RÆLINGEN KOMMUNE

REGLEMENT FOR INFORMASJONSSIKKERHET OG IKT I RÆLINGEN KOMMUNE

Innhold

Formålet med reglementet

Elektronisk behandling av opplysninger gir mange muligheter, men skaper også utfordringer for informasjonssikkerheten. Vi lever i en kompleks og sårbar dataverden, hvor feil bruk av våre datasystemer kan få store konsekvenser for kommunen. Reglementet, som alle ansatte har ansvar for å følge, skal bidra til en effektiv og sikker drift av IKT-systemene, samt korrekt bruk av data.

Formålet med reglementet er å bevisstgjøre hver arbeidstaker om den tillatte bruken av IKT i kommunen. Reglementet omhandler bl.a. sikring av data, innsyn, misbruk, samt den enkeltes ansvar for dette. Arbeidstaker har en plikt til å bruke kommunens IKT-systemer på en forsvarlig og etisk måte. Bruken skal være i kommunens interesse og følge gjeldende lovverk og reglement.

Anvendelse

Reglementet gjelder for bruk i Rælingen kommune eller for bruk av utstyr som er eid av Rælingen kommune. Telefonsystemene våre, skrivere, trådløst nettverk, mobiltelefoner og annet datautstyr er også en viktig del av vår infrastruktur, og reglementet omfatter også disse systemene. Reglementet er en del av tilsettingskontrakten som alle ansatte må sette seg inn i og skrive under på.

Ansvar for IKT-utstyr

Kommunens IKT-systemer og alt utstyr knyttet til dette er kommunens eiendom og stilles til arbeidstakers disposisjon, for bruk som arbeidsverktøy. Endring av systemoppsett på PC eller annet IKT-utstyr skal gjøres av Øyeren IKT, i samråd med Øyeren IKT eller av IKT-ansvarlige på skolene. Alle feil eller mistanker om feil i IKT-systemene skal meldes til Øyeren IKT snarest mulig. Arbeidstaker plikter å beskytte utstyret mot tyveri eller ureglementert bruk.

Postadresse: Postboks 100 2025 Fjerdingby
Besøksadresse: Bjørnholthagan 6 2008 Fjerdingby
Organisasjonsnr.: 952 540 556
Internett: www.ralingen.kommune.no
E-post: postmottak@ralingen.kommune.no
Telefon: 63 83 51 10
Telefaks: 63 83 52 33
Bankgiro: 1503.0543707

Ansvar for informasjonssikkerhet

Øyeren IKT (ØIKT) har ansvar for kommunens robusthet, dvs at organisasjonen og systemene er motstandsdyktige, og evner å gjenopprette normaltilstand ved hendelser.

Rælingen kommune har ansvaret for informasjonssikkerheten, herunder sikre at informasjon ikke blir kjent for uvedkommende (konfidensialitet), ikke blir endret utilsiktet eller av uvedkommende (integritet) og er tilgjengelig ved behov (tilgjengelighet). Informasjonssikkerhetsansvarlig ved digitaliseringsavdelingen støtter virksomhetsledelsen i informasjonssikkerhetsspørsmål, herunder er pådriver og tilrettelegger for en god etablering og gjennomføring av internkontroll innen informasjonssikkerhet i hele organisasjonen.

Hver enkelt ansatt, herunder fast ansatte, midlertidige ansatte eller vikarer er forpliktet til å gjøre seg kjent med og til enhver tid følge vedtatte sikkerhetsbestemmelser. Du har som bruker av IKT-systemene et eget ansvar for at særlige kategorier personopplysninger, tidligere kalt sensitive personopplysninger, ikke kommer på avveie eller misbrukes på noe vis.

Reglementet er en hjelp for deg til å kunne ivareta dette ansvaret.

Datasikkerhet

Alle ansatte plikter å sikre at utenforstående ikke får tilgang til Rælingen kommunes telefoner, datasystemer, nettverk og utstyr. Dette krever bl.a. at ansatte:

- Logger ut fra og slår av PC/terminal utenom arbeidstiden
- Logger ut av systemer ved fravær fra arbeidsplassen
- Låser PC/terminal m/skjermbeskytter ved korte fravær fra datamaskinen (møter o.l.)

Alle som skal ha tilgang til IKT-systemene vil få tildelt et brukernavn og et passord. Øyeren IKT har ansvaret for tildelingen etter at leder, gjennom lønns- og personalmelding, har meldt fra om tilsettingen, eller endring av tilganger på eksisterende brukere.

Brukernavn og passord er personlig. Som ansatt har du ansvaret for å beskytte nettverkspassordet ditt. La ikke andre koble seg på IKT-utstyr eller IKT-systemer med ditt passord. Dersom du har mistanke om at passordet har blitt kjent av uvedkommende, skal passordet byttes og hendelsen rapporteres som et avvik i Compilo.

Ansatte har taushetsplikt om personlige forhold som vedkommende har fått kjennskap til gjennom sitt tilsettingsforhold i kommunen. Dersom en ansatt er usikker mht. lovlighet av registrering av opplysninger, skal nærmeste leder eller Øyeren IKT kontaktes.

Personopplysninger skal kun lagres/skrives på maskiner og i systemer som er godkjent for dette. Disse maskinene/systemene må enten være tilkoblet intern sone eller sikker sone. Private filer skal ikke lagres i kommunens IKT-systemer. Lagring av data på lokal harddisk skal ikke forekomme. Det er utarbeidet en «lagringsguide» som beskriver mer detaljert hva som kan lagres hvor. Den finner du i Compilo.

Mobile lagringsenheter, for eksempel minnepinne og minnebrikker, utgjør en risiko ved ubevisst bruk. De kan også lett komme på avveie grunnet små i størrelse. Sensitive opplysninger må ikke lagres på mobil enhet hvis ikke data er kryptert/anonymisert. Et alternativ kan være å ha anonyme data og et kodeark ved siden av som kobler til person.

Ansattes innføring av eksterne data kan medføre at vi kan få datavirus og/eller datainnbrudd på våre nett. Derfor skal ikke maskiner/utstyr brukt utenfor Rælingen kommunes nett, kobles på våre nett uten at dette er avklart med og godkjent av Øyeren IKT. Privat datautstyr tillates ikke i Rælingen kommunes nettverk.

Ansatte er pliktig til å gjennomføre opplæring/kurs på datasystemene til Rælingen kommune, slik at vi sikrer at riktig bruk blir ivaretatt. Den ansattes leder er ansvarlig for at dette utføres så raskt som mulig etter ansettelse.

Ansatte plikter å rapportere til nærmeste leder eller til Øyeren IKT om forhold som kan ha betydning for brudd på Rælingen kommunes visjon, verdier og policy som er relatert til informasjonssikkerheten.

All saksbehandling skal utføres i kommunens sak-/ arkivsystem, eventuelt relevant fagsystem.

Sikker sone

Ansatte med tilgang til fagsystem der det behandles sensitiv informasjon på sikker sone må sørge for at slik informasjon ikke gjøres kjent for uvedkommende, og at sensitive data ikke lagres elektronisk andre steder enn på «sikker sone».

Det er ikke tillatt å skrive ut dokumenter fra sikker sone, så fremt det ikke er på en godkjent skriver plassert i fagenhetens kontormiljø som er beskyttet med «sikker utskrift.»

Ved bruk av fjernarbeidstilgang mot sikker sone skal alt IKT-utstyr behandles med særdeles høy forsiktighet. Bruk av fjernarbeidstilgang mot sikker sone på offentlige steder, slik som caféer, flyplasser og lignende, er ikke tillatt. Ved bruk av fjernarbeidstilgang mot sikker sone skal den ansatte være påpasselig slik at utenforstående ikke får innsyn på dataskjermen og kan se sensitive opplysninger.

Bruk av e-post

Elektronisk post må, forutsatt at den ikke er kryptert, betraktes å være relativt lett tilgjengelig for uvedkommende. Sensitive personopplysninger og annen sensitiv informasjon må ikke sendes som e-post. Sensitiv informasjon kan alternativt opplyses med telefonsamtale eller sendes med brev.

Dersom det mottas e-post med særskilte kategorier/sensitive personopplysninger, skal den ikke sendes videre, men skrives ut, slettes og sendes på papir til arkivet for skanning og registrering, eventuelt til vedkommende som kan skanne og registrere til fagsystem der henvendelsen skal besvares.

Lurer du på hva som betraktes som særskilte kategorier/sensitive personopplysninger, finner du informasjon her: Lenke til personvernforordningen artikkel 9: https://lovdata.no/dokument/NL/lov/2018-06-15-38/KAPITTEL_gdpr-2#gdpr/a9)

Det må ikke legges inn vedlegg og/eller tekst som inneholder sensitive personopplysninger i kalenderfunksjonen til Outlook da kalenderne til de fleste ansatte er åpne for alle.

Ikke klikk på lenker, eller åpne vedlegg i e-post dersom du har mistanke om at den kan være falsk. Ta skjermbilde av e-posten og send til Øyeren IKT for sjekk. (Ikke videresend).

Arkivverdig e-post skal sendes/legges i sak-/ arkivsystemet eller relevant fagsystem
Det er ikke tillatt å benytte kommunal e-post adresse til private formål slik som handel og aktivitet på internett da dette utgjør en sikkerhetsrisiko.

Viktig å rydde/slette. De ansatte mottar daglig store mengder e-post. For at ikke kommunens e-postkontoer skal fylles er det viktig at den enkelte rydder og sletter innhold i postkassen sin ved jevne mellomrom. Ved avslutning av arbeidsforholdet vil e-postkontoen bli slettet.

Innsyn

Arbeidsgiver kan bare gjøre innsyn i ansattes e-post, personlige filområder i kommunens datanettverk og annet elektronisk utstyr som er stilt til arbeidstakers disposisjon i to tilfeller; Når det er nødvendig for å ivareta driften av virksomheten, eller dersom det er en begrunnet mistanke om at arbeidstakers bruk av elektronisk lagret materiale medfører grovt brudd på arbeidstakers plikter. Annet elektronisk utstyr kan være f.eks chat-tjeneste, PC, mobiltelefon og nettbrett. Arbeidsgiver har **ikke** rett til innsyn i arbeidstakers egne kommunikasjonsmidler og private e-postkasser.

Det er et grunnkrav i personvernforordningen (GDPR) at innsyn må være nødvendig for et spesifikt formål. Det sentrale i kravet er at arbeidsgiver må overveie om det finnes mindre inngripende metoder for å oppnå samme formål.

Prosedyrer for innsyn skal følge § 3 i forskrift om arbeidsgivers innsyn i e-postkasse og annet elektronisk lagret materiale. Det er utarbeidet en egen rutine basert på forskriften som beskriver prosedyre som Øyeren IKT følger ved behov for innsyn. Rutinen ligger i Compilo. Det skal bl.a. så langt som mulig sendes varsel om innsyn til arbeidstaker som skal inneholde en begrunnelse for hvorfor innsyn skal gjøres, samt informasjon om arbeidstakers rettigheter.

Les eventuelt mer om dette i forskriften nevnt over.

Overvåking av brukere/driftsovervåking

Overvåking av nettverkene og brannmurer foregår kontinuerlig av drifts- og sikkerhetsmessige årsaker, samt for å sikre best mulig dataflyt. Ved mistanke om sikkerhetsbrudd vil loggene kunne benyttes i vurderingen.

Ansvarlig driftspersonell ved Øyeren IKT har taushetsplikt med hensyn til opplysninger om brukeren eller brukerens virksomhet, unntatt forhold som kan representere brudd på reglementet som blir varslet videre iht gjeldende varslingsrutiner.

Etisk riktig bruk

Det er ikke lov å bruke IKT-systemene til aktiviteter som strider mot norsk lov eller mot kommunens etiske retningslinjer.

Arbeidstaker må som bruker av IKT-systemene selv være oppmerksom på trusler fra internett og bidra til at disse utgjør en lavest mulig risiko for kommunen. Ansatte skal heller ikke benytte Rælingen kommunes nettverk/utstyr for egen privat og eller kommersiell vinning.

Repeterende brudd på det ovenstående kan få konsekvenser for den ansattes arbeidsforhold.

Brudd på arbeidskontrakt

Brudd på gjeldene reglement kan medføre at brukere nektes adgang til Rælingen kommunes nettverk/datamaskiner og annet utstyr.

Brudd på personvern, taushetsplikt m.m kan føre til erstatningsplikt eller politianmeldelse.

Arbeidstaker er ansvarlig for å tilegne seg tilstrekkelig kompetanse i bruk av IKT, gjennom å etterspørre opplæringstiltak eller delta på de som blir arrangert.