Sikkerhetsorganisasjonen

Gjelder for: Alle ansatte

Vedtatt av: Rådmannen

Dokumentansvarlig (Enhet): Interne tjenester

Revisjonsintervall: Årlig

Distribusjon: Intranett, hjemmeside, QM+

Merknad: Vedlegg til Håndbok for informasjonssikkerhet.

Innhold

1. Formål og ansvar for informasjonssikkerhet

Formålet med dette dokumentet er å beskrive organiseringen av arbeidet med informasjonssikkerhet slik at det er tydelig hvem som er ansvarlig på ulike områder, og hva de er ansvarlig for.

Ansvaret for informasjonssikkerhet innebærer både et overordnet ansvar for at kommunen har tilfredsstillende og dekkende informasjonssikkerhet iht. gjeldende lovverk, og et ansvar for at ledere på alle nivåer, ansatte, innleid personell og leverandører følger de spesifikke krav og plikter som gjelder i kommunen. Databehandler har et selvstendig ansvar for at gjeldende lovverk følges slik det er regulert i avtale med kommunen eller andre parter.

2. Loven

Personvernforordningen artikkel 24 - Den behandlingsansvarliges ansvar (utdrag):
Skal den behandlingsansvarlige gjennomføre egnede tekniske og organisatoriske tiltak for å sikre og påvise at behandlingen utføres i samsvar med denne forordning..

- Rådmannen har det overordnete ansvar for at informasjonssikkerheten i kommunen ligger på et forsvarlig nivå.
- Rådmannen er som behandlingsansvarlig ansvarlig for at det etableres en sikkerhetsorganisasjon som koordinerer og gjennomfører informasjonssikkerhetsarbeidet.
- Behandlingsansvarlig kan delegere operativt ansvar for daglige arbeidsoppgaver, men ikke ansvaret i forhold til loven.
- Utøvelsen av sikkerhetsansvaret og -arbeidet vil skje på ulike nivå i organisasjonen. Organiseringen og innholdet i oppgaver og roller vil være dynamisk.

3. Organisering og roller

Det er etablert en sikkerhetsorganisasjon med følgende roller til å ivareta rådmannens ansvar knyttet til informasjonssikkerhetsarbeid og personvern:

1. Rådmann
2. Rådmannens ledergruppe
3. Sikkerhetsleder
4. Sikkerhetsteam
   - Dokumentsikkerhet (arkivleder)
   - Fysisk sikkerhet (bygg- og eiendomssjef)
   - IKT sikkerhet (IKT-leder)
   - Internkontroll (kvalitetsansvarlig)
   - Normen (rådgiver helse og omsorg)
5. Systemeier (Kommunalsjef)
6. Enhetsledere
7. Systemansvarlig
8. Ansatt
9. Faggruppe IKT
10. Beredskapsleder
11. Personvernombud

Alle roller i sikkerhetsorganisasjonen skal ha en stedfortreder.

Dokumentreferanse
Sikkerhetsorganisasjon Eigersund kommune – Informasjonssikkerhet og personvern
Medlemmer i sikkerhetsteam (lenke kommer)
Faktaark 01 - Ansvar og organisering (Normen)

3.1 Rådmann (behandlingsansvarlig)

Som overordnet ansvarlig er rådmannen behandlingsansvarlig i Eigersund kommune og skal sørge for:

- Å fastsette mål og strategi for informasjonssikkerhet
- At kommunen har en sikkerhetsorganisasjon med ansvar for å etablere og iverksette et styringssystem for informasjonssikkerhet, dokumentere systemet, samt gjennomføre tiltak knyttet til informasjonssikkerheten.
- At det etableres rutiner som sikrer at personvernombudet på riktig måte og til rett tid involveres i alle spørsmål som gjelder vern av personopplysninger.
- Tilstrekkelige ressurser, både personell og økonomiske, slik at tilfredsstillende informasjonssikkerhet og personvern opprettholdes.
- At styringssystem for informasjonssikkerhet er en del av kommunens helhetlige internkontroll.

Behandlingsansvarlig kan ikke delegere sitt juridiske ansvar, men det daglige operative behandlingsansvaret for informasjonssikkerhet er i Eigersund kommune delegert til systemeier (kommunalsjef).

3.2 Rådmannens ledergruppe

- Vedta akseptabelt sikkerhetsnivå.
- Vedta innkjøp, anskaffelse eller større oppgradering av eksisterende IKT-løsninger på bakgrunn av innstilling fra faggruppe IKT.
- Være pådriver i kommunens arbeid innen informasjonssikkerhet og personvern.
- Delta i gjennomføring av ledelsens årlige gjennomgang av sikkerhet (LGS).

3.3 Sikkerhetsleder

- Sørge for en hensiktsmessig og velfungerende sikkerhetsorganisasjon.
- Påse at vedtatt akseptabelt sikkerhetsnivå overholdes.
- Lede og gjennomføre ledelsens årlige gjennomgang av sikkerhet.
- Lede sikkerhetsteam
- Lede Faggruppe IKT.
- Etablere og vedlikeholde kommunens internkontrollsystem for informasjonssikkerhet og personvern, herunder:
  - Gjennomføre sikkerhetsrevisjon.
  - Påse at det gjennomføres risikovurderinger.
  - Påse at det gjennomføres opplærings- og motivasjonstiltak for å ivareta informasjonssikkerhet og personvern.
  - Påse at registeroversikt over alle behandlinger vedlikeholdes.
  - Påse at avviksmeldinger følges opp.

- Påse at sikkerhetsarbeid, så langt det er hensiktsmessig, er integrert på tvers av internkontrollområder.

- Holde organisasjonen faglig oppdatert innen informasjonssikkerhet og personvern.

3.4 Sikkerhetsteam

Kommunens sikkerhetsteam består av:

- Sikkerhetsleder (teamleder)
- Dokumentsikkerhet (arkivleder)
- Fysisk sikkerhet (bygg- og eiendomssjef)
- IKT sikkerhet (IKT-leder)
- Internkontroll (kvalitetsansvarlig)
- Normen (rådgiver helse og omsorg)

Sikkerhetsteamet møtes 2 ganger i året, og ellers ved behov. Alle har et ansvar for å:

- Støtte sikkerhetsleder i arbeidet med informasjonssikkerhet og personvern
- Holde organisasjonen faglig oppdatert innen informasjonssikkerhet og personvern – hvert fagområde.
- Delta i ledelsens årlige gjennomgang.
- Delta i faggruppe IKT (ansvarlig for fysisk sikkerhet møter ved behov)

3.4.1 Dokumentsikkerhet (arkivleder)

- Sørge for tilfredsstillende informasjonssikkerhet og personvern, herunder:
  - Påse at gjeldende lovverk, instrukser og rutiner for dokumentsikkerhet følges.
  - Påse riktig bruk av gradering av dokumenter

3.4.2 Fysisk sikkerhet (bygg- og eiendomssjef)

- Sørge for tilfredsstillende informasjonssikkerhet og personvern, herunder:
  - Påse at fysisk sikkerhet og tilgang til kommunens bygg og eiendom (skallsikring) blir tilfredsstillende ivaretatt iht. gjeldende lovverk, instrukser og rutiner.
  - Påse at det er tilfredsstillende kontroll på fysiske og elektroniske nøkler, koder o.l. som gir adgang til kommunens bygg og eiendom.

3.4.3 IKT- sikkerhet (IKT-leder)

- Sørge for tilfredsstillende informasjonssikkerhet og personvern, herunder:
  - Bidra i prosessen med å gjennomføre risikovurderinger.
  - Bidra i prosessen med å gjennomføre opplærings- og motivasjonstiltak for å ivareta informasjonssikkerhet og personvern.
  - Sikre at den daglige driften av kommunens datanettverk og IKT-system drives i samsvar med sikkerhetspolitikken.
  - Sørge for at det jevnlig blir foretatt dokumenterte stikkprøver av driftslogger i ulike system der dette ikke kan gjøres av andre systemansvarlige.
  - Sørge for at alle elementer i datanettverket er dokumentert med iverksatte sikkerhetstiltak og at dokumentasjonen er tilgjengelig
- Vedlikeholde IT-beredskapsplan.

3.4.4 Internkontroll (kvalitetsansvarlig)

- Følge opp og koordinere internkontroll- og kvalitetsarbeidet, herunder informasjonssikkerhet, for alle områder i og sikre et helhetlig internkontrollsystem for kommunen.
- Bidra til tilfredsstillende rutiner og verktøy for avvikshåndtering knyttet til informasjonssikkerhet og personvern.

3.4.5 Normen (rådgiver helse og omsorg)

- Sørge for tilfredsstillende informasjonssikkerhet og personvern, herunder:
  - Påse at Normens krav blir ivaretatt

3.5 Systemeier (Kommunalsjef)

Det daglige operative behandlingsansvaret for informasjonssikkerheten i den enkelte avdeling er delegert fra behandlingsansvarlig til systemeier. Dette innebærer også et ansvar for de IKT-løsninger vedkommende er systemeier for.

Systemeier har delegert deler av det daglige operative behandlingsansvaret til enhetsleder og systemansvarlig.

- Sørge for tilfredsstillende informasjonssikkerhet og personvern, herunder:
  - Påse at gjeldende lovverk, instrukser og rutiner følges.
  - Gjennomføre årlig egenkontroll av informasjonssikkerheten i avdelingen.
  - Påse at avvik blir rapportert og følges opp.
  - Oppnevne og autorisere systemansvarlige med stedfortredere og superbrukere ved behov.
  - Sikre at forholdet til leverandører, partnere og andre eksterne aktører er i samsvar med gjeldende krav.
  - Påse at det utarbeides brukerinstrukser og gjennomføres risikovurderinger for alle behandlinger av personopplysninger.
  - Påse at aktuelle saker blir meldt opp til faggruppe IKT.
  - Påse at oversikt over behandlinger av personopplysninger innenfor egen avdeling holdes oppdatert til enhver tid.
  - Støtte enhetsledere i arbeidet med informasjonssikkerhet, ref. ansvar beskrevet i punkt 3.6 «Enhetsledere».

3.6 Enhetsledere

Deler av det daglige operative behandlingsansvaret for informasjonssikkerheten i den enkelte enhet er delegert fra systemeier til enhetsleder.

3.6.1 Enhetsleder med personalansvar

- Autorisere enhetens ansatte for tilgang til IKT-løsninger og gradert informasjon i egen enhet ut fra tjenstlig behov.
- Holde oversikt og sørge for at autorisasjon, tilganger, nøkler, lagringsmedia og annet utstyr inndras når behov opphører, ansatt slutter eller går ut i langvarig permisjon.
- Sørge for at enhetens ansatte har lest og forstått de til enhver tid gjeldende instrukser og rutiner innen informasjonssikkerhet og personvern.
- Sørge for at enhetens ansatte har signert "Taushetserklæring i Eigersund kommune."
- Sørge for at informasjonssikkerhet og personvern er tema på enhetsmøter

- Gjennomgå enhetens avvik innen informasjonssikkerhet og personvern sammen med enhetens ansatte, minimum en gang i året.
- Sørge for at ansatte gjennomgår nødvendig opplæring innen informasjonssikkerhet og personvern.
- Overfor systemeier bidra til at punktene beskrevet i 3.6.2 «Enhetsleder uten personalansvar» følges opp.

3.6.2 Leder uten personalansvar (fagansvarlig)

- Overfor systemeier bidra til at:
  - Det skapes en positiv sikkerhetskultur i enheten.
  - Informasjonssikkerhet og personvern i enheten blir tilfredsstillende ivaretatt iht. gjeldende lovverk, instrukser og rutiner.
  - Enhetens avvik innen informasjonssikkerhet og personvern følges opp med nødvendige tiltak.
  - Gjeldende brukerinstruks for bruk av enhetens IKT-løsninger følges.
  - Nye eller endrede behov i behandling av personopplysninger blir gjort kjent.

3.7 Systemansvarlig (IKT-løsning)

Deler av det daglige operative behandlingsansvaret for informasjonssikkerheten i de enkelte IKT-løsningene er delegert fra systemeier til systemansvarlig.

- Sørge for tilfredsstillende informasjonssikkerhet og personvern, herunder:
  - Gi tilgang til IKT-løsningen etter skriftlig autorisasjon fra enhetsleder
  - Sørge for at gjeldende brukerinstruks følges.
  - Gjennomføre risikovurdering av IKT-løsningen
  - Sørge for at avvik innen informasjonssikkerhet og personvern rapporteres.
  - Bidra i gjennomføring av opplærings- og motivasjonstiltak for å ivareta informasjonssikkerhet og personvern.
  - Ha kontakt med leverandør vedrørende IKT-løsningens funksjonalitet og dokumentasjon.

Ved behov for ekstra ressurser kan det oppnevnes superbrukere som bistår systemansvarlig og stedfortreder med arbeidsoppgavene ute i enhetene.

3.8 Ansatt

Med ansatte menes fast og midlertidig ansatt, samt innleid personell (for eks. konsulent eller håndverker), studenter, praktikanter, mv. Informasjonssikkerhet er hver enkelt medarbeiders ansvar.

- Forstå betydningen av sikker behandling av informasjon i forbindelse med eget arbeid.
- Være kjent med og følge gjeldende aktuelle lovverk, instrukser og rutiner innen informasjonssikkerhet og personvern.
- Rapportere avvik innen informasjonssikkerhet og personvern.
- Delta i opplæring innen informasjonssikkerhet og personvern.
- Foreslå tiltak til forbedringer

Dokumentreferanse

Instruks – Informasjonssikkerhet for ansatte

3.9 Faggruppe IKT

- Er et rådgivende organ innen informasjonssikkerhet, behandling av personopplysninger og personvern.
- Avgi innstilling til rådmannens ledergruppe før vedtak om innkjøp, anskaffelse eller større oppgradering av eksisterende ikt-løsninger og påse at:
  - Det er klart definert hvilke arbeidsområder og oppgaver løsningen skal ivareta og hvilke det ikke er tillatt brukt til.
  - Løsningen ivaretar tilfredsstillende informasjonssikkerhet og personvern.
  - Det er definert hvem som er systemeier.
- Være pådriver i kommunens arbeid innen informasjonssikkerhet og personvern.

Dokumentreferanse
(kommer)

3.10 Beredskapsleder

- Påse at det er etablert tilfredsstillende planverk og beredskapstiltak innen informasjonssikkerhet og personvern.
- Delta i ledelsens årlige gjennomgang.

3.11 Personvernombud

Personombudets oppgaver står beskrevet i personvernforordningen artikkel 39.

- Informere og gi råd om de forpliktelsene kommunen har etter personvernlovgivningen.
- Kontrollere overholdelsen av personvernregelverket.
- Ved behov, gi råd om vurdering av personvernkonsekvenser (DPIA)
- Samarbeide med Datatilsynet og fungere som kontaktpunkt for tilsynet ved spørsmål.
- Ved behov, rådføre med Datatilsynet.
- Prioritere innsatsen dit hvor personvernrisikoen er høyest.
- Bidra til å få oversikt over behandlingene.
- Ta i mot henvendelser fra de registrerte om alle spørsmål knyttet til behandling av deres opplysninger, og om utøvelsen av rettighetene de har i henhold til personvernforordningen.