Innføring informasjonssikkerhet og personvern for vikarer og ansatte i Sør-Odal kommune

Kunnskap om personvern og informasjonssikkerhet.

I Sør-Odal kommune skal vi behandle personopplysninger og informasjon i tråd med kravene i relevante lover og forskrifter. Som ansatt skal du ha kjennskap til informasjonssikkerhet og vite hvordan behandling av personopplysninger skal foregå i daglig drift, for å sikre allmenn tillit til behandling og omdømme i det offentlige rom.

Taushetserklæring

Som ansatt har du en yrkesmessig taushetsplikt, som skal etterleves ved all håndtering av taushetsbelagte opplysninger. Taushetserklæring skrives under på eget skjema.

Du har et selvstendig ansvar for å overholde taushetsplikten og ivareta sikkerhet og personvern på vegne av kommunen.

Personvernet innebærer at

- vi styrker innbyggernes frihet og rettigheter. Opplysninger om en person skal betraktes som dennes eiendom, og behandles med varsomhet (personopplysningsloven).

- Personopplysninger skal kun brukes til det formålet de er samlet inn til.
- Hvis ikke bruken av opplysningene kan hjemles i lov eller avtale må vi be om samtykke til å få bruke dem.
- Den som har gitt samtykke kan trekke dette tilbake når som helst.
- Det skal informeres klart og tydelig til den som er registrert hva opplysningene om dem skal brukes til og hvordan vi håndterer dem.
- De som er registrert har rett til å se hva som er lagret om dem.

Det er rådmannen som er ansvarlig for behandling av personopplysningene, men delegerer nødvendigvis dette til de som håndterer og benytter opplysningene i arbeidet. I Sør-Odal kommune informerer vi om dette gjennom «personvernerklæringen».

Informasjonssikkerhet innebærer at

- informasjonen er tilgjengelig *kun* for den som trenger den
- den *er tilgjengelig* når den trengs
- informasjonen er *riktig*

Teknologisk og fysisk

- Mye av det følgende omhandler nødvendigvis hvordan vi skal benytte tekniske hjelpemidler (data, e-post osv), fordi vi i stadig større grad benytter dette når vi behandler informasjon. Dette må du forholde deg til selv om du ikke benytter tekniske hjelpemidler i jobben din.

Informasjonssikkerhet og personvern gjelder også for fysiske dokumenter (og muntlige opplysninger).

Generelt om bruk av datautstyr

Sør-Odal kommune er medlem av Hedmark IKT (HIKT), interkommunalt IT-selskap som drifter - og utvikler løsninger for og med 7 kommuner.

Når vi trenger hjelp eller har behov for endringer er det hit vi henvender oss på telefon eller via selvbetjeningsportalen og helpdesk.

Kommunenes informasjonssystemer er beregnet på jobbrelaterte formål. Privat bruk, f.eks. e-post og private filer, tillates i begrenset omfang så lenge det ikke påvirker jobbrelaterte oppgaver.

Brukernavn, passord og skjermsparer
Du blir tildelt brukernavn og førstegangs passord. Brukernavnet og passordet er strengt personlig. Datamaskinen skal som hovedregel låses når arbeidsplassen forlates i kortere eller lengre perioder. Det kan du enkelt gjøre ved å benytte Ctrl + Alt + Delete, - og du kan raskt logge deg på igjen. Maskinen skal være satt opp med automatisk skjermsparer med aktivering etter 10 minutters inaktivitet. Du skal alltid logge av før du overlater maskinen til andre.

Internett

Det er ikke tillatt å laste ned utuktig materiale, opphavsrettslig beskyttet materiale (f.eks. musikk, filmer og programvare) eller annet som er i strid med lovverket. Tjenester for ulovlig fildeling og priatkopiering tillates ikke. Ressurskrevende tjenester, f.eks. radiolytting og TV/videostreaming skal begrenses for ikke å påvirke jobbrelatert trafikk i nettet. Kommunen har anledning til å logge informasjon om internett- og e-posttrafikk for å sikre alminnelig drift, samt sporing ved aktuelle sikkerhetsbrudd.

E-post

All jobbrelatert e-post (innkommende og utgående) skal gå gjennom kommunens e-postløsning. Arkivverdig e-post skal journalføres i WebSak.
Husk at sensitiv personinformasjon aldri skal sendes med E-post.

Det skal vises stor aktsomhet med bruk av internett og e-post på PC-er som er tilkoblet datanettverk hvor sensitive opplysninger blir behandlet.

Sosiale medier

Ansatte i kommunene må være bevisste på hva som deles på sosiale medier. Ansatte vil alltid være en representant for kommunene, i større eller mindre grad. Du finner mer om dette under etiske retningslinjer og som egne retningslinjer i "Kilden".

Fysisk adgang og personalsikkerhet

Dersom du mister nøkkel eller adgangskort, skal det umiddelbart meldes fra til servicetorget.
Ansatte som slutter eller går ut i permisjon, skal levere nøkler/nøkkelkort til sin nærmeste leder.

Den som mottar besøk, er ansvarlig for at besøkende:

- hentes og følges tilbake
- ikke oppholder seg i kommunens lokaler uten i følge med en av de ansatte

Lagring og oppbevaring

Elektronisk lagring av sensitiv informasjon skal kun skje i fagsystemer eller WebSak(sak/arkiv) - som er tilstrekkelig sikret.

Alle må sørge for sikkerhet på eget kontor eller arbeidsplass slik at papirer/minnepenner etc med sensitiv informasjon er låst inne og utilgjengelig for uvedkommende.

Informasjon som ikke skal arkiveres skal du slette når du ikke trenger den lenger. Dette er typisk interne arbeidsdokumenter som du lagrer på eget område (H:)

Det skal ikke være innsyn til skjermer eller papirer som inneholder sensitiv informasjon slik at uvedkommende kan få tilgang til opplysningene.

Avvik

Dersom du oppdager at informasjon ikke blir håndtert i samsvar med lov, forskrift, policy, eller den kommer på avveie, - da skal du melde avvik i "Kilden".

Avvik relatert til informasjonssikkerhet som blir meldt inn til leder, skal straks behandles, for å redusere eventuell skade ved hendelsen. Hvordan avikene håndteres videre finner du i Kilden:
Prosedyre for avvikshåndtering informasjonssikkerhet