# Vedlegg

## 3.1 Eksempler på sikkerhetsansvar, -roller og oppgaver

Eksemplene under er basert på virksomheter i sektoren, og gir en oversikt over mulige roller og ansvarsområder. Eksemplene er ment til inspirasjon slik at ansvarsområder blir vurdert og ansvaret plassert. Matrisene må tilpasses lokale forhold og utvides med relevante roller for akkurat din virksomhet, for eksempel med personvernrådgiver, forsker, prosjektleder og/eller systemkoordinator.

|  |
| --- |
| **Eksempel 1 på sikkerhetsansvar, -roller og -oppgaver internt i virksomheten****Matrisen må tilpasses lokale forhold****<Virksomhet>** |
| **Funksjon:** | **Virksomhetens leder** | **Leder** | **Ansatt/medarbeider** | **Fagansvarlig IKT** |  **Fagansvarlig sikkerhet**  | **Systemeier** |
| **Ansvar** | * Sørge for at det er etablert et styringssystem for informasjonssikkerhet og at dette vedlikeholdes
* Sørge for at informasjonssikkerheten er tilfredsstillende
* Bestemme formålet med behandlingen av personopplysninger
* Bestemme hvilke hjelpemidler som skal brukes
 | * Sørge for opplæring av ansatte
* Beredskap
* Tildele, vedlikeholde og inndra roller/ tilgang
* Rapportere avvik i samsvar med virksomhetens prosedyrer for dette
* Følge opp forskningsprosjekt
 | * Gjøre seg kjent med og følge lover, regler og prosedyrer
* Melde avvik
 | * Sørge for at informasjonssystemet er tilgjengelig
* Sørge for at informasjonssystemet oppfyller Normens krav
* Sørge for at informasjonssystemet fungerer som besluttet
* Etablere ansvarskart for informasjonssystemet
 | * Overvåke at informasjonssystemet benyttes i samsvar med bestemmelser og prosedyrer
* Rapportere til dataansvarlig
 | * Sørge for at sitt informasjonssystem er tilgjengelig
* Sørge for at sitt informasjonssystem oppfyller Normens krav
* Sørge for at informasjonssystemet fungerer som besluttet
* Definere tilgangsroller
* Rapportere til IKT-ansvarlig
 |
| **Rolle** | *Dataansvarlig* | *Leder med personalansvar* | *Systembruker* | *Bestiller* | *Fagansvarlig informasjonssikkerhet* | *Systemeier for et system* |
| **Oppgaver** | * Vedta, implementere, vedlikeholde og følge opp bruken av styringssystem for informasjonssikkerhet
* Gjennomføre ledelsens gjennomgang
* Melde brudd på personopplysnings-sikkerheten til Datatilsynet
 | * Sørge for at det gis opplæring i nødvendige systemer og i informasjonssikkerhet
* Lage og teste beredskapsprosedyrer for systemsvikt
* Sørge for risikovurderinger og overvåke risiko
* Tildele den enkelte medarbeider korrekt rolle og bestille tilgang til nettverk og system
* Vedlikeholde medarbeidernes tilgangsnivå
* Inndra tilgang ved opphør av arbeidsforhold
* Sørge for at forskningsprosjekt blir meldt til den regionale etiske komité (REK)
* Følge opp at forskningsprosjekt følger plan
* Behandle avvik
* Etablere og følge opp tilganger og evt. avtaler om tilgang på tvers
 | * Lese og følge gjeldende regler
* Gjøre seg kjent med styringssystem for informasjonssikkerhet
 | * Utarbeide og vedlikeholde prosedyrer rundt egen funksjon
* Utarbeide og inngå serviceavtale om drift og vedlikehold av informasjonssystemet
* Utarbeide beredskapsplan
* Ivareta konfigurasjonskontroll ved endringer av informasjonssystemet
* Sørge for risikovurderinger og overvåke risiko
* Vurdere eventuell løsning for fjernaksess opp mot veileder for fjernaksess
* Følge opp partnere, leverandør og databehandlere i forhold til informasjonssikkerhet
* Håndtere meldte avvik
* Rådgiving
* Sørge for at det blir utpekt systemeier for det enkelte system og holde oversikt over disse
 | * Utarbeide og vedlikeholde prosedyrer rundt egen funksjon
* Utforming av styrende, utførende og kontrollerende dokument i styringssystemet for informasjonssikkerhet
* Forberede ledelsens gjennomgang
* Følge opp iverksetting av tiltak som er besluttet gjennomført
* Samordne og gjennomføre sikkerhetsrevisjoner
* Vurdere rapporterte avvik
* Forestå risikovurderinger
* Godkjenne dokument til styringssystemet for informasjonssikkerhet
* Erverve og vedlikeholde kunnskap om trusler, sårbarhet, sikkerhetstiltak og -teknikker, sikkerhetskrav
* Opplæring
* Rådgiving
 | * Utarbeide og vedlikeholde prosedyrer rundt egen funksjon
* Bistå IKT-ansvarlig i å utarbeide vedlegg til serviceavtale
* Bistå IKT-ansvarlig i å utarbeide avtaler om endringer av sitt systems konfigurasjon
* Definere tilgangsroller for sitt system og gjøre disse kjent
* Sørge for risikovurderinger og overvåke risiko
* Følge opp partnere, leverandør og databehandlere i forhold til informasjonssikkerhet
* Håndtere meldte avvik
* Følge opp tilgang på tvers
 |