Instruks

Informasjonssikkerhet og personvern

Instruks for alle ansatte - informasjonssikkerhet

Gjelder for: Alle ansatte

Vedtatt av: Rådmannen

Dato: 20.09.2018 | **JpID:** 18/30465

Dokumentansvarlig (Enhet): Interne tjenester

Revisjonsintervall: Årlig

Distribusjon: Intranett, hjemmeside, QM+

Merknad: Alle ansatte skal ha signert på at instruksen er lest og forstått ved ansettelse.

Innholdsfortegnelse

1. INNLEDNING

Denne instruksen gjelder alle ansatte i Eigersund kommune og regulerer ansvar, plikter og retningslinjer for informasjonssikkerhet og personvern.

Instruksen er en del av den grunnleggende opplæringen nye ansatte skal ha før de får tilgang til Eigersund kommunes informasjonssystemer[1].

Den nyansatte skal skriftlig bekrefte at han/hun har forstått og akseptert å følge denne instruksen og tilhørende rutiner og prosedyrer i sitt arbeid i Eigersund kommune.

1.1. Hensikt

God informasjonssikkerhet oppnås gjennom den enkelte ansattes holdning og årvåkenhet, og ved at den enkelte ansatte tar ansvar for informasjonssikkerheten og følger gjeldende retningslinjer innenfor sitt arbeidsområde.

Instruksen skal bidra til riktig behandling av personopplysninger, tilfredsstillende informasjonssikkerhet og korrekt og riktig anvendelse av kommunens informasjonssystemer.

Instruksen skal bidra til å hindre uønsket bruk av kommunens IKT-løsninger og til å styrke informasjonssikkerheten i kommunen.

1.2. Ansvarsforhold

Den enkelte ansatte er selv ansvarlig for at denne instruksen følges.

Enhetsleder er ansvarlig for å gjøre instruksen kjent for den ansatte, og påse at ingen nye ansatte får tilgang til kommunens informasjonssystemer før denne instruksen er kjent og forstått.

Brudd på instruksen håndteres i henhold til kommunens avvikshåndteringsrutiner.

Etterlevelse av denne instruksen vil bli sporadisk kontrollert gjennom kommunens internkontrollsystem.

1.3. Definisjoner

Se dokumentet "Definisjoner" som du finner her: Definisjoner – Informasjonssikkerhet og personvern

[1] ***Informasjonssystem:*** Et system for innsamling, lagring, behandling, overføring og presentasjon av informasjon. Et informasjonssystem kan være helt manuelt eller et system basert på IKT.

2. INFORMASJONSSIKKERHET I EIGERSUND KOMMUNE

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.

Som ansatt i Eigersund kommune skal du være kjent med:

2.1 Sikkerhetsorganisasjon – rolle og ansvar

For mer utfyllende informasjon se Sikkerhetsorganisasjon i Eigersund kommune.

Som ansatt skal du kjenne til hvordan kommunen har organisert sikkerhetsarbeidet. Personvernlovgivningen definerer roller som angir ansvars- og myndighetsområde for å ha et effektivt internkontrollsystem.

Behandlingsansvarlig
Rådmannen er behandlingsansvarlig i Eigersund kommune, og har det overordnede ansvaret for at de personopplysninger kommunen behandler er tilfredsstillende sikret. Behandlingsansvarlig kan delegere operativt ansvar for daglige arbeidsoppgaver, men ikke ansvaret i forhold til lovverket.

Daglig ansvar
Det daglige ansvaret innenfor det enkelte fagområde er delegert fra kommunalsjef (systemeier) til den enkelte enhetsleder. Den ansatte har selv et ansvar for det daglige praktiske sikkerhetsarbeidet og oppfølgingen innen egen enhet.

Sikkerhetsleder
Koordinerer sikkerhetsarbeidet i kommunen. Sikkerhetsleder har ansvar for oppfølging av informasjonssikkerhet og kvalitetssikring av retningslinjer og rutiner på et overordnet nivå.

Personvernombud
Personvernombudet har både en rådgiverfunksjon og en kontrollfunksjon. Personvernombudet bistår kommunens innbyggere / tjenestemottakere ved for eksempel krav om innsyn. Personvernombudet gir også råd til kommunens sikkerhetsorganisasjon for å sikre tilfredsstillende informasjonssikkerhet.

IKT sikkerhet
IKT-leder er ansvarlig for teknisk drift av kommunens IKT-løsninger (både utstyr og systemer) og tilhørende sikkerhetstiltak.

Faggruppe IKT

Faggruppe IKT er et rådgivende organ innen informasjonssikkerhet og personvern. Avgir innstilling til rådmannens ledergruppe før vedtak om anskaffelse eller større oppgradering av eksisterende IKT-løsninger foretas.

Systemansvarlig
Hvert fagsystem har en systemansvarlig, og du må vite hvem som er ansvarlig for de fagsystem som du benytter. Systemansvarlig har blant annet ansvar for ajourhold og vedlikehold av tilganger. Det er ofte systemansvarlig du skal henvende deg til dersom du har behov for mer opplæring.

Ansatte
Kommunens ansatte skal bruke informasjonssystemene til å utføre pålagte oppgaver, og skal autoriseres for tilgang etter gjeldende rutiner for dette. Alle ansatte skal ha nødvendige kunnskaper for å bruke systemene i samsvar med fastlagte rutiner, og opplæring skal være gitt før tilgang gis. Alle har et ansvar for å melde avvik i tråd med kommunens rutiner for avvikshåndtering.

2.2 Mål og strategier for informasjonssikkerhet

For mer utfyllende informasjon se Håndbok for informasjonssikkerhet kapittel 4 - Sikkerhetsmål og sikkerhetsstrategi.

Sikkerhetsmål:
Eigersund kommunes 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.

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

- ***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.

- ***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.

2.3 Sikkerhetstiltak alle ansatte skal følge

Overordnede rutiner og retningslinjer for informasjonssikkerhet finner du på kommunens intranett, og i kommunens kvalitetssystem. Her ligger også kommunens Håndbok for informasjonssikkerhet som du som ansatt plikter å gjøre deg kjent med.

I tillegg vil den enkelte enhet ha lokale rutiner for informasjonssikkerhet. Disse er publisert under enhetens eget område i kommunens kvalitetssystem.

2.3.1. Opplæring

- Du har rett og plikt til å gjennomgå nødvendig opplæring.
- Nærmeste leder er ansvarlig for at du får opplæring.
- Alle ansatte i Eigersund kommune skal ha grunnopplæring i informasjonssikkerhet og i de fagsystemer de skal benytte.

- Alle ansatte skal ha opplæring i hvordan de melder avvik på informasjonssikkerhet og hvordan avvik behandles.

2.3.2. Taushetsplikt

Se også QM+ (INFO - Ansettelsesforhold:rutiner, reglementer m.m): Prosedyre for introduksjon av nyansatte og taushetserklæring

- Alle som tjenestegjør for Eigersund kommune skal signere en taushetserklæring i forbindelse med inngåelse av arbeidskontrakt eller oppdragsavtale. Signert taushetserklæring skal arkiveres i kommunens sak-/arkivsystem.

- Taushetsplikten gjelder ikke bare utad, men også overfor andre medarbeidere som ikke har tjenstlig behov for tilgang til opplysningene.

- Taushetsplikten gjelder også etter at arbeidsforholdet er avsluttet, og varer i praksis livet ut.

- Alle ansatte må være bevisst på hvilken type informasjon man til enhver tid behandler, og om det kan være til skade for enkeltpersoner, kommunen eller andre om den kommer på avveier. Dette gjelder for eksempel opplysninger om tjenestemottakere, ansatte, kommunens virksomhet, sikkerhetsmessige og organisatoriske forhold, både i muntlig, skriftlig og elektronisk format, herunder også lyd og bilder.

- Informasjon skal alltid lagres forsvarlig. I de aller fleste tilfeller betyr dette at informasjon lagres i kommunens sak-/arkivsystem eller andre aktuelle fagsystemer. Er man i tvil, kontakt nærmeste leder eller sentralarkivet.

- Ingen ansatte skal aktivt søke opplysninger som ikke er nødvendige for utførelse av deres arbeidsoppgaver (snoking), verken gjennom samtale eller gjennomgang av manuelle eller digitale dokumenter. Dette gjelder spesielt for konfidensielle og sensitive opplysninger, og selv om opplysningene rent praktisk er tilgjengelig for vedkommende.

- Kontakt nærmeste leder snarest når IKT-utstyr eller informasjon kommer på avveier.

2.3.3. Bruk av kommunens IKT-løsninger

Ved å signere på denne instruksen bekrefter du også at du har gjort deg kjent med Instruks - Bruk av kommunens IKT-løsninger.

Instruksen gjelder for alle ansatte og innleid personell med tilgang til kommunens IKT-løsninger. Instruksen regulerer ansvar, plikter og retningslinjer for alle som benytter IKT-løsninger i Eigersund kommune.

Instruksen skal bidra til å hindre uønsket bruk av kommunens IKT-løsninger og til å styrke informasjonssikkerheten i kommunen.

2.3.4. Sikkerhet og orden på egen arbeidsplass

Alle ansatte er ansvarlig for at sensitiv / gradert informasjon på egen arbeidsplass er forsvarlig sikret.

- La ikke sensitiv / gradert informasjon ligge tilgjengelig for uvedkommende på arbeidsplassen.

- Velg korrekt utskriftsenhet (skriver, kopimaskin mv.) og sørg for at utskrifter hentes umiddelbart, med mindre utskriftstjenester som for eks. passord eller «FollowMe» benyttes.
- Oppbevar lagringsmedier med sensitiv / gradert informasjon på en sikker måte (innelåst).
- Kast ikke sensitiv / gradert informasjon i papirkurven, men makuler den. Makulering av gradert informasjon skal gjøres på en slik måte at det ikke under noen omstendigheter er mulig å rekonstruere informasjonen. Dette gjøres fortrinnsvis ved bruk av makuleringsmaskin, brenning eller fysisk knusing.
- Datamedier som ikke lenger er i bruk skal leveres inn til IKT-kontoret for forsvarlig destruksjon.
- Sørg for at uvedkommende ikke har tilgang til steder hvor manuelle arkiv, IKT-utstyr o.l. er plassert uten ifølge med en ansatt.
- Lås alltid maskin når du forlater den (bruk "Windows"-tasten + "L"-tasten). Skru av maskinen når du går for dagen.

2.3.5. Den registrertes rettigheter

De som er registrert i en av Eigersund kommune sine systemer har rett på innsyn i egne opplysninger. Vedkommende har også rett til å be om at uriktige, ufullstendige eller opplysninger Eigersund kommune ikke har adgang til å behandle blir rettet, slettet eller supplert.

Slike henvendelser skal videreformidles i henhold til interne rutiner, oftest til nærmeste leder. Fordi du som ansatt har et formidlingsansvar vedrørende den registrertes rettigheter, må du kjenne til følgende rutiner i møte med innbyggere, tjenestemottakere o.a.:

- *Rutine for iverksettelse eller opphør av behandling av personopplysninger*
- *Rutine for innhenting og kontroll av samtykke*
- *Rutine for informasjonsplikt ved innsamling av personopplysninger*
- *Rutine for innsyn i personopplysninger (kommer)*
- *Rutine for sletting av personopplysninger*
- *Rutine for retting og supplering av personopplysninger*

Krav fra den registrerte skal besvares kostnadsfritt og senest innen 30 dager.

Se også Personvernerklæring på våre nettsider.

2.4 Kommunens rutiner for avvikshåndtering - informasjonssikkerhet

Ethvert brudd på lov, forskrift eller interne retningslinjer og instrukser skal rapporteres snarest for om mulig å minimere skadeomfang og unngå gjentakelse.

Kommunen har et elektronisk avvikssystem hvor informasjonssikkerhet er et eget avviksområde.

Alle ansatte skal melde avvik når de oppdager brudd på sikkerhetstiltak og/eller når oppgaver er utført i strid med de rutiner som er besluttet.

Å melde avvik er uttrykk for en sikkerhetskultur hvor de ansatte bidrar til tilfredsstillende informasjonssikkerhet i hele kommunen. Alle ansatte i vår kommune har medansvar for å sikre personvern, og å bidra med en bevisst holdning i informasjonssikkerhet i sitt daglige arbeid.

Dersom behandling av personopplysninger og bruk av kommunens IKT-løsninger skjer i strid med gjeldende lovverk og kommunens retningslinjer, anses dette som tjenesteforsømmelse, og vil kunne føre til sanksjoner i henhold til gjeldende rutiner og reglement.

2.5 Kommunens håndbok for informasjonssikkerhet

Kommunens "Håndbok for informasjonssikkerhet" er et verktøy for ledere og ansatte i kommunen for å ivareta tilfredsstillende informasjonssikkerhet.

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.

Håndboken er tilgjengelig på kommunens intranettsider samt i kommunens kvalitetssystem, og ved å trykke på denne linken: Håndbok for informasjonssikkerhet.