



Oslo

Systemeier

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

Systemeier skal sørge for at systemet etterlever relevante lovkrav og kommunens regelverk innen personvern og informasjonssikkerhet. Dette utføres gjennom en risikobasert tilnærming.

Systemeier skal holde oversikt over relevante lovkrav og definere krav til ivaretagelse av informasjonssikkerhet og personvern for etterlevelse gjennom hele systemets levetid.

Systemeier har ansvar for å sikre at informasjonssikkerhet og personvern blir fulgt opp i systemforvaltningen. Systemeier kan inngå avtale med en systemforvalter om delegering av slike oppgaver. Systemeier plikter å følge opp Systemforvalters etterlevelse av avtalen.

Systemeier skal stille krav om og påse at innebygd personvern og informasjonssikkerhet blir ivaretatt i systemet. Systemeier skal legge til rette for gode tekniske funksjoner og rutiner for internkontroll der systemet brukes og forvaltes.

Systemeier skal rapportere etterlevelse av krav til informasjonssikkerhet og personvern til sin virksomhetsleder.

PLANLEGGE OG DOKUMENTERE

- Utarbeide årsplan for ivaretagelse av personvern og informasjonssikkerhet for systemet
- Dokumentere tilstand på personvern og informasjonssikkerhet for virksomhetsleder, gjennom løpende risikostyring og oppsummering av hendelser.
- Dokumentere rutiner for å ivareta informasjonssikkerhet og personvern for bruk av systemet, og gjøre dette kjent for virksomhetsleder. Dette gjelder også dersom systemet skal benyttes i andre virksomheter.
- Delegering av oppgaver til systemforvalter skal dokumenteres og skal følge kommunens *Mal for forvaltningsavtale*.

RISIKOSTYRING

- Kartlegge og verdivurdere informasjon som systemet behandler.
- Vurdere og dokumentere personvernkonsekvenser ved all behandling av personopplysninger i systemet.
- Sikre at personvern og informasjonssikkerhet ivaretas i avtaler med leverandører av applikasjoner, forvaltning og drift, herunder etablering av databehandleravtaler.
- Gjennomføre risikovurderinger ved anskaffelse, videreutvikling og gjennom systemets levetid.
- Sørge for innebygget informasjonssikkerhet i systemet
- Ta stilling til om systemets risiko er akseptabel.
- Beslutte og følge opp risikoreduserende tiltak som er nødvendige for å oppnå akseptabel risiko.
- Jevnlig rapportere restrisiko til virksomhetsleder.

KOMPETANSE

- Tilrettelegge for nødvendig opplæring innen informasjonssikkerhet og personvern for alle brukere av systemet.

INTERNKONTROLL

- Gjennomføre periodiske gjennomganger, tester og revisjoner av informasjonssikkerhet og personvern av systemet.
- Påse at kontroll av brukertilganger gjennomføres i virksomheten eller virksomhetene som bruker systemet.
- Gjennomføre kontroll av interne og eksterne leverandørers arbeid med informasjonssikkerhet og personvern og tilhørende avtaler.

INNEBYGD PERSONVERN

- Sikre at systemet oppfyller aktuelle krav til innebygd personvern.

TILGANGSSTYRING

- Sikre at retningslinjer for tilgang til systemet er beskrevet for alle tilgangsnivåer.
- Sikre at systemet har funksjonalitet for lederes kontroll av ansattes tilganger inkludert brukere med privilegerte rettigheter.

HENDELSER OG AVVIK

- Etablere rutiner for å kunne oppdage, håndtere og rapportere hendelser og avvik på informasjonssikkerhet- og personvernområdet.
- Håndtere hendelser og avvik på informasjonssikkerhets- og personvernområdet.
- Iverksette tiltak for å redusere konsekvenser av hendelser og avvik og sannsynligheten for at disse inntreffer igjen.
- Rapportere alvorlige hendelser og avvik iht. til interne rutiner.

BEREDSKAP

- Inkludere informasjonssikkerhet og personvern for systemet i beredskapsplaner og øvelser.
- Påse at leverandører har beredskapsplaner og at øvelser gjennomføres både hos leverandør og i samarbeid med leverandør