Håndbok for

Informasjonssikkerhet i Eigersund kommune

Gjelder for: Alle ansatte

Vedtatt av: Rådmannen

Dato: 20.09.2018| **JpID:** 18/30458

Dokumentansvarlig (Enhet): Interne tjenester

Revisjonsintervall: Årlig

Distribusjon: Intranett, hjemmeside, QM+

Merknad:

Innhold

1. Informasjonssikkerhet og personvern

Informasjonssikkerhet handler om å håndtere risiko relatert til kommunens informasjonsverdier og behandling av personopplysninger. Vi skal sikre at informasjon ikke er tilgjengelig uten autorisasjon (konfidensialitet), at informasjon ikke uautorisert endres eller ødelegges (integritet) og at informasjon er til stede og anvendelig for medarbeidere slik at pålagte oppgaver kan utføres (tilgjengelighet).

Personvern handler om den registrerte sin rett til et privatliv og rett til å bestemme over egne personopplysninger.

EUs forordning for personvern, The General Data Protection Regulation (GDPR), blir norsk lov i 2018. Forordningen erstatter da gjeldende norsk personvernlovgivning som er bygget på EUs personverndirektiv fra 1995. Eigersund kommune arbeider kontinuerlig med å oppdatere styringsdokumenter, instrukser og rutiner for å kunne etterleve det nye regelverket.

I Eigersund kommune følger vi norm for informasjonssikkerhet i helse og omsorgstjenesten (Normen). Normen er juridisk bindende for Eigersund kommune gjennom signert avtale for tilknytning til Norsk Helsenett.

Normen stiller krav som detaljerer og supplerer gjeldende regelverk, først og fremst personvern- og helselovgivningens krav til å etablere tilfredsstillende informasjonssikkerhet for systemer som behandler helse- og personopplysninger.

Formål og omfang

Denne håndboka for informasjonssikkerhet er et verktøy for ledere og ansatte i Eigersund kommune for å ivareta tilfredsstillende informasjonssikkerhet og personvern.

Håndboken gjelder all informasjonsbehandling som skjer internt i Eigersund kommune og som kommunen har ansvaret for eksternt. Dette omfatter all behandling, lagring og kommunikasjon av informasjon både muntlig, på papir og digitalt. All bruk av IKT-løsninger er også inkludert.

Definisjoner

Definisjon av sentrale begreper som benyttes i dokumentasjon av kommunens informasjonssikkerhet og personvern er beskrevet i følgende dokument:
Definisjoner – Informasjonssikkerhet og personvern

Lovgrunnlag og kildehenvisninger

Sikkerhetshåndboka, samt gjeldende rutiner og instrukser, er en del av kommunens internkontroll for informasjonssikkerhet. Følgende regelverk og kilder ligger til grunn:

FL	Lov om behandlingsmåten i forvaltningssaker (forvaltningsloven)
eFF	Forskrift om elektronisk kommunikasjon med og i forvaltningen (eForvaltningsforskriften)
POL	Lov om behandling av personopplysninger (personopplysningsloven)
HOL	Lov om kommunale helse- og omsorgstjenester m.m. (helse- og omsorgstjenesteloven)
HPL	Lov om helsepersonell mv. (helsepersonelloven)
HRL	Lov om helseregistre og behandling av helseopplysninger (helseregisterloven)
PBL	Lov om pasient- og brukerrettigheter (pasient- og brukerrettighetsloven)

- Norm for informasjonssikkerhet i helse- og omsorgssektoren (Normen)
- Organisasjonskart – Eigersund kommune
- Personvernprinsippene (Datatilsynet)
- Rådmannens internkontroll (Orden i eget hus - KS)
- Veileder: Internkontroll og informasjonssikkerhet (Datatilsynet)
- Veileder: Internkontroll i praksis - informasjonssikkerhet (Difi)

2. Personvernprinsippene

Eigersund kommune behandler personopplysninger i samsvar med de grunnleggende personvernprinsippene, jf. personvernforordningens artikkel 5. Her følger en kort beskrivelse av prinsippene. For mer utfyllende informasjon se veileder fra Datatilsynet.

Lovlig, rettferdig og gjennomsiktig
Respekter de registrertes interesser og forventninger. Informer på en forståelig måte.

Formålsbegrensning
Opplysningene skal brukes til uttrykkelig angitte og legitime formål, og ikke (senere) til uforenelige formål.

Dataminimering
Personopplysningene skal være tilstrekkelige, relevante og begrenset til hva som er nødvendig.

Riktighet
Ukorrekte eller utdaterte personopplysninger skal rettes eller slettes.

Lagringsbegrensning
Det skal ikke være mulig å identifisere de registrerte lenger enn hva som er nødvendig for formålet.

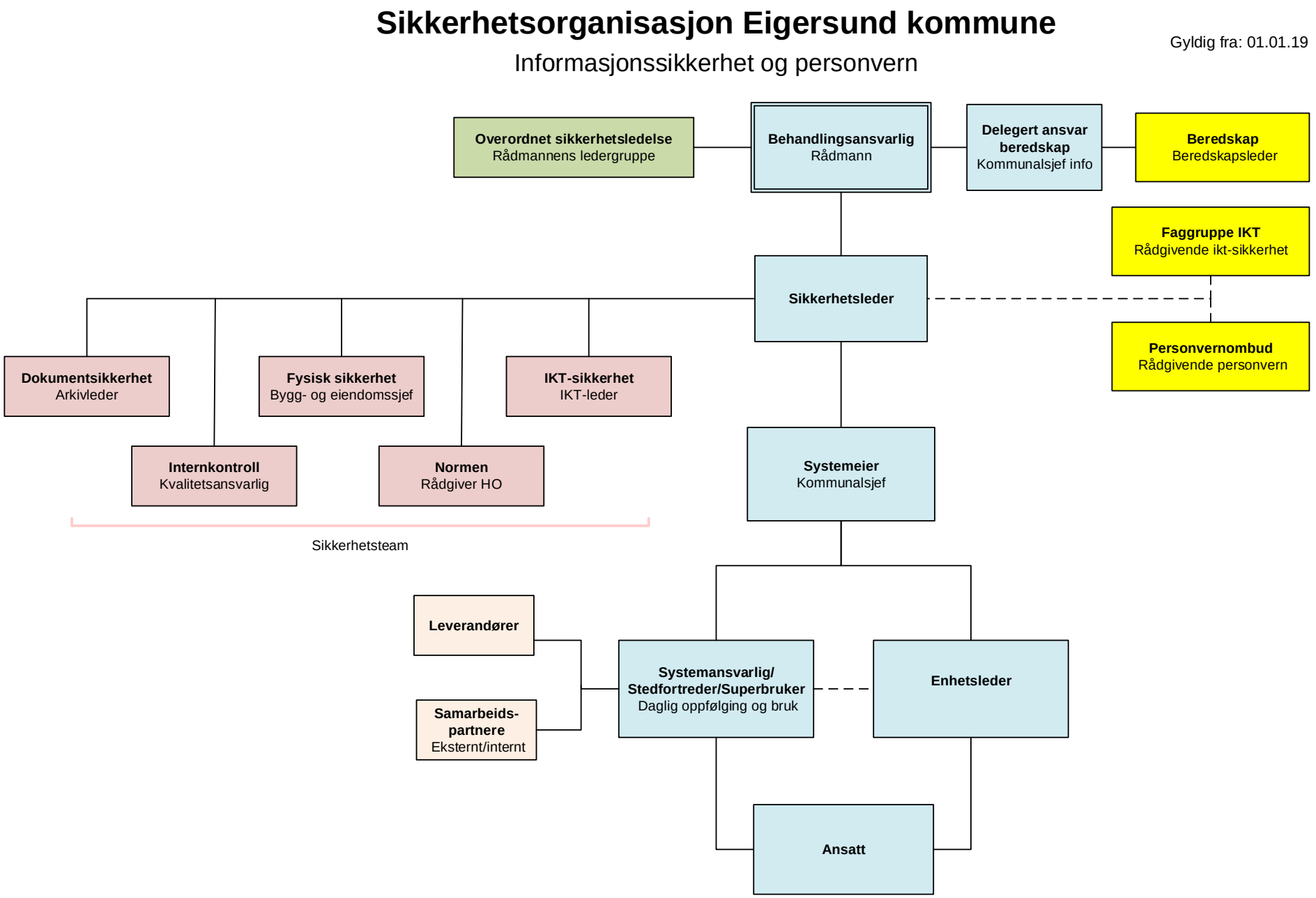
Integritet og fortrolighet
Personopplysninger sikres mot uautorisert tilgang og mot tap, ødeleggelse eller skade.

Ansvarlighet
Eigersund kommune har ansvar for, og må kunne dokumentere, etterlevelse.

3. Sikkerhetsorganisasjon og ansvarsfordeling

Som overordnet ansvarlig er rådmannen behandlingsansvarlig i Eigersund kommune. Følgende sikkerhetsorganisasjon er etablert for å ivareta rådmannens ansvar knyttet til informasjonssikkerhetsarbeid og personvern:

Figur 3.1 Sikkerhetsorganisasjon Eigersund kommune



For mer utfyllende informasjon om sikkerhetsorganisasjonen og ansvarsfordeling se: Sikkerhetsorganisasjonen.

Dokumentreferanse
Sikkerhetsorganisasjon kart - Informasjonssikkerhet og personvern
Gjeldende sikkerhetsteam (kommer)
Normen faktaark 01 - Ansvar og organisering

4. Sikkerhetsmål og sikkerhetsstrategi

Eigersund kommunes sikkerhetsmål og sikkerhetsstrategi gjelder all informasjonsbehandling som skjer internt i Eigersund kommune og som kommunen har ansvaret for eksternt. Dette omfatter all behandling, lagring og kommunikasjon av informasjon både muntlig, på papir og digitalt. All bruk av IKT-løsninger er også inkludert.

Formålet med informasjonsbehandling i Eigersund kommune er å understøtte våre oppgaver og tjenester slik at vi kan nå våre mål og realisere vår visjon. Kommunens mål og prioriteringer framkommer i vår overordnede strategi og virksomhetsplan. De er sammenfattet i vår visjon «sammen for alle».

En informasjonsbehandling som er målorientert, effektiv, lovlig og til å stole på er avgjørende for at kommunen skal lykkes. Tilstrekkelig og balansert informasjonssikkerhet er en kritisk faktor for å understøtte dette.

Mål for informasjonssikkerhet
Vår behandling av informasjon er i samsvar med lover, regler og avtaler, og bidrar på en formåls- og kostnadseffektiv måte til best mulig realisering av kommunens samlede mål.

Konfidensialitet
Bare personer med innsynsrett og ansatte med tjenstlig behov får kjennskap til taushetspliktig informasjon. Bare personer med innsynsrett og de ansatte som ledelsen har bestemt, får kjennskap til informasjon som kommunen har unntatt offentlighet av andre grunner enn taushetsplikt.

Integritet
Informasjon som kommunen har ansvaret for blir bare produsert og endret av ansatte eller eksterne som har fullmakt til dette. Informasjon blir ikke endret utilsiktet. Informasjonen skal være fullstendig, oppdatert og korrekt.

Tilgjengelighet
Relevant informasjon og hensiktsmessige IKT-løsninger er tilgjengelig på en effektiv måte for ansatte, innbyggere og næringslivet.

Strategi for informasjonssikkerhet
Det er etablert en sikkerhetsorganisasjon med klare ansvars- og myndighetsforhold.

Det skal gjennomføres tilfredsstillende internkontroll, herunder avvikshåndtering, sikkerhetsrevisjoner og ledelsens årlige gjennomgang.

Alle ansatte skal ha et bevisst forhold til og overholde kommunens instruks for informasjonssikkerhet.

De datatekniske løsninger som benyttes skal støtte opp om sikkerhetsmål og – strategier gjennom tilfredsstillende forvaltning av utstyr, system og data.

Konfidensialitet
Brannmurer, fysisk kontroll og opplæring sikrer tilgang bare for autoriserte brukere. Lagring av personopplysninger hvor konfidensialitet er nødvendig skal bare skje på kommunens egne datasystemer og lagringsmedier. Sensitive personopplysninger skal utelukkende behandles i sikre soner.

Integritet
Autorisert personell får kun tilgang til datasystemet gjennom innlogging med personlig passord eller kode og aktiviteten kan spores. Kommunen har etablert antivirusløsning slik at ødeleggende programvare ikke skal kunne endre lagrede personopplysninger.

Tilgjengelighet
Sentral backupløsning sikrer at informasjon som er lagret på kommunens servere kan gjenopprettes. Alternative manuelle prosedyrer sikrer tilgjengelighet for informasjon som er viktig for liv og helse når IKT-løsningene er utilgjengelige.

Ansvar
Rådmann har ansvar for at det etableres sikkerhetsmål og sikkerhetsstrategi for kommunens behandlinger av personopplysninger, og for at disse dokumenteres og gjøres kjent i kommunen.

Dokumentreferanse
Normen (gjeldende utgave) - kap. 4.2 og 4.3

5. Oversikt over behandling av opplysninger

Eigersund kommune skal til enhver tid ha en oppdatert oversikt over hvilke behandlinger av personopplysninger som foretas, og hvilke opplysninger som inngår i disse.

Oversikten er nødvendig for at vi skal kunne ivareta våre plikter. Oversikten danner også grunnlag for utarbeidelse av sikkerhetsmål og sikkerhetsstrategi, og vil være underlag ved risikovurderinger og klassifisering av IKT-løsninger.

Oversikten, som skal føres i kommunens digitale register (Draftit Privacy Records), omfatter *blant annet* følgende:

- Hvilke opplysninger som lagres og formålet med behandlingen
- Hjemmelsgrunnlag for behandlingen
- Omfanget av behandlingen
- Hvor og hvor lenge opplysningene lagres
- Bruk av databehandlere

Ansvar
Rådmann har ansvar for å det dokumenteres hvilke personopplysninger som behandles i kommunen.

Kommunalsjef har ansvar for å påse at avdelingen utarbeider og vedlikeholder oversikt.

Ansatte skal delta i utarbeiding og vedlikehold av oversikt.

Sikkerhetsleder skal påse at oversikt vedlikeholdes.

Personvernombud skal bidra til å få oversikt over behandlingene.

Dokumentreferanse
Rutine – Bruk av Draftit Privacy Records (kommer)
Oversikt behandlinger på kommunens nettsider (kommer)
Personvernerklæring
Normen faktaark 13 - Oversikt over behandlinger av helse - og personopplysninger i virksomheten

6. Risikovurderinger

Risikovurdering skal gjennomføres før eller ved iverksettelse av ny behandling av personopplysninger eller ved endringer i behandlingen som har betydning for informasjonssikkerheten. Slike endringer kan være endring i type opplysninger som behandles, organisasjonsendringer eller tekniske og bygningsmessige endringer. Grundighet og omfang av risikovurderingen bestemmes ut fra den enkelte situasjon som skal vurderes.

En risikovurdering består av fem hoveddeler:

- Kartlegge risiko: *Oversikt identifiserte trusler, hva kan gå galt?*
- Vurdere risiko: *Sannsynlighet og konsekvens, hvor galt kan det gå?*
- Dokumentere tiltak: *Hva er gjort for å unngå at det går galt?*
- Vurdere tiltak: *Er det nok til å redusere risiko til et akseptabelt nivå?*
- Følge opp tiltak: *Skal vi endre eller etablere kontrolltiltak?*

Nivå for akseptabel risiko skal fastsettes før behandling av personopplysninger startes og før risikovurderinger gjennomføres. Det arbeides med å fastsette overordnet nivå for akseptabel risiko i Eigersund kommune.

Som hovedregel skal alle gjennomførte risikovurderinger dokumenteres i kommunens kvalitetssystem (QM+). Unntak gjelder dersom gradert informasjon inngår i risikovurderingen. Alle risikovurderinger skal arkiveres i kommunens sak-/arkivsystem.

En risikovurdering av informasjonssikkerhet vurderer sannsynligheten for brudd på sikring av konfidensialitet, integritet og tilgjengelighet. Dersom det er sannsynlig at behandlingen vil medføre høy risiko for en persons rettigheter og friheter, skal det gjennomføres en vurdering av konsekvenser for personvernet (Data Protection Impact Assessment – DPIA) jf. GDPR artikkel 35. Eksempler hvor vi må gjennomføre DPIA kan være ved:

- systematisk og omfattende vurdering av personlige forhold når opplysningene brukes til automatiserte avgjørelser
- behandling av sensitive personopplysninger i stort omfang
- systematisk overvåking av offentlig område i stort omfang

Ved høy risiko for personvernet, som ikke kan begrenses, skal personvernombudet involvere Datatilsynet i forhåndsdrøftelser.

Ansvar
Rådmann fastsetter nivå for akseptabel risiko.

Kommunalsjef er ansvarlig for at det gjennomføres risikovurderinger i sin avdeling i henhold til gjeldende rutiner.

Dokumentreferanse
Gjeldende overordnet nivå for akseptabel risiko (kommer)
Rutine for gjennomføring av risikovurdering (kommer)
Normen faktaark 05 - Fastsette nivå for akseptabel risiko

7. Sikkerhetsrevisjon

Det skal jevnlig, minimum årlig og ved større systemendringer, utføres sikkerhetsrevisjon for bruk av informasjonssystem i kommunen, jf. ledelsens gjennomgang av sikkerhet kapittel 8.

I tillegg skal sikkerhetsleder og personvernombud periodisk utføre sikkerhetskontroll. Ved gjennomføring av kontrollen skal blant annet følgende elementer gjennomgås:

- Enhetens oversikt over behandling av personopplysninger
- Opplæring av ansatte
- Gjennomgang av avvik registrert siden forrige kontroll
- Autorisasjon og tilgangskontroll

Samlet danner resultatet av sikkerhetsrevisjoner og sikkerhetskontroller grunnlag for eventuelle endringer i sikkerhetsmål, -strategi og organisering. Avvik som eventuelt avdekkes, behandles i henhold til rutiner for avvikshåndtering (QM+).

Ansvar
Personvernombud og sikkerhetsleder skal utføre sikkerhetskontroller og påse at det gjennomføres sikkerhetsrevisjoner.

Dokumentreferanse
Mal sikkerhetsrevisjon (kommer)
Normen faktaark 06 - Sikkerhetsrevisjon

8. Ledelsens gjennomgang

Overordnet ledelse skal årlig foreta en gjennomgang av kommunens internkontroll og kvalitetssystem, herunder informasjonssikkerhet og personvern. Ledelsens gjennomgang skal som et minimum sikre at vi har gode overordnede styrende dokumenter i samsvar med gjeldende lovverk, og at disse etterleves i praksis.

Aktuelle deltakere ved gjennomgangen av informasjonssikkerhet og personvern er sikkerhetsleder, personvernombud, systemeiere, medlemmer i sikkerhetsteamet og beredskapsleder. Deltakerne presenterer status, avvikshåndtering og tiltak innen sitt ansvarsområde.

Møtet skal ende opp med en handlingsplan som inkluderer aktuelle sikkerhetstiltak som skal iverksettes, hvilken risiko som aksepteres, samt eventuelle behov for forbedring av styrende dokumenter.

Prosessflyt ledelsens gjennomgang av informasjonssikkerhet og personvern vises i figur 8.1 på neste side.

Grunnlag for gjennomgangen:

- Registrerte avvik / resultat fra avviksbehandling
- Rapporter fra offentlige tilsyn
- Resultater fra sikkerhetsrevisjon, jf. kapittel 7
- Endringer i lover og forskrifter
- Endringer i trusselbildet som kommer fram i gjennomførte risikovurderinger
- Organisatoriske endringer
- Bygningsmessige endringer

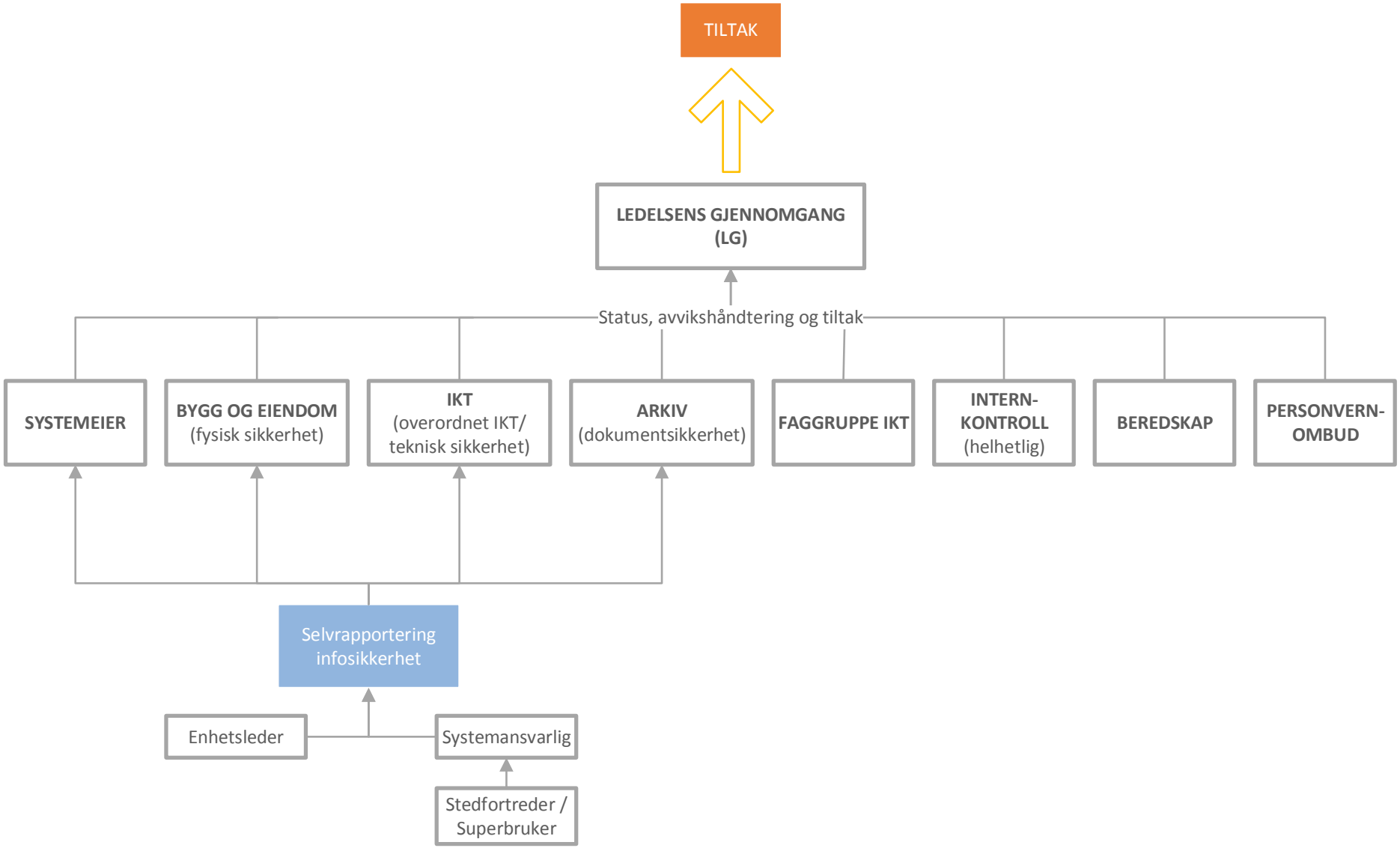
Ansvar
Rådmann er ansvarlig for årlig gjennomføring av ledelsens gjennomgang.

Sikkerhetsleder skal forberede ledelsens gjennomgang av informasjonssikkerhet og personvern og følge opp gjennomføring av handlingsplan.

Kommunalsjef og enhetsleder skal gjøre resultatet av ledelsens gjennomgang kjent for de ansatte.

Dokumentreferanse
Ledelsens gjennomgang av informasjonssikkerhet og personvern (sjekkliste kommer)
Prosessflyt - Ledelsens gjennomgang av informasjonssikkerhet og personvern

Figur 8.1 Ledelsens gjennomgang av informasjonssikkerhet og personvern



9. Konfigurasjon

Med *konfigurasjon* menes informasjonssystemets utforming, det vil utstyr og program, samt sammenkoblinger mellom disse.

Kommunen skal til enhver tid ha oversikt og kontroll over IKT-utstyr og programvare som benyttes i virksomheten. Kommunens informasjonssystem skal konfigureres slik at tilfredsstillende informasjonssikkerhet oppnås i henhold til kommunens sikkerhetsstrategi, risikovurderinger og beslutninger om sikkerhetstiltak.

Konfigurasjonskontroll omfatter all programvare, servere, nettverksutstyr, interne og eksterne kommunikasjonsforbindelser m.m. som eies / disponeres av kommunen.

Følgende gjelder:

- Kommunens informasjonssystem er inndelt i soner som gjenspeiler skillet mellom behandling av sensitive (sikker sone) og "ikke-sensitive personopplysninger" (intern sone).

- Denne soneinndelte konfigurasjonen sikrer også at ansatte (brukere) skilles med tanke på nettverkstilgang for kun å nå opplysninger som de er autorisert for.

- De deler av informasjonssystemet hvor sensitive personopplysninger behandles, er videre inndelt i samsvar med formålet med behandlingen av personopplysninger / tjenester kommunen leverer.

- Sikker sone er adskilt fra eksterne nett med to sikkerhetsbarrierer. All aktivitet skal initieres fra sikker sone til intern sone (og til eksterne nett)

- Eigersund kommune drifter noen fagsystemer for andre kommuner. Tilgang til disse fagsystemene er adskilt fra kommunens øvrige nett ved bruk av egne nettverkssoner.

- På hjemmekontor benyttes kun kommunens hjemmekontorløsning. Hjemmekontorløsningen skal sikre at uautoriserte personer ikke får tilgang til kommunens informasjonssystem.

- Kommunens informasjonssystem skal være konfigurert i samsvar med konfigurasjonskart. Kun utstyr eller program eiet / disponert av kommunen skal inngå i informasjonssystemet.

- Endringer i informasjonssystemets konfigurasjon skal utføres planmessig og systematisk og sikre at
    - *Alle konfigurasjonsendringer er i samsvar med besluttet sikkerhetsstrategi*
    - *Informasjonssystemet fungerer som forutsatt også etter at endringen er gjennomført.*

- Kommunens informasjonssystem er beskrevet i dokumentet "Beskrivelse av Eigersund kommunes informasjonssystem". IKT-kontoret skal kunne fremlegge denne tekniske dokumentasjonen ved tilsyn, intern kvalitetsrevisjon og kontroll.

Ansvar

IKT-leder har ansvar for utforming og vedlikehold av konfigurasjonene og tilhørende dokumentasjon knyttet til informasjonssystemenes infrastruktur og driftstekniske forhold.

Systemeiere / Systemansvarlige / Superbrukere har ansvar for vedlikehold av konfigurasjonene og tilhørende dokumentasjon knyttet til fagsystemene.

IKT-leder / Systemeier er ansvarlig for at det foreligger nødvendige avtaler (SLA, databehandleravtaler) ved outsourcing av hele eller deler av kommunens IKT-driftstjenester eller når kommunen selv er databehandler for andre.

Dokumentreferanse
Instruks - Bruk av kommunens IKT-løsninger
Instruks - Informasjonssikkerhet for ansatte
Normen Faktaark 20a-c - Sikkerhets- og samhandlingsarkitektur

10. Avvik og avvikshåndtering

Avvik innen informasjonssikkerhet og personvern er brudd på etablert regelverk og prosedyrer som skal sikre konfidensialitet, integritet og tilgjengelighet.

Systematisk håndtering av avvik skal bidra til at brudd på lover, forskrifter, instrukser og rutiner rapporteres til ansvarlig person og sikre mulighet for læring og forbedring. Dersom det ikke er samsvar mellom fastlagte instrukser eller rutiner og hvordan informasjonssystemet faktisk benyttes, skal resultatet fra avvikshåndteringen benyttes som grunnlag ved eventuelle endringer.

Den enkelte medarbeider har ansvar for å rapportere avvik. Kommunens elektroniske kvalitetssystem (QM+) og gjeldende avviksrutiner skal benyttes.

Eksempler på situasjoner som gjør det nødvendig å iverksette rapportering og avvikshåndtering:

- Utilsiktet utlevering av personopplysninger, eller ved mistanke om slik utlevering.
- Medarbeidere som benytter informasjonssystem uten autorisasjon.
- Feil i utstyr eller program som kan ha innvirkning på informasjonssikkerheten eller driften av informasjonssystemet
- Brudd på taushetsplikten

Ved avvik som trolig vil medføre en risiko for personers rettigheter og friheter skal Datatilsynet varsles, jf. GDPR Artikkel 33. Dette skal skje uten ugrunnet opphold og senest 72 timer etter at avviket ble avdekket. Ved høy risiko skal den behandlingsansvarlige uten ugrunnet opphold underrette den registrerte om bruddet, jf. GDPR Artikkel 34.

Ansvar
Ansatte er ansvarlig for å rapportere avvik.

Enhetsleder er ansvarlig for å følge opp rapporterte avvik.

Sikkerhetsleder er ansvarlig for å påse at varslingsrutine følges.

Dokumentreferanse
Rutine for å melde avvik (kommer)
Rutine for varsling til Datatilsynet og de registrerte (kommer)

11. Partnere og leverandører

Når eksterne partnere / leverandører behandler personopplysninger på vegne av Eigersund kommune skal det alltid foreligge en skriftlig avtale som regulerer denne behandlingen, såkalt databehandleravtale.

- Databehandleravtalen skal være signert av begge parter før behandlingen iverksettes.
- Databehandleravtalen skal være i tråd med de til enhver tid gjeldende lovkrav, og signeres av systemeier. Alle databehandleravtaler arkiveres i kommunens sak-/arkivsystem.
- Kommunen skal ha oversikt over personell hos partnere eller leverandør som gis adgang til kommunens datautstyr eller programmer hvor personopplysninger behandles.
- Ansatte hos partnere eller leverandører som gis adgang til kommunens datautstyr eller programmer skal underskrive taushetserklæring før adgang gis.
- Det er i utgangspunktet ikke tillatt å gi ansatte hos partnere og leverandører tilgang til kommunens IKT-løsninger med fjernstyringsverktøy, som for eks. Teamviewer, med mindre dette er godkjent av IKT-kontoret.
- Alle som kobler seg opp til kommunens informasjonssystem ved bruk av slike fjernstyringsverktøy, skal informere om formål med oppkoblingen før denne tillates. De skal også gi tilbakemelding de ikke lenger har behov for tilkoblingen, og hva de har gjort mens de var koblet opp.
- Denne type fjerntilgang tillates kun så lenge det er nødvendig for den aktuelle oppgaven, og skal stenges umiddelbart når behovet opphører. Den som aktiverer fjerntilkoblingen plikter å loggføre hendelsen.
- For hjemmekontortilgang gjelder egen rutine, se lenke under.

Ansvar

Ansatte som aktiverer fjerntilkobling plikter å loggføre hendelsen.

Enhetsleder skal påse at eksternt personell signerer taushetserklæring ved behov.

Systemeier er ansvarlig for at det foreligger en signert databehandleravtale ved behov.

Dokumentreferanse

Mal - databehandleravtale
Rutine for hjemmekontortilgang (kommer)
Taushetserklæring (kommer)
Leverandøroversikt (kommer)
Normen faktaark 10 - Bruk av databehandler

12. Kompetanse

God sikkerhet forutsetter god opplæring og tilstrekkelig kompetanse hos de ansatte. Det er viktig å gjøre informasjonssikkerhet og personvern til en del av de ansattes daglige oppgaver – som en integrert del av kommunens internkontroll.

- Alle ansatte skal gis nødvendig opplæring i informasjonssikkerhet og personvern. Dette skal som minimum omfatte:
    - Instruks - Bruk av kommunens IKT-løsninger
    - Instruks - Informasjonssikkerhet for ansatte
    - Overordnede rutiner og instrukser.
    - Enhetsspesifikke rutiner og instrukser.
    - Håndbok for informasjonssikkerhet

- Enhetsleder er ansvarlig for at slik opplæring blir gitt til ansatte i sin enhet.

- Krav til opplæring i informasjonssikkerhet og personvern samt tilhørende rutiner er samlet i en egen opplæringsplan (se lenke under). I tillegg til de ansatte omfatter planen også aktuelle opplæringstiltak for systemansvarlige, superbruker o.a. med spesielle roller i forhold til bruk og administrasjon av kommunens informasjonssystem.

- Dokumentasjon av de til enhver tid gjeldende rutiner og instrukser skal være tilgjengelig for alle ansatte på kommunens intranett og i kommunens avvikshåndteringssystem.

Det tilbys ulike former for opplæring innen informasjonssikkerhet og personvern, alt etter behov. Du finner mer informasjon om dette på kommunens intranett.

Ansvar
Rådmann fastsetter minimumskrav til ansattes kompetanse innen informasjonssikkerhet og personvern.

Enhetsleder er ansvarlig for at nødvendig opplæring blir gitt til ansatte i sin enhet.

Ansatte har selv ansvar for å følge opp og praktisere vedtatte regler og sikringstiltak. Dette innebærer årvåkenhet i det daglige arbeidet. Alle avvik som oppdages skal meldes nærmeste overordnede ved bruk av kommunens avvikshåndteringssystem.

Dokumentreferanse
Kurs og e-læring på intranett – informasjonssikkerhet og personvern
Opplæringsplan – informasjonssikkerhet og personvern (kommer)
Taushetserklæring (kommer)

13. Autorisasjon

Med autorisasjon menes at en person, i et ansettelsesforhold, i en bestemt rolle, gis en bestemt rettighet til: Lesing av tekst og bilder, registrering, redigering, retting, sletting og/eller sperring av opplysninger.

Autorisasjon er personlig og skal registreres i et autorisasjonsregister.

Noen ansatte vil kunne ha utvidede systemrettigheter og/eller arkivtilgang, som superbrukere, systemansvarlige, arkivpersonell og ikt-personell. For disse påhviler det et særskilt ansvar i utøvelsen av sine rettigheter.

Det skal bare gis adgang til områder og utstyr, manuelle eller digitale informasjonssystemer, i den grad det er nødvendig for å utføre pålagte oppgaver. Alle typer autorisasjon som gis skal være i henhold til kommunens gjeldende sikkerhetsstrategi.

- Enhetsleder er autorisasjonsansvarlig for manuelle og elektroniske behandlinger av personopplysninger i sin enhet, og skal:
    - *Besørge at alle nye ansatte, vikarer og periodisk personell får tilgang til aktuelle informasjonssystemer ved tilsetting i henhold til tjenstlige behov.*
    - *Skriftlig informere aktuelle instanser (IKT Brukerhjelpen, systemansvarlige o.l.) om endringer i behov for tilgang til informasjonssystemene.*
    - *Trekke tilbake autorisasjoner når ansatte slutter eller ikke lenger har tjenstlig behov for autorisasjonen. Ved endringer i arbeidsforhold eller ansvar skal den ansattes tilganger i kommunens informasjonssystemer vurderes.*
    - *Føre et autorisasjonsregister med oversikt over hvilke IKT-løsninger / manuelle behandlinger hver enkelt ansatt er autorisert for. Dette autorisasjonsregisteret skal oppdateres hver gang det skjer endringer og skal oppbevares i minst 5 år.*
    - *Årlig gjennomgå brukertilganger i egen enhet og gi melding til IKT Brukerhjelpen og andre dersom tilganger skal slettes eller endres.*

- Personer med periodisk arbeid for kommunens, f.eks. konsulenter, håndverkere, studenter og praktikanter, skal underskrive taushetserklæring, og være underlagt klare regler å forholde seg til når det gjelder:
    - *Hva de kan gjøre og ikke kan gjøre,*
    - *Hvor de kan oppholde seg,*
    - *Hvilke informasjoner de kan få tilgang til,*
    - *Hvilke konsekvenser eventuelle sikkerhetsbrudd kan få.*

- Ved sikkerhetsbrudd skal tilgangsstyringen for det aktuelle informasjonsområdet kontrolleres. Alle avvik registreres og behandles i henhold til gjeldende rutiner i kommunens kvalitetssystem (QM+).

Ansvar

Enhetsleder er autorisasjonsansvarlig for elektroniske og manuelle behandlinger av personopplysninger i sin enhet, og er ansvarlig for at taushetserklæring undertegnes.

Ansatte har selv et ansvar for sikkerheten på eget kontor / arbeidsplass, herunder å bidra til at uvedkommende ikke får tilgang til lagrede elektroniske opplysninger eller informasjon i papirform på arbeidsplassen.

IKT-kontoret / systemansvarlige / superbrukere har ansvar for tildeling, endring og tilbaketrekking av autorisasjon til kommunens IKT-løsninger i henhold til melding fra autorisasjonsansvarlig (enhetsleder).

Dokumentreferanse
Normen faktaark 14 – Tilgangsstyring
Taushetserklæring (Se QM+)
Sjekkliste – introduksjon av nyansatte (Se QM+)
Sjekkliste – avslutning av arbeidsforhold (Se QM+)

14. Fysisk sikkerhet

Tilfredsstillende fysisk sikkerhet er viktig for å hindre at uvedkommende får tilgang til opplysninger. Det er et samspill mellom tiltak for fysisk sikring og tiltak for elektronisk sikring. Tiltakene er gjensidig avhengig av hverandre for at tilfredsstillende sikkerhet skal oppnås.

Trusler som kan utløses ved for dårlig fysisk sikring kan bl.a. være:

- *At uvedkommende får tilgang til utstyr hvor kommunens informasjon behandles.*
- *Tyveri av datautstyr eller sikkerhetskopier.*
- *Sabotasje og hærverk mot vitale deler av informasjonssystemet.*

Risikovurderinger
Det skal gjennomføres risikovurderinger for alle fysiske arealer som skal sikres mot uautorisert adgang. Dette gjelder både på overordnet nivå og internt i hver enhet.

Adgangskontroll
Adgang til kommunens lokaler skal kontrolleres.

Bygg og eiendomssjef har ansvar for «skallsikring» av kommunens lokaler, samt administrasjon av adgangskontroll.

Enhetsleder skal sørge for at lokaler og utstyr i sin enhet er forsvarlig sikret. Det skal legges spesiell vekt på å sikre områder / rom hvor det det behandles gradert informasjon. Det tilstrebes at alle slike områder kontrolleres av digitalt adgangskontrollsystem.

Enhetsleder skal, på samme måte som ved autorisasjon til IKT-løsninger, føre oversikt over hvem som har tjenstlig behov for adgang til ulike områder og rom. Enhetsleder er ansvarlig for å melde fra skriftlig til bygg og eiendomsseksjonen om behov for og endringer i tilgang.

Adgang til dedikerte rom med driftsutstyr (f.eks. serverrom) skal kun gis til personell med absolutte behov for tilgang. Generelt skal adgang i størst mulig grad begrenses.

Bygg og eiendomsseksjonens rutine for tildeling av nøkler / adgangskort gjelder.

Det er i dag varierende grad av besøkskontroll i de ulike enhetene. Det skal tilstrebes at besøkende i størst mulig grad alltid følges av ansatt ved opphold i kommunens lokaler.

Fysisk sikring av utstyr i andre lokaler
Utstyr som benyttes utenfor kommunens lokaler, f.eks. hjemmekontor, skal sikres fysisk ved bruk av normal bygningsmessig sikkerhet. Vinduer skal være låst / lukket når lokalet ikke er i bruk.

Ansvar
Enhetsleder skal sørge for at lokale og utstyr i sin enhet er forsvarlig fysisk sikret.

Ansatte har selv et ansvar for fysisk sikkerhet på eget kontor / arbeidsplass.

Bygg og eiendomssjef har ansvar for «skallsikring» av kommunens lokaler, samt administrasjon av adgangskontroll.

Dokumentreferanse
Rutine for tildeling av nøkler og adgangskort (kommer)
Normen faktaark 17 – Fysisk sikring av områder og utstyr
Normen faktaark 29 - Hjemmekontor

15. Dokumentsikkerhet

Dokumentsikkerhet omfatter sikker håndtering og oppbevaring av dokumenter i alle former. Det vil si alt fra tradisjonell papirformat til all informasjon som kan leses, lyttes til, fremføres eller overføres, ved hjelp av maskinelt utstyr.

Sentrale momenter innenfor dokumentsikkerhet:

- Merking
- Journalføring
- Forsendelse, intern ombringelse og medbringelse på reise
- Utlån, mangfoldiggjøring og annen spredning
- Tilintetgjøring, evakuering og rekonstruksjon
- Kontroll og rapportering

Ansvar
Ansatte har selv et ansvar for å ivareta tilfredsstillende dokumentsikkerhet.
Arkivleder har ansvar for å utarbeide og vedlikeholde overordnede rutiner og instrukser for dokumentsikkerhet.

Dokumentreferanse
Arkivplan Eigersund kommune
NSM - Dokumentsikkerhet
Instruks - Bruk av kommunens IKT-løsninger
Instruks - Informasjonssikkerhet for ansatte

16. Internkontroll

Internkontroll for informasjonssikkerhet i Eigersund kommune skal bidra til

- helhetlig styring og riktig utvikling
- kvalitet og effektivitet i tjenestene
- godt omdømme og legitimitet
- etterlevelse av politiske vedtak, lover og forskrifter, instrukser og rutiner

Tabellen som følger er en kartlegging av internkontroll for informasjonssikkerhet i Eigersund kommune. Punktene er hentet fra Datatilsynets sjekkliste for kommunens internkontroll datert 2012.

Regelverket inneholder en rekke krav og påbud. I sjekklisten er regelkravene omsatt til påstander som kommunen svarer "ja" eller "nei" på. I første kolonne i tabellen blir dette visuelt fremvist som grønt (ja) og rødt (nei).

Ideelt sett skal vi kunne svare ja på alle spørsmål i sjekklista. Det betyr at kommunen etterlever personopplysningsloven på en god måte. For alle spørsmål der svaret er nei, må det sørges for å innføre tiltak, sikre dokumentasjon, eller bygge opp systemer for å sikre at vi etterlever loven.

Sjekklisten er delt inn i fire hoveddeler:

- Styrende del – Overordnet fokus, hovedsakelig rettet mot ledelsen.
- Gjennomførende del – Praktisk fokus, rutiner som sikrer at ansatte følger regelverket.
- Kontrollerende del – Kontrollrutiner som sikrer at kommunen etterlever regelverket.
- Andre forhold – Andre viktige elementer som taushetsplikt og forhold til andre virksomheter.

Aktører beskrevet i tabellen er ansvarlig (A), kontrollør (K) og utfører (U). Referansen gir en henvisning til gjeldende dokumentasjon, instruks eller rutine.

Styrende del

	SJEKKLISTE	REFERANSE
	BEHANDLINGSANSVAR	
1	Vi har en dokumentert oversikt over hvem som er ansvarlig for behandling av personopplysninger.	Håndbok kapittel 3 (Sikkerhetsorg.) Håndbok kapittel 4 (Mål og strategi)
	KARTLEGGING AV PERSONOPPLYSNINGER SOM BEHANDLES	
2	Vi har en skriftlig oversikt over hvilke personopplysninger som behandles.	Håndbok kapittel 5 (Oversikt behandling av personoppl.)
3	Vi har avklart det rettslige grunnlaget for hver behandling (hjemmelsgrunnlag).	
4	Vi har dokumentert hvilket formål de ulike opplysningene er samlet inn for.	
5	Vi har vurdert at formål er i samsvar med hjemmelsgrunnlag.	

6	Vi har oversikt over hvilke krav i personopplysningsloven og tilhørende forskrift som gjelder for oss.	
	RAMMER FOR INFORMASJONSSIKKERHET	
7	Vi har fastsatt sikkerhetsmål.	Håndbok kapittel 4 (Mål og strategi)
8	Våre valg og prioriteringer i sikkerhetsarbeidet er beskrevet i en sikkerhetsstrategi.	
9	Sikkerhetsmål og sikkerhetsstrategi blir gjennomgått årlig for å klarlegge at strategiene dekker våre behov.	
10	Vi har fastsatt kommunens akseptkriterier (akseptabel risiko basert på sikkerhetsmål/-strategi).	Håndbok kapittel 6 (Risikovurderinger)
11	Vi har gjennomført en risikovurdering som dokumenterer at risikoen for sikkerhetsbrudd ligger innenfor kommunens fastsatte akseptkriterier.	
12	Vi har etablert og dokumentert en sikkerhetsorganisasjon hvor roller og ansvar for informasjonssikkerhet er klart definert.	Håndbok kapittel 3 (Sikkerhetsorg.)
13	Vi har en skriftlig, samlet oversikt over informasjonssystemets utforming.	Håndbok kapittel 9 (Konfigurasjon)

Gjennomførende del

	SJEKKLISTE	**AKTØR**	**REFERANSE**
	RUTINER FOR BEHANDLING AV PERSONOPPLYSNINGER		
14	Vi har rutiner som sikrer at innbyggere og andre registrerte får informasjon om sine rettigheter til a. innsyn i informasjon b. retting av feil informasjon c. supplering av personlig informasjon ved behandling av personopplysninger der behandlingsgrunnlaget er fastsatt i lov eller forskrift.	Kvalitetssystem QM+: Informasjonssikkerhet og personvern - Rutiner	
15	Vi har rutiner som sikrer at det innhentes samtykke eller inngås avtale når det vil utgjøre behandlingsgrunnlaget.		
16	Vi har etablert rutiner for sletting av personopplysninger.		
17	Vi har rutiner for iverksettelse eller opphør av behandling av personopplysninger.		

18	Vi har rutiner for innføring og bruk av automatiserte avgjørelser.	
	DAGLIG INFORMASJONSSIKKERHET	
19	Vi har klare regler for de ansattes bruk av informasjonssystemene.	Kvalitetsystem QM+: Infosikkerhet/ Instrukser • Infosikkerhet for ansatte
20	Vi har sørget for å gjøre de ansatte oppmerksom på reglene.	
21	Vi har god oversikt over brukerne av informasjonssystemet. Det er fastsatt gode rutiner for tildeling av rettigheter i systemet og for å oppheve slike når det er relevant.	Håndbok kapittel 13 (Autorisasjon)
22	Våre informasjonssikkerhetssystem har logger som benyttes til å føre kontroll med eventuell misbruk av systemet.	
23	Våre sikkerhetstiltak er begrenset til tiltak som medarbeidere ikke kan påvirke eller lett omgå.	Håndbok kapittel 9 (Konfigurasjon)
24	Vi har et velfungerende system for sikkerhetskopiering.	Håndbok kapittel 15 (Dokumentsikkerhet)
25	Våre sikkerhetskopier blir testet jevnlig for sikre at disse fungerer dersom originaldata skulle bli kompromittert.	
26	De ansatte er kjent med og har undertegnet avtale om at kommunens internkontroll legges til grunn for eget arbeid. Det vil si at de må forholde seg til internkontrollen i sitt daglige virke.	Håndbok kapittel 12 (Kompetanse)
	RUTINER FOR DAGLIG INFORMASJONSSIKKERHET	
27	Vi har rutine for bruk av internett.	Kvalitetsystem QM+: Infosikkerhet/ Instrukser • Infosikkerhet for ansatte • Bruk av kommunens IKT-løsninger
28	Vi har rutine for bruk av e-post.	
29	Vi har rutine for utskrift.	
30	Vi har rutine for makulering av dokumenter	
31	Vi har rutine for sikkerhet og orden på eget kontor.	
32	Vi har rutine for innleid personell og håndverkere.	
33	Vi har rutine for bruk av hjemmekontor.	
34	Vi har rutine for bruk av mobilt utstyr.	
35	Vi har rutine for adgangskontroll.	Håndbok kapittel 14 (Fysisk sikkerhet)

	SIKRING AV KONFIDENSIALITET, TILGJENGELIGHET OG INTEGRITET	
36	Vi har etablert tiltak for å sikre tilstrekkelig konfidensialitet for opplysningene som behandles i egne systemer.	Håndbok: • kapittel 9 (Konfigurasjon) • kapittel 11 (Partnere og leverandører) • kapittel 12 (Kompetanse) • kapittel 13 (Autorisasjon) • kapittel 14 (Fysisk sikkerhet) • kapittel 15 (Dokumentsikkerhet)
37	Vi har etablert tiltak for å sikre at ansatte har tilgang til alle relevante personopplysninger som er nødvendig for vedkommende sitt arbeid.	
38	Vi har sikret oss at endring av personopplysninger i systemene kun kan gjøres av autorisert personell.	
39	Vi har etablert tiltak mot ødeleggende programvare.	
	SIKKERHETSHENDELSER	
40	Vi har sikkerhetstiltak som hindrer uautorisert bruk av informasjonssystemet.	Håndbok kapittel 9 (Konfigurasjon)
41	Vi har et system som gjør at forsøk på uautorisert bruk av informasjonssystemet blir registrert slik at det kan følges opp videre.	

Kontrollerende del

	SJEKKLISTE	AKTØR	REFERANSE
	STIKKONTROLL OG AVVIKSHÅNDTERING		
42	Vi har rutiner for gjennomføring av regelmessige stikkontroller.	Håndbok kapittel 7 (Sikkerhetsrevisjon)	
43	Vi har gjennomført stikkontroll av informasjonssikkerhetssystemet i løpet av de 12 siste månedene.		
44	Vi skriver rapport med oppsummering av funn og ved behov forslag til tiltak etter stikkontroll.		
45	Vi har rutiner for å følge opp tiltaksplan fra stikkontroll.		
46	Vi har et system for hvordan avvik som oppstår i det daglige skal håndteres. Det betyr blant annet at de ansatte har mulighet til å rapportere avvik.	Håndbok kapittel 10 (Avvik og avvikshåndtering)	
	SIKKERHETSREVISJON		
47	Vi gjennomfører regelmessige sikkerhetsrevisjoner.	Håndbok kapittel 7 (Sikkerhetsrevisjon)	

48	Sikkerhetsrevisjonen vurderer organisering.	
49	Sikkerhetsrevisjonen vurderer sikkerhetstiltak.	
50	Sikkerhetsrevisjonen vurderer bruk av kommunikasjonspartner.	
51	Sikkerhetsrevisjonen vurderer sikkerhet hos leverandører.	
52	Vi har rutiner for regelmessig gjennomgang av informasjonssystemets fysiske informasjonssikkerhet.	
53	Vi har rutiner for regelmessig gjennomgang av den logiske sikringen av informasjon i informasjonssystemet.	
54	Sikkerhetstiltakene vi har, hindrer uautorisert tilgang til annet utstyr av betydning for informasjonssikkerheten.	

Andre forhold

	SJEKKLISTE	AKTØR	REFERANSE
	TAUSHETSPLIKT		
55	Vi har rutiner for å sikre at taushetsplikt etterleves der dette er nødvendig. For eksempel må alle som behandler beskyttelsesverdig informasjon undertegne en taushetserklæring.	Håndbok: • kapittel 11 (Partnere og leverandører) • kapittel 13 (Autorisasjon) Kvalitetsystem QM+: Infosikkerhet/ Instrukser • Infosikkerhet for ansatte	
56	De ansatte har taushetsplikt for informasjon som har betydning for informasjonssikkerheten.		
	DATABEHANDLERE		
57	Vi har oversikt over hvilke databehandlere vi bruker.	Håndbok kapittel 11 (Partnere og leverandører)	
58	Vi har inngått skriftlig databehandleravtale med alle eksterne virksomheter som behandler eller har tilgang til personopplysninger vi har ansvar for.		
	DOKUMENTASJON		
59	Vi har skriftlige rutiner for hvordan informasjonssystemet skal brukes og hvordan informasjon med betydning for informasjonssikkerheten er dokumentert.	Kvalitetsystem QM+: Infosikkerhet/ Instrukser • Infosikkerhet for ansatte • Bruk av kommunens IKT-løsninger	

60	Når dokumentasjonen for oppbygging av informasjonssystemet oppdateres eller erstattes, sørger vi for at all dokumentasjon for det gamle informasjonssystemet lagres i fem år.	Interne rutiner
61	Vi lagrer registreringer av uautorisert bruk og forsøk på uautorisert bruk av informasjonssystemet i minst 3 måneder.	
62	Vi lagrer registreringer av alle hendelser med betydning for sikkerheten i minst 3 måneder.	

17. Faggruppe IKT

Faggruppe IKT er et internt organ som koordinerer anskaffelser av IKT-løsninger og arbeid med informasjonssikkerhet og personvern:

- *Anskaffelse, integrasjon og koordinering*
  Faggruppen skal sørge for at all anskaffelse eller oppgradering av IKT-løsninger skal skje i tråd med kommunens IKT-strategi. Det skal også påses at kravene til arkivtjeneste, informasjonssikkerhet og personvern er ivaretatt før sak fremmes til rådmannens ledergruppe for avgjørelse.
- *Informasjonssikkerhet og personvern*
  Faggruppen skal være et rådgivende organ og pådriver for tiltak innen informasjonssikkerhet og personvern.

Faggruppen består av medlemmer som representerer fagområdene informasjonssikkerhet, personvern, IKT og innkjøp, samt kommunens sektorovergripende fagsystemer. Medlemmene har ikke nødvendigvis budsjettansvar og gruppen har derfor ingen beslutningsmyndighet. Faggruppen gir en skriftlig innstilling til rådmannens ledergruppe som tar endelig beslutning.

Dokumentreferanse
Instruks Faggruppe IKT (kommer)
Skjema og maler (kommer)

18. Personvernombud

Som offentlig virksomhet er Eigersund kommune pålagt å ha personvernombud, jf. personvernforordningen artikkel 37.

Personvernombud i Eigersund kommune:

Hilde F. Nilson
Fagleder digitalisering
e-post: personvernombud@eigersund.kommune.no
Telefon: 51 46 80 48

Kontaktinformasjon til ombudet finnes på kommunens hjemmesider.

Et personvernombud er en formelt oppnevnt kontakt for personvern og informasjonssikkerhet internt i organisasjonen mot ledelse/ansatte og eksternt mot Datatilsynet/den registrerte. Ombudet skal håndtere henvendelser fra de ulike aktørene og kan være et bindeledd mellom disse. Ombudet skal være en ressursperson som har kunnskap om virksomheten og behandlingen av personopplysninger.

Det juridiske ansvaret for at behandlingen av personopplysninger skjer i tråd med regelverket ligger hos behandlingsansvarlig (Rådmannen). Personvernombudet har som oppgave å gi råd og veiledning om hvordan Eigersund kommune best mulig kan ivareta personverninteressene. Dette innebærer blant annet å:

- Informere og gi råd om de forpliktelsene kommunen har etter personvernlovgivningen
- Kontrollere overholdelsen av personvernregelverket
- Gi råd om vurdering av personvernkonsekvenser
- Samarbeide og rådføre med Datatilsynet
- Bidra til å få oversikt over behandlingene
- Ta imot henvendelser fra de registrerte om personvernspørsmål

Personvernombudet skal tidlig involveres i alle saker som handler om behandling av personopplysninger i kommunen. Personvernombudet rapporterer til høyeste ledelsesnivå.

Dokumentreferanse
Kontaktinformasjon personvernombud
Sikkerhetsorganisasjonen
Rutiner (kommer)
Normen faktaark 35 – Personvernombud