



Oslo

Systemforvalter

Ansvar for informasjonssikkerhet og personvern

Rollekortene er veiledninger, basert på styrende dokumenter i Oslo kommune og anerkjent praksis på fagområdene. 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

Systemforvalter skal gjennomføre oppgaver innen informasjonssikkerhet og personvern for systemet i hele forvaltningsperioden dersom dette er delegert fra Systemeier. Delegeringen skal avtales skriftlig og kan baseres på kommunens *Mal for forvaltningsavtale*.

Systemforvalter kan ta beslutninger på vegne av Systemeier innenfor delegert myndighetsområde og gjeldende økonomiske rammer, dersom dette er avtalt innenfor eksempelvis følgende områder:

- Informasjonssikkerhet og personvern knyttet til anskaffelse og utfasing av systemer
- Foreslå og beslutte hva som er nødvendige risikoreduserende tiltak for å oppnå akseptabel risiko for virksomheten.

Systemforvalter skal rapportere etterlevelse av krav til informasjonssikkerhet og personvern til Systemeier.

Systemforvalter skal rapportere om hendelser og avvik innenfor informasjonssikkerhet og personvern til Systemeier.

PLANLEGGE OG DOKUMENTERE

- Planlegge gjennomføring av aktiviteter i utarbeidet årsplan for informasjonssikkerhet og personvern i systemet.
- Dokumentere tilstand på personvern og informasjonssikkerhet til systemeier gjennom egenerklæring og oppsummering av hendelser
- Dokumentere rutiner for å ivareta informasjonssikkerhet og personvern for bruk av systemet.

RISIKOSTYRING

- Bidra i kartlegging og verdivurdering av informasjon som systemet behandler.
- Bidra i vurdering og dokumentering av personvernkonsekvenser ved all behandling av personopplysninger i systemet.
- Sørg for at akseptabel risiko til enhver tid opprettholdes for systemet
- Sørg for at personvern og informasjonssikkerhet ivaretas i avtaler med leverandører av applikasjoner, forvaltning og drift, herunder etablering av databehandleravtaler.
- Gjennomføre risikovurderinger ved anskaffelse, ved vesentlige endringer og jevnlig gjennom systemets levetid.
- Planlegge og implementere risikoreduserende tiltak som sikrer at informasjonssikkerhet og personvern blir overholdt ved anskaffelse, endring og drift.
- Gjennomføre gjennomganger, tester og revisjoner av informasjonssikkerhet og personvern i systemet.
- Sørg for iverksetting av oppdateringer eller endringer som er nødvendige for å opprettholde informasjonssikkerheten og ivaretagelsen av personvern i systemet.
- Dokumentere og jevnlig rapportere restrisiko til systemeier, inkludert informasjon om sårbarheter, krav og endringer på informasjonssikkerhet og personvern.
- Sørg for at risikostyring omfatter hele leverandørkjeden.

KOMPETANSE

- Tilby opplæring innen informasjonssikkerhet og personvern for trygg og forsvarlig bruk av systemet.

INTERNKONTROLL OG LEVERANDØRKONTROLL

- Gjennomføre internkontrolltiltak på regelmessig basis av egen drift og forvaltning for systemet
- Gjennomføre kontroll av tilganger for privilegerte brukere og andre brukere i forvaltningen, og legge til rette for kontroll av brukertilganger i virksomheter som bruker systemet
- Følge opp avtaler med interne og eksterne leverandører og jevnlig påse at de oppfyller kravene til informasjonssikkerhet og personvern.

INNEBYGD PERSONVERN

- Sørg for at systemet oppfyller aktuelle krav til innebygd personvern.

TILGANGSSTYRING

- Sørg for at retningslinjer for tilgang til systemet er beskrevet for alle tilgangsnivåer.
- Sørg for at systemet har funksjonalitet for ledes kontroll av ansattes tilganger, inkludert brukere med privilegerte rettigheter.
- Beskrive krav til utforming og gjennomføring av autorisasjonsprosessen og andre tiltak som skal sikre at tilgang kun gis i tråd med tjenstlig behov.

HENDELSER OG AVVIK

- Utføre etablerte rutiner for å kunne oppdage hendelser og avvik på informasjonssikkerhets- og personvernområdet.
- Rapportere alvorlige hendelser og avvik iht. interne rutiner til systemeier.
- Håndtere avvik og informasjonssikkerhets- og personvernhendelser.
- Iverksette tiltak for å redusere konsekvenser av hendelser og avvik og sannsynligheten for at disse inntreffer igjen.
- Informere om status på avvik og hendelser til brukere av systemet.

BEREDSKAP

- Utarbeide nødvendige beredskapsplaner og -løsninger for systemet som ivaretar informasjonssikkerhet og personvern.
- Gjennomføre beredskapsøvelser både internt og i samarbeid med interne og eksterne leverandører.