# Organisering

## Organisasjonskart

*<Eksempel. Fylles ut med eget organisasjonskart>*

<Daglig leder>

<Personvernombud>

<Sikkerhetsansvarlig>

<Administrasjon>

<Utviklingsansvarlig>

<IKT-ansvarlig>

## Sikkerhetsorganisasjon

*<Fylles ut med sikkerhetsrelaterte roller samt eventuell beskrivelse av oppgaver/ansvarsområder for avdelinger. Nedenfor er eksempler på roller og ansvar. >*

## Daglig leder

Daglig leder har det overordnede ansvaret for sikkerhet og behandling av personopplysninger i *<virksomhet>*, og for at vi etterlever kravene i personopplysningsloven *<og evt. andre regelverk>*

### Sikkerhetsansvarlig

Den sikkerhetsansvarlige er delegert ansvar for og myndighet til å implementere informasjonssikkerhet og internkontroll i samsvar med det som fremgår av dette internkontrollsystemet. Den sikkerhetsansvarlige rapporterer til daglig leder, og skal holde leder informert om alle spørsmål som har betydning for informasjonssikkerheten.

Sikkerhetsansvarliges ansvarsområder er definert i egen stillingsinstruks og i dette dokumentet:

* Utarbeide og vedlikeholde virksomhetens internkontrollsystem.
* Ansvarlig for vedlikehold av dokumentet *<Oversikt over behandlinger / Protokoll over behandlingsaktiviteter>*.
* Se til at de gjeldende sikkerhetsbestemmelser, instrukser og rutiner blir fulgt.
* Ansvar for at kontrollerende aktiviteter blir gjennomført.
* Gi beskjed om mislighold muntlig eller skriftlig, avhengig av misligholdets karakter.
* Sørge for at alle ansatte har kjennskap til internkontrollsystemet og tilhørende sikkerhetsbestemmelser, instrukser og rutiner.
* Ha samtaler om informasjonssikkerheten ved ansettelse og ved avslutning av et ansettelsesforhold.

### IKT-ansvarlig

Den IKT-ansvarlige har et selvstendig ansvar for å opprettholde *<virksomhet>s* informasjonssystem i samsvar med føringer som fremgår av internkontrollsystemet.

### Arkivleder

Arkivlederen har det daglige ansvaret for arkivarbeidet i *<virksomhet>*, herunder å ivareta den operative sikkerheten i virksomhetens fysiske og logiske arkiv.

### Webansvarlig

Den Webansvarlige har det daglige ansvaret for å vedlikeholde og utvikle *<virksomhet>s* elektroniske kommunikasjonskanaler, herunder å ivareta den operative sikkerheten i disse systemene.

### Ansvarlig for fysisk sikkerhet

I rollen ligger det daglige ansvaret for den fysiske sikkerheten i *<virksomhet>s* lokaler, herunder automatisk adgangskontroll og revisjon av tilganger.

## Andre roller

### Verdieier

Verdieier utpekes av ledelsen, og er hovedansvarlig for en konkret system-, personal eller informasjonsverdi. Verdieieren har det overordnede ansvaret for at det gjennomføres risikovurderinger, at risikoreduserende tiltak implementeres, gjennomføring av DPIA, oppdatering av dokumentasjon ol.

### Verdiadministrator/daglig ansvarlig

Verdiadministrator/daglig ansvarlig utfører oppgaver og tiltak, og har ansvar for implementering av beslutninger fattet av verdieier.

### Personvernombud

Hensikten med personvernombudet er å styrke virksomhetens evne til å etterleve regelverk for behandling av personopplysninger. Personvernombudets rolle og oppgaver følger av personvernforordningen artiklene 37, 38 og 39. Sentrale gjøremål er å gi råd i egen organisasjon og å følge med på vår egen etterlevelse av personvernregelverket og *<virksomhet>s* egne retningslinjer for behandling av personopplysninger. Ombudet har også en viktig funksjon som kontaktperson for de som virksomheten behandler personopplysninger om. Personvernombudet har taushetsplikt.

### Avdelingsdirektør

Avdelingsdirektør er ansvarlig for å bidra til at avdelingens medarbeidere behandler personopplysninger i henhold til *<virksomhet>s* internkontrollsystem.

Den enkelte medarbeider skal være kjent med virksomhetens internkontrollsystem og følge de rutiner og instrukser som er relevante for stillingen. Plikten skal gjøres kjent for den enkelte medarbeider av nærmeste leder.

### Den enkelte medarbeider

Den enkelte medarbeider har et selvstendig ansvar for å gjøre seg kjent med instrukser som gjelder for informasjonssikkerhet.

*<Virksomhet>s* medarbeidere med tjenstlig tilgang til informasjonssystemet skal kjenne hvilket ansvar og plikter de har. Alle medarbeidere skal være informert om den taushetsplikt som gjelder for hver enkelt og skal underskrive egen taushetserklæring. Alle medarbeidere skal ha tilstrekkelig kunnskaper om bruk av informasjonssystemet.

Den enkelte medarbeider har plikt til å melde brudd på instrukser for informasjonssikkerhet til den sikkerhetsansvarlige. Dette skjer i henhold til egen rutine i internkontrollsystemet.

## Krisestab

Krisestab skal settes når det har skjedd en alvorlig situasjon, eller når det er stor sannsynlighet for at det kan skje. Dette kan være en alvorlig situasjon for *<virksomhet>* som virksomhet, eller andre beredskapshendelser som krever ekstraordinær handling.

I første rekke er det daglig leder som setter krisestab, dernest avdelingsdirektører.

*Eksempel:*

I *<virksomhet>* er disse i krisestaben:

* Daglig leder NN
* Avdelingsdirektør NN
* Avdelingsdirektør NN
* Økonomiansvarlig NN
* Sikkerhetsansvarlig NN

## Kompetanse

### Internkontrollen skal følges

Alle har plikt til å holde seg oppdatert på *<virksomhet>s* internkontroll, og følge rutinen i sitt daglige arbeide. Internkontrollen er en del av arbeidsgivers instruksjon til arbeidstakeren, og skal følges.

### Grunnopplæring

Nærmeste leder skal ved ansettelse sørge for at det gis en grunnopplæring i internkontrollsystemet, og at medarbeideren bekrefter at internkontrollen er gjennomgått og forstått. At dette er gjennomgått skal fremgå av sjekklisten for nyansettelser, og returneres administrasjonen etter fullført.

### Årlig gjennomgang

Den sikkerhetsansvarlige skal årlig følge opp at den enkelte medarbeider er kjent med internkontrollen, og om nødvendig sørge for at den blir gjennomgått. Den sikkerhetsansvarlige skal også føre en oversikt som viser at en slik gjennomgang er foretatt i samsvar med fastsatt frist. Av oversikten skal det fremgå hvilke enkeltansatte som har fått informasjon.

Dersom det etter purring ikke lar seg gjøre å ha en gjennomgang med den ansatte, skal brukerkontoer stenges. Avdelingsdirektør og nærmeste leder skal varsles om slik stenging.

Den sikkerhetsansvarlige arkiverer årlige bekreftelser. Eventuell stenging av kontoer skal behandles som et avvik.