Målgrupper og temaer for opplæring

**Vi har her presentert eksempler på både målgrupper og tema som kan brukes som et utgangspunkt for identifisering av målgrupper og relevante opplæringstema i den enkelte virksomhet.**

Kompetanse- og kulturutvikling er en viktig brikke i styringen av informasjonssikkerhet. De ansatte må kjenne de styringsaktivitetene som er vesentlig for dem, og gis nødvendig opplæring. Hva som er vesentlig vil variere ut fra hvilken rolle man har i virksomheten. Digitaliseringsdirektoratets [kompetansebeskrivelser for roller i arbeidet med styring og kontroll av informasjonssikkerhet](https://www.digdir.no/informasjonssikkerhet/kompetansebeskrivelser-roller-innen-styring-og-kontroll-av-informasjonssikkerhet/1107) beskriver relevant kompetanse for ulike roller i sikkerhetsarbeidet. De kan også brukes når man identifiserer relevante temaer for opplæring.

**Toppleder/toppledergruppen**

* Hva er informasjonssikkerhet
* Internkontrollarbeid og sammenhengen mellom internkontroll og informasjonssikkerhet
* Ledelsens ansvar for informasjonssikkerhet
* Oversikt over styringsaktiviteter og hvem som bør ha ansvaret

**Risikoeiere (Linjeledere, operativt ansvarlig)**

* Tilsvarende som toppledergruppen, i tillegg
* Kunnskap om, eller forståelse for hovedelementene i
  + foranalyse av ansvarsområde
  + analyse av eksterne krav
  + taktisk oppdeling og gruppering
  + vurdere behov for risikovurderinger
  + planlegging og gjennomføring av risikovurdering
  + foreslå håndtering av risikoer
  + godkjenne forslag til risikohåndtering
  + iverksette godkjente sikkerhetstiltak
  + vurdere risiko etter hendelser
  + vurdering av risiko ved anskaffelser og utvikling

**Systemeier fellessystem**

* Tilsvarende som for risikoeiere, men litt mer operasjonelt på de ulike delene som involverer dem spesielt

**Prosessledere for risikovurderinger og risikohåndtering**

* Hva er risiko og risikovurderinger
* Risikovurderingene og risikohåndteringens plass i styringen av informasjonssikkerhet
* Metoden for risikovurdering
* Metoden for å foreslå håndtering av risikoer
* Hvordan tilpasse metoden til ulike situasjoner
* Håndteringsansvarlig sin rolle i aktiviteten Iverksette godkjente tiltak (evt. for egen målgruppe)

**Tiltaksleverandører (f.eks. IT-leder)**

* Hva er risiko og risikovurderinger
* Hva er risikohåndtering
* Etablere fellessikring og tydeliggjøre tilleggssikring
* Utforme og etablere sikkerhetstiltak
* Oppdatere fellessikringen
* Overvåking og hendelseshåndtering
* Måling av effekt av sikkerhetstiltak
* Sårbarhetsvurderinger

**Alle ansatte**

* Forståelse for hva informasjonssikkerhet er
* Kunnskap om:
  + Formål og mål for eget arbeid
  + Spesielle retningslinjer som gjelder alle i virksomheten, som:
    - Individuelt ansvar i forbindelse med informasjonssikkerhet
    - Krav ved generell bruk av IKT-utstyr
  + Krav til konfidensialitet, integritet og tilgjengelighet på informasjon i eget arbeid
  + Retningslinjer og rutiner som angår eget arbeid, som:
    - Beskrivelse av arbeidsprosesser, rutiner og eget ansvar
    - Beskrivelse av etablerte sikkerhetstiltak den enkelte må kjenne
    - Krav ved bruk av spesifikke informasjonssystemer
  + Rutiner for rapportering av informasjonssikkerhetshendelser
* Kunnskap om hvor de kan finne informasjon om:
  + Virksomhetens overordnede mål og strategi
  + Virksomhetens policy for informasjonssikkerhet
  + Retningslinjer som beskriver roller, ansvar og styringsaktiviteter
  + Hvor man finner retningslinjer og rutiner ved behov