Oslo

Virksomhetsleder

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

Virksomhetsleder skal gjennom aktiv risikostyring ivareta informasjonssikkerhet, personvern og internkontroll i egen virksomhet i henhold til personopplysningsloven, sikkerhetsloven, annen lovgivning og kommunens eget regelverk. Styringssystemet som understøtter risikostyringen skal holdes oppdatert for å ivareta de til enhver tid gjeldende myndighetskrav innenfor taushetsplikt, personvern og informasjonssikkerhet. Virksomhetsleder skal godkjenne styrende dokumenter i styringssystemet for informasjonssikkerhet og personvern.

Virksomhetsleder kan delegere myndighet til å utføre informasjonssikkerhets- og personvernoppgaver til en eller flere ledere eller ansatte. Der virksomheten har et systemeieransvar, bør virksomhetsleder utpeke en systemeier som ivaretar oppgavene.

Virksomhetsleder skal sette av tilstrekkelige ressurser til arbeidet med informasjonssikkerhet og personvern og godkjenne organiseringen av arbeidet. Ressursene skal inneha rett kompetanse for arbeidet.

Virksomhetsleder skal måle etterlevelse av krav til informasjonssikkerhet og personvern, og gjennomføre ledelsens gjennomgang på regelmessig basis, minimum årlig.

Versjon 2.0

Virksomhetsleder

skal sørge for at følgende oppgaver løses:

Oslo

PLANLEGGE
- Årsplan for informasjonssikkerhets- og personvernaktiviteter blir utarbeidet
- Årlig rapportere fra ledelsens gjennomgang, virksomhetsleders egenerklæring og en oppsummering av hendelser og avvik til overordnet byrådsavdeling.

RISIKOSTYRING
- Definere og vedlikeholde akseptabelt risikonivå innenfor rammene gitt av overordnet byrådsavdeling.
- Kartlegge og verdivurdere all informasjon som virksomheten behandler.
- Utfylle og vedlikeholde behandlingsoversikt for personopplysninger.
- Inngå og vedlikeholde databehandleravtaler med leverandører.
- Gjennomføre personvernkonsekvensvurdering ved behandling av personopplysninger.
- Jevnlig gjennomføre risikovurderinger av informasjonsbehandlingsprosesser og av egne systemer i virksomheten.
- Gjennomføre risikovurderinger ved bruk av leverandører, både vurderinger av leverandørens tilnærming til risikostyring og vurdering av deres løsninger under hele kontraktsperioden.
- Iverksette nødvendige tiltak og/eller fremlegge restrisiko ut over akseptabelt risikonivå for overordnet byrådsavdeling.
- Overholde sikkerhetskrav og -rutiner ved bruk av fellessystemer, sektorsystemer og infrastruktur.

RESSURSER OG KOMPETANSE
- Sikre nødvendig kapasitet og kompetanse for informasjonssikkerhet og personvern for å ivareta oppgavene.
- Gjennomføre tilstrekkelig opplæring av alle ansatte innenfor informasjonssikkerhet og personvern.

SIKKERHETSREVISJON OG INTERNKONTROLL
- Gjennomføre sikkerhetsrevisjon for å måle virksomhetens etterlevelse av styringssystemets krav til informasjonssikkerhet og personvern, samt styringssystemets effektivitet i virksomheten.
- Jevnlig kontrollere at ansattes og annet personells tilganger er i tråd med tjenstlig behov.
- Gjennomføre kontroll av leverandørers arbeid med informasjonssikkerhet og personvern

TILGANGSSTYRING OG PERSONELLSIKKERHET
- Autorisere ansattes tilgang til IKT-systemer i henhold til tjenstlig behov og gjeldende retningslinjer for det enkelte system.
- Ivareta informasjonssikkerhet og personvern ved ansettelser, fratredelser og endringer av arbeidsforhold.
- Sikre at nødvendige taushetserklæringer blir signert (f.eks. egne ansatte, innleide og leverandører).

FYSISK SIKRING
- Sikre at uautoriserte ikke får adgang til beskyttelsesverdig informasjon, IKT-utstyr og infrastruktur.
- Ivareta adgangskontroll til virksomhetens lokaler.

HENDELSER OG AVVIK
- Etablere rutiner for å oppdage, håndtere og rapportere hendelser og avvik på personvern og informasjonssikkerhet.
- Varsle alvorlige hendelser og avvik til driftsleverandør og overordnet byrådsavdeling, samt kommunens personvernombud.
- Varsle Datatilsynet og andre tilsynsmyndigheter i henhold til relevante lover og forskrifter.

BEREDSKAP
- Inkludere informasjonssikkerhet og personvern i virksomhetens beredskapsplaner og øvelser.