Målgrupper og tema for opplæring

**Vi har her presentert døme på både målgrupper og tema som kan brukast som eit utgangspunkt for identifisering av målgrupper og relevante opplæringstema i den einskilde verksemd.**

Kompetanse- og kulturutvikling er ei viktig brikke i styringa av informasjonssikkerheit. Dei tilsette må kjenne dei styringsaktivitetane som er vesentlege for dei, og få naudsynt opplæring. Kva som er vesentleg vil variere ut frå kva rolle ein har i verksemda. Digitaliseringsdirektoratets [kompetansebeskrivingar for roller i arbeidet med styring og kontroll av informasjonssikkerheit](https://www.digdir.no/informasjonssikkerhet/kompetansebeskrivelser-roller-innen-styring-og-kontroll-av-informasjonssikkerhet/1107) beskriv relevant kompetanse for ulike rollar i sikkerheitsarbeidet. Dei kan også brukast når ein identifiserer relevante tema for opplæring.

**Toppleiar/toppleiargruppa**

* Kva er informasjonssikkerheit
* Internkontrollarbeid og samanhengen mellom internkontroll og informasjonssikkerheit
* Leiinga sitt ansvar for informasjonssikkerheit
* Oversikt over styringsaktivitetar og kven som bør ha ansvaret

**Risikoeigarar (Linjeleiarar, operativt ansvarleg)**

* Tilsvarande som toppleiargruppa, i tillegg
* Kunnskap om, eller forståing for hovudelementa i
  + foranalyse av ansvarsområde
  + analyse av eksterne krav
  + taktisk oppdeling og gruppering
  + vurdere behov for risikovurderingar
  + planlegging og gjennomføring av risikovurdering
  + føreslå handtering av risikoar
  + godkjenne forslag til risikohandtering
  + sette i verk godkjende sikkerheitstiltak
  + vurdere risiko etter hendingar
  + vurdering av risiko ved anskaffingar og utvikling

**Systemeigar fellessystem**

* Tilsvarande som for risikoeigarar, men litt meir operasjonelt på dei ulike delane som involverer dei spesielt

**Prosessleiarar for risikovurderingar og risikohandtering**

* Kva er risiko og risikovurderingar
* Risikovurderingane og risikohandteringa sin plass i styringa av informasjonssikkerheit
* Metoden for risikovurdering
* Metoden for å føreslå handtering av risikoar
* Korleis tilpasse metoden til ulike situasjonar
* Handteringsansvarleg si rolle i aktiviteten
* Sette i verk godkjende tiltak (evt. for eiga målgruppe)

**Tiltaksleverandørar (t.d. IT-leiar)**

* Kva er risiko og risikovurderingar
* Kva er risikohandtering
* Etablere fellessikring og tydeleggjere tilleggssikring
* Utforme og etablere tryggingstiltak
* Oppdatere fellessikringa
* Overvaking og hendingshandtering
* Måling av effekt av tryggingstiltak
* Sårbarheitsvurderingar

**Alle tilsette**

* Forståing for kva informasjonssikkerheit er
* Kunnskap om:
  + Føremål og mål for eige arbeid
  + Spesielle retningslinjer som gjeld alle i verksemda, som:
    - Individuelt ansvar i samband med informasjonssikkerheit
    - Krav ved generell bruk av IKT-utstyr
  + Krav til konfidensialitet, integritet og tilgjenge på informasjon i eige arbeid
  + Retningslinjer og rutinar som angår eige arbeid, som:
    - Beskriving av arbeidsprosessar, rutinar og eige ansvar
    - Beskriving av etablerte tryggingstiltak den einskilde må kjenne
    - Krav ved bruk av spesifikke informasjonssystem
  + Rutinar for rapportering av informasjonssikkerheitshendingar
* Kunnskap om kor dei kan finne informasjon om:
  + Verksemda sine overordna mål og strategi
  + Verksemda sin policy for informasjonssikkerheit
  + Retningslinjer som beskriv rollar, ansvar og styringsaktivitetar
  + Kor ein finn retningslinjer og rutinar ved behov