunikasjon skal unngås.
- E-post skal avsluttes med navn, tittel og virksomhetsnavn i henhold til kommunens mal for signatur.
- Kontroller alltid avsenders adresse. Åpne aldri vedlegg eller linker fra avsendere du ikke kjenner eller forventer noe fra.
- Kontroller alltid at du sender epost til riktig mottaker(e), slik at utilsiktet distribusjon av epost unngås. Vær spesielt oppmerksom ved bruk av epostgrupper.

- Automatisk videresending av epost til andre adresser skal unngås. Videresending til private epostadresser er ikke tillatt.
- Bruk av andre ansattes e-postadresser for sending av e-post er ikke tillatt uten samtykke fra den som eier e-postkontoen.
- Sensitive personopplysninger og informasjon unntatt offentlighet skal ikke sendes per epost.
- Vær restriktiv med å oppgi din e-postadresse, og med hva du svarer eller abonnerer på av nyhetslister og lignende. Dette for å hindre unødig risikoeksponering som virus, spam, innbruddsforsøk og lignende.
- Kalendere skal brukes for at sentralbord og kollegaer skal ha oversikt over ansattes tilgjengelighet, ferier osv..
- Kalendere skal som standard være åpne av hensyn til tilgjengelighet og åpenhet. Møtedetaljer/agenda kan ved behov sendes i egen epost. Sensitiv informasjon skal aldri legges inn i kalender.
- Ved planlagt fravær skal fraværsassistenten benyttes med melding om fravær og eventuell kontaktinformasjon til andre.

2.6 Når arbeidsforholdet opphører

Brukertilgangen blir stanset ved opphør av ansattforhold og dine lagrede dokumenter og eposter vil bli slettet. Du må forsikre deg om at informasjon som eies av organisasjonen er overlevert organisasjonen og ikke blir liggende igjen på dine personlige områder. Utstyr, nøkler, adgangskort osv. som tilhører organisasjonen skal tilbakeleveres.

2.7 Avhending av IT-utstyr

Alle PC'er skal innleveres til Ikomm for sikker sletting og avhending. Ikomm tar også imot annet IT-utstyr (EE-avfall) hvor det er eller har vært lagret informasjon. Avtal med din leder hvordan bestilling/avhending skal skje.

2.8 Avvik og/eller brudd på personopplysningssikkerhet for ansatte

Ved oppdagelse av brudd på informasjonssikkerheten eller personvernet, er det ditt ansvar å rapportere til nærmeste leder og sørge for at det opprettes et avvik i TQM.

Brudd på Personopplysningssikkerheten skal varsles til:

- Personvernombudet
- Fagansvarlig for informasjonssikkerhet
- Datatilsynet via Altinn **innen 72 timer.**

3 Informasjonssikkerhet for ledere

Som leder er man også en ansatt. Derfor gjelder alle kravene til ansatte også for ledere.

3.1 Tilgang og brukerkontroll

Lederen er ansvarlig for at ansatte har undertegnet ansettelseskontrakt og taushetserklæring før de får tilgang til IT- og fagsystemene.

Lederen skal sørge for at ansatte i sin virksomhet er registrert hos IKOMM slik at brukeren kan få utdelt brukernavn og passord og tilgang til kommunes IT-utstyr, fagsystemer og nettverk.

Lederen er ansvarlig for at ansattes gis tilgang til systemer og programmer og at tilgangene til enhver tid er begrenset til kun det de har behov for i jobben.

Lederen er ansvarlig for å gi riktig tilgang til enhetens lokaler.

3.2 Lagring og behandling av data

Leder har ansvar for at ansatte følger retningslinjene for lagring og bruk av fagsystemer. (Vis til disse) Dette betyr også dokumentbehandling i fagsystemene, på hjemme- eller fellesområdet eller i Teams, SharePoint og OneDrive for kommune. Leder har ansvar for at formålet med behandling av personopplysninger skal registreres. Det skal utarbeides ros-analyser ved nye system eller større endringer i et fagsystem.

3.3 Behandling av sensitive opplysninger

Leder er ansvarlig for å sikre at ansatte er kjent med og følger rutiner for behandling av sensitive opplysninger i systemene. Ledere skal ha informasjonssikkerhet som tema jevnlig på møter i virksomheten.

3.4 Anskaffelse av IT-utstyr og programvare/lisenser

Leder skal sørge for at ansattes IT-utstyr anskaffes i henhold til kommunenes innkjøpsavtaler. PC'er skal anskaffes og konfigureres via Ikomm.

3.5 Avhending av IT-utstyr

Alle PC'er skal innleveres til Ikomm for sikker sletting og avhending. Ikomm tar også imot annet IT-utstyr (EE-avfall). Avtal alltid tidspunkt for henting/levering av datautstyr med Ikomm.
Vær oppmerksom på at det kan være egne rutiner for avhending av andre typer utstyr som kan være leaset, inneholde informasjon eller av andre årsaker avhendes på spesiell måte.

3.6 Opplæring

Leder er ansvarlig for at ansatte kjenner til og har lest informasjonssikkerhetshåndboken og andre retningslinjer og rutiner.

Leder er ansvarlig for at ansatte får tilstrekkelig opplæring i de systemene som skal benyttes. Dette innbefatter:

- grunnleggende IT og Windows kompetanse
- grunnleggende kompetanse i Microsoft Office programmer og hva som skal lagres hvor
- opplæring i fagprogram
- kunnskap om innholdet i informasjonssikkerhetshåndboken

3.7 Når ansatte slutter

Leder er ansvarlig for å ha rutiner for avslutning av ansattforhold som inneholder blant annet disse punktene:

Leder er ansvarlig for å melde opphør av ansattforhold i lønnssystemet.
Leder er ansvarlig for at innsamling av nøkler, smartkort og ID-kort.
Leder er ansvarlig for tilgang til nettverk, system, data og skytjenester opphører.
Leder er ansvarlig for innlevering av utstyr.

3.8 Avvik og/eller brudd på personopplysningssikkerhet

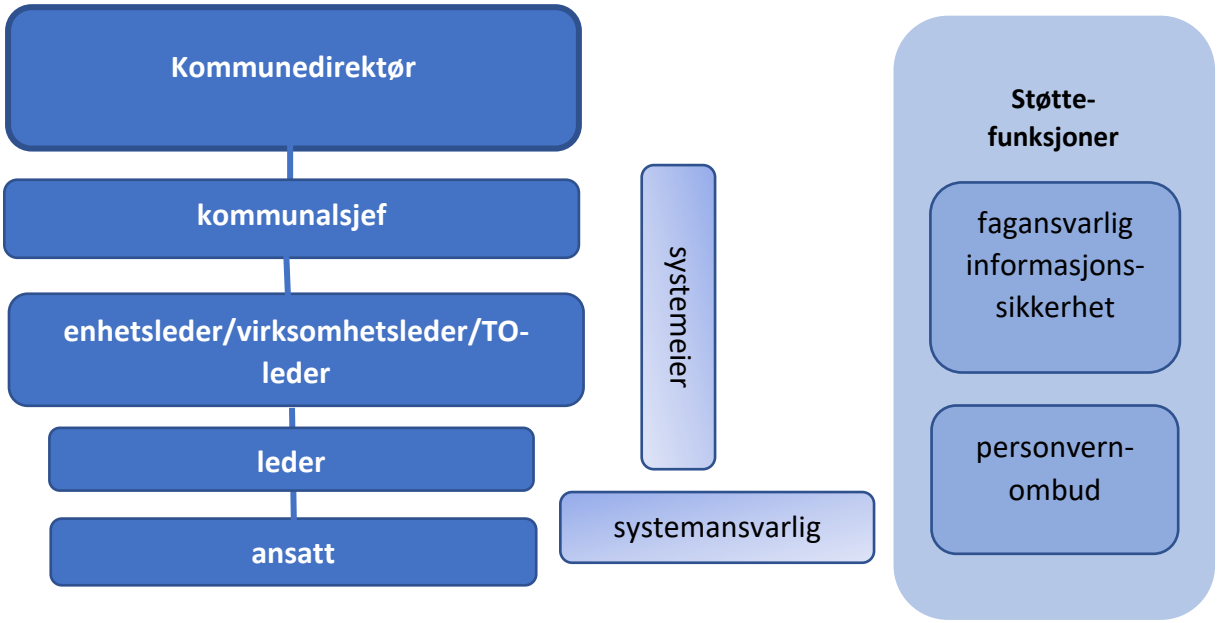
Leder har ansvar for at alle i virksomheten kjenner til hvordan avvik skal registreres i TQM avvikssystem. Dette skal gjøres med en gang avviket er oppdaget.

Brudd på Personopplysningssikkerheten skal varsles til:

- Personvernombudet
- Fagansvarlig for informasjonssikkerhet
- Datatilsynet via Altinn innen 72 timer. Se egen prosedyre.

4 Sikkerhetsorganisasjon - organisering og ansvar

Ansvaret for at informasjonssikkerhetshåndboken og tilhørende retningslinjer og prosedyrer overholdes følger linjeledelsen. Det vil si at det utøvende ansvaret for informasjonssikkerhet kan delegeres i linja fra kommunedirektør ned til enhetsledere/virksomhetsledere/TO-ledere. For å sikre lovbestemt oppfølging av informasjonssikkerhetsarbeidet er dette en del av ledelsens årlige gjennomgang.



4.1 Roller

Alle ansatte i kommunen skal overholde informasjonssikkerhetsreglementet, og beskytte verdien som ligger av informasjon i fagsystemer, elektroniske enheter og infrastruktur.

Kommunedirektøren og ledere

Kommunedirektøren har hovedansvaret for informasjonssikkerhet og behandling av personopplysninger i kommunen. Det daglige ansvaret er delegert i linjen til enhetsleder/virksomhetsleder/TO-leder som er *behandlingsansvarlig* for den aktuelle behandlingen. Delegeringen omfatter kun oppgavene, ikke det overordnede ansvaret.

Den enkelte leder har det daglige ansvaret for den praktiske oppfølgingen av sikkerhetsarbeidet i egen virksomhet. Leder er også ansvarlig for å initiere og bistå i risikovurderinger. For råd og veiledning ta kontakt med fagansvarlig for informasjonssikkerhet.

Virksomhetsleder er ansvarlig for å behandle personopplysninger på en lovlig, rettferdig og gjennomsiktig måte, ha et behandlingsgrunnlag, behandle

personopplysningene på en sikker måte og sikre at de registrerte får utøvd sine rettigheter.

Virksomhetsleder må sørge for å etablere alle nødvendige organisatoriske og tekniske tiltak for å sikre at regelverket etterleves til enhver tid. Virksomhetsleder må kunne dokumentere at den opptrer i samsvar med reglene. Dette gjelder også med hensyn til forsvarlig valg av databehandler. Virksomhetsleder kan med andre ord ikke frasi seg ansvaret for å etterleve regelverket fordi selve behandlingen av personopplysningene skjer hos en annen virksomhet.

Fagansvarlig informasjonssikkerhet

Fagansvarlig informasjonssikkerhet skal være pådriver og rådgiver for trygg og god forvaltning av kommunens informasjon og gi råd til ansatte og ledere i informasjonssikkerhetsspørsmål. Drive holdningsskapende arbeid, spre kunnskap og være en pådriver for fagfeltet.

Involveres i arbeid med risikovurderinger ved innføring av nye eller ved endring av eksisterende IKT-løsninger og ved revisjoner.

Personvernombud

Personvernombudet skal bistå kommunen i spørsmål om personvern og informasjonssikkerhet. Personvernombudet har taushetsplikt, skal ikke motta instruksjoner i forbindelse med utføring av oppgavene som personvernombud og rapporterer til kommunedirektørens ledergruppe.
Personvernombudet kontrollerer overholdelse av forordningen og skal kunne gi råd i personvernkonsekvensutredninger og kontrollere gjennomføringen av den.

Ved brudd på personvernlovgivning skal personvernombudet varsles.

Elever

Elever er brukere av kommunenes IT-systemer og det er viktig at kommunen sikrer at disse også følger de kommunale retningslinjene for informasjonssikkerhet. Dette er en spesielt sårbar gruppe som må tas ekstra hensyn til ved vurdering av personvern og informasjonssikkerhet.

IT-drift (Ikomm, samt flere leverandører)

IT-driftsleverandør (Ikomm m.fl.) er ansvarlig for at informasjonssikkerheten ivaretas i infrastruktur, maskinvare og sikkerhetssystemer. Dette må sikres gjennom krav i driftsavtaler samt revisjon og kontroll av disse.

IT-driftsleverandøren ivaretar en sentral beredskapsplan for å håndtere driftsavbrudd som vurderes å være av et slikt omfang at de skaper vesentlige forstyrrelser for større deler av kommunens virksomhet, og/eller som kan gi følgeskader for tredjepart.

Leverandør/partner

Informasjonssikkerhet reguleres i kontrakt og databehandleravtale mellom leverandører og kommunen. Det skal inngås databehandleravtale med leverandører/firmaer/partner som behandler personopplysninger. Kommunen skal alltid ha rett til innsyn og måling av hvorvidt sikkerhetskrav blir fulgt av leverandør eller eksterne ansatte.

Mal til databehandleravtale finnes i TQM. Alle databehandleravtaler arkiveres i kommunens sak-/arkivsystem.

Systemeier

Systemeier er eier av fagsystemene/IT-systemene som naturlig hører inn under området TO-leder/virksomhetsleder/enhetsleder er ansvarlig for. Systemeier er ansvarlig for å ivareta informasjonssikkerheten i fagsystemene/IT-systemene. Virksomhetsleder/enhetsleder oppnevner en person for daglig ivaretakelse av systemansvarlig rollen. Systemeier har også ansvar for å utarbeide risikoanalyse og registrere fagsystemene i Behandlingsprotokoll (artikkelprotokoll 30).

Systemansvarlig

Systemansvarlig er utpekt av Systemeier. De har hovedansvar for å gi opplæring til ansatte av fagsystemene/IT-systemene om forsvarlig forvaltning av informasjonen.

Daglig drift, herunder oppretting av roller og tilgangsstyring, samt videreutvikling og endring av system. Initiere og gjennomføre ROS-arbeid og utarbeide rutiner/retningslinjer for bruk av systemet i samarbeid med systemeier.

4.2 IT-system – anskaffelse, forvaltning og avhending

Informasjon i IT-løsninger går gjennom et livsløp, gjennom anskaffelse, drift, arkivering og avvikling.

Anskaffelse av nytt IT-system

I anskaffelsesprosessen skal det stilles krav om innebygd personvern og personvern som standardinnstilling. Dette betyr bl.a. at det skal være et system for retting og sletting. Det er viktig å sikre at personopplysninger ikke kommer på avveie, derfor må det stilles krav til løsninger hvor personvern har høy prioritet.
Det skal utnevnes en systemeier som er behandlingsansvarlig for systemet og har ansvaret for at oppgavene rundt forvaltningen og risikoanalyse. Systemeieren rådfører seg med personvernombud i alle spørsmål knyttet til personvern og behandling av personopplysninger.

Systemeier er ansvarlig for å gjennomføre ROS analyse der formålet med behandlingen av personopplysninger i systemet blir gjennomført og personopplysningene blir redegjort for. Det skal alltid vurderes om en DPIA skal utarbeides.

Forvaltning av IT-systemet

Det skal gjennomføres årlig informasjonssikkerhetsgjennomgang med oppdatering av risikovurderingen. Det er systemeier som er ansvarlig for gjennomføring av årlig informasjonssikkerhetsgjennomgang, og informasjonssikkerhetsanavarlig og/eller personvernrådgiver samt representant fra IT-drift skal delta.
Databehandleravtaler skal gjennomgås og fornyes ved behov.

Avhending og arkivering av IT-system

Når et IT-system ikke lenger skal brukes, skal data som ligger i systemet sikres med hensyn til konfidensialitet, integritet og tilgjengelighet. Informasjonen skal arkiveres iht. lovverket, og det skal være mulig å videreføre bruk i andre systemer.
Systemeier er ansvarlig for at informasjonen blir ivaretatt på en trygg måte når systemet ikke lenger er i bruk. Arkivtjenesten bistår sammen med systemeier for å sikre rett forvaring.

5 Internkontroll

Internkontroll for informasjonssikkerhet etableres via informasjonssikkerhetshåndboka og de underliggende prosedyrene for å sikre at kommunen er i stand til å følge kravene til informasjonssikkerhet og personvern. Internkontroll bygges på tre grunnleggende elementer:

Styrende

Informasjonssikkerhetshåndboka, så vel som enkelte prosedyrer definerer målsetning, organisering, ansvar og myndighet. Ledelsens gjennomgang for informasjonssikkerhet og personvern som gjennomføres årlig skal være styrende for videreutvikling av tiltak og mål innen området.

Gjennomførende

Informasjonssikkerhetshåndboka tar for seg forklaring av hvilket ansvar den enkelte leder og ansatte i kommunen har. Underliggende prosedyrer i kvalitetssystemet beskriver nærmere behandling av informasjon.

Kontrollerende

Kontrollerende prosedyrer har som formål å verifisere at krav til informasjonssikkerhet og personvern overholdes. Kommunens egenkontroll er sentral i dette arbeidet, samt hendelse og avviksbehandling og vurdering av tiltak. Informasjonssikkerhetshåndboka skal holdes oppdatert til enhver tid.

5.1 Risikohåndtering

Ledere skal foreta:

- Løpende risikovurderinger for informasjonssikkerhet og personvern i sin enhet
- Risikovurderinger og tiltak skal dokumenteres i TQM
- Årlig risikogjennomgang og DPIA, sett i sammenheng med årlig revisjon av prosedyrer i TQM ved hendelser eller endringer i systemer
- Systematisk følge opp måloppnåelse, etterlevelse, kompetanse og kultur

5.2 Avvikshåndtering

Formålet med avviksbehandlingen er å få kunnskap om hendelser slik at kommunen samlet kan begrense skadene, lære av hendelsene, endre rutiner og implementere gode løsninger for å hindre at liknende hendelser skjer igjen. Avvik skal meldes både ved brudd på informasjonssikkerheten og ved brudd på personopplysningsloven. Brudd på personopplysningsloven skal også meldes til datatilsynet.

Uønskede hendelser som skal meldes som avvik kan være enkeltepisoder, gjentakende episoder, overtredelser, svikt i rutiner, funksjonsfeil i fagsystemet eller mistanke om andre brudd på informasjonssikkerheten. Eventuelle informasjonssikkerhets brudd må vurderes med tanke på om det har eller kan forekomme personvernbrudd. Alle ansatte som oppdager avvik har selv ansvar for å melde dette i TQM.

Ved brudd på informasjonssikkerheten skal det gjøres en vurdering av tiltak og om aktuelle leverandører må kontaktes. Ved alvorlige brudd skal også vise det til egne varslingsrutiner i TQM.

5.3 Loggføring

For å sikre integritet og sporbarhet skal all aktivitet i fagsystemer som behandler personinformasjon loggføres, slik som endring og sletting av opplysninger, men også søk etter opplysninger. Gjennomsyn og kontroll av logger gjøres ved behov av systemeier og leder.

5.4 Oppdatering av systemoversikt

Alle systemenes behandling for informasjonssikkerhetsgjennomgang utgjør grunnlaget for systemoversikten i regneark/DigiOrden som til enhver tid skal være oppdatert.

Fagansvarlig for informasjonssikkerhet, gjerne i samråd med personvernombudet, koordinerer arbeidet med årlig gjennomgang av informasjonssikkerheten, og sikrer at informasjonssikkerhetsgjennomgang med risikovurdering blir dokumentert. Systemeiere har ansvaret for at nye opplysninger om sine system blir oppdatert.

5.5 Ledelsens gjennomgang av informasjonssikkerheten

Ledelsens gjennomgang skal holdes årlig for kommunedirektørens ledergruppe. I møte skal det oppsummeres status for informasjonssikkerhetsarbeidet i kommunen, samt avdekke om sikkerheten ivaretas iht. mål, strategier og prosedyrer og beslutte tiltak for det videre sikkerhetsarbeidet. Tiltak som skal sikre at sikkerhetsmål, strategi og organisering av informasjonssikkerhetssystemet er oppdaterte og i samsvar med kommunens behov.

I ledelsens gjennomgang skal bl.a. følgende punkter gjennomgås og vurderes:

- Resultater og hovedkonklusjoner fra informasjonssikkerhetsrevisjoner
- Registrerte avvik
- Rapporter fra offentlige og interne tilsyn
- Endringer i lover, forskrifter og offentlige sikkerhetskrav
- Endringer i de personopplysninger virksomheten skal behandle
- Endringer i trusselbildet som kommer fram i gjennomførte risikovurderinger
- Status på hendelser rundt teknisk informasjonssikkerhet
- Organisatoriske endringer
- Bygningsmessige endringer
- Planer og fremdrift for å ivareta intern kontroll og informasjonssikkerhet