



Oslo

Informasjonssikkerhets- koordinator (ISK)

Rollekortene er veiledninger, basert på relevante styrende dokumenter i Oslo kommune. Det er ikke obligatorisk å ta i bruk rollekortene, med mindre dette er besluttet i den enkelte sektor/virksomhet.

Rollekortene beskriver typiske oppgaver for informasjonssikkerhet og/eller personvern som tilligger ulike roller. Oppgavene kan tilpasses den enkelte virksomhet, med mindre annet er bestemt.

ROLLE

Informasjonssikkerhetskoordinator (ISK) skal bistå virksomhetsleder i arbeidet med å sikre etterlevelse av regelverket. Koordinatoren vil også være en sentral rådgiver for virksomhetsleder og øvrig ledelse. Av denne grunn er det viktig at informasjonssikkerhetskoordinator får rapportere direkte til virksomhetsleder.

Informasjonssikkerhetskoordinatoren må samarbeide med virksomhetens personvernkoordinator (PKO), dersom denne rollen ivaretas av en annen ansatt. Det er også nødvendig å samarbeide med andre relevante roller, f.eks. systemeiere, systemforvaltere, sikkerhetsledere mv., både internt i virksomheten og ellers i kommunen.

Koordinatoren er virksomhetens kontaktpunkt innen informasjons- og IKT-sikkerhet for overordnet byrådsavdeling og for kommunens sentrale fagmiljø innen personvern og informasjonssikkerhet i Byrådsavdeling for finans.

Informasjonssikkerhetskoordinatoren er *ikke ansvarlig* for virksomhetens etterlevelse av lovverket for informasjonssikkerhet eller kommunens interne regelverk – dette ansvaret tilligger virksomhetsleder.

PLANLEGGE

- Utarbeide årsplan for virksomhetens oppgaver innen informasjonssikkerhet.
- Bistå virksomhetsleder i oppfølgingen av årsplanen.
- Utarbeide og vedlikeholde styrende dokumenter for informasjonssikkerhet for virksomheten, i tråd med kommunens styrende dokumenter.
- Forvalte oversikt over gjeldende myndighetskrav for å ivareta taushetsplikt og informasjonssikkerhet.

RÅDGIVNING OG KONTAKTPERSON

- Gi råd og veiledning innen informasjonssikkerhet til ledelsen og ansatte, både generelt og i prosjekter og anskaffelser.
- Bistå med å implementere informasjonssikkerhet i arbeidsprosesser.
- Være virksomhetenes kontaktperson innen spørsmål og oppgaver relatert til informasjonssikkerhet overfor overordnet byrådsavdeling, Byrådsavdeling for finans og kommunens personvernombud.

KOMPETANSE

- Vedlikeholde egen kompetanse på fagområdet.
- Delta på kommunens arrangementer og kurs for koordinatorene.
- Tilrettelegge for nødvendig og målrettet opplæring i informasjonssikkerhet til alle ansatte i virksomheten, inkludert ledelsen.
- Koordinere og delta i felles kampanjer for informasjonssikkerhet i virksomheten.

RISIKOSTYRING

- Bistå ved gjennomføring av overordnet risikovurdering for informasjonssikkerhet.
- Koordinere gjennomføringen av risikovurderinger og oppfølging av status.
- Bistå i å fasilitere virksomhetens risikovurderinger etter behov.
- Oppfølging av uakseptabel risiko.

RUTINER

- Bidra til å etablere og vedlikeholde rutiner innen informasjonssikkerhetsområdet, bl.a. for autorisering og tilgangskontroll, og for beredskap.
- Følge opp at etablerte rutiner etterleves.
- Bidra til å gjennomføre beredskapsøvelser for å sikre kontinuitet i virksomhetens tjenester.

HENDELSER OG AVVIK

- Bidra til å håndtere informasjonssikkerhetshendelser- og brudd.
- Bidra til oversikt over alle avvik og sikkerhetsbrudd.
- Rapportere alvorlige sikkerhetsbrudd til virksomhetsleder.

RAPPORTERING

- Bistå ved rapportering av alvorlige sikkerhetsbrudd til overordnet byrådsavdeling og til Byrådsavdeling for finans.
- Bistå virksomhetsleder med rapportering av informasjonssikkerhetstilstand gjennom virksomhetsleders egenerklæring, ledelsens gjennomgang og en oppsummering av hendelser og avvik.