Digdir

digdir.no

Kompetanse- og kulturutvikling

Digdir i sikkerhetsmåneden

NIFS – 6.6.2023

Katrine Aam Svendsen

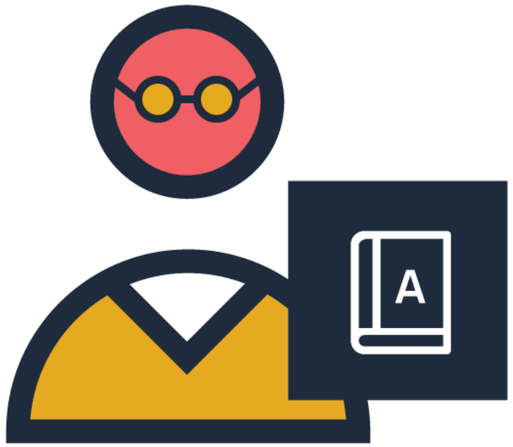
Jeg skal snakke om…

- Hjelpemidler til planlegging
- Hjelpemidler til gjennomføring
- Hvordan kan Digdir bistå?

En sikkerhetsmåned i endring…?

https://cybersecuritymonth.eu/

Kompetanse – en del av internkontrollen



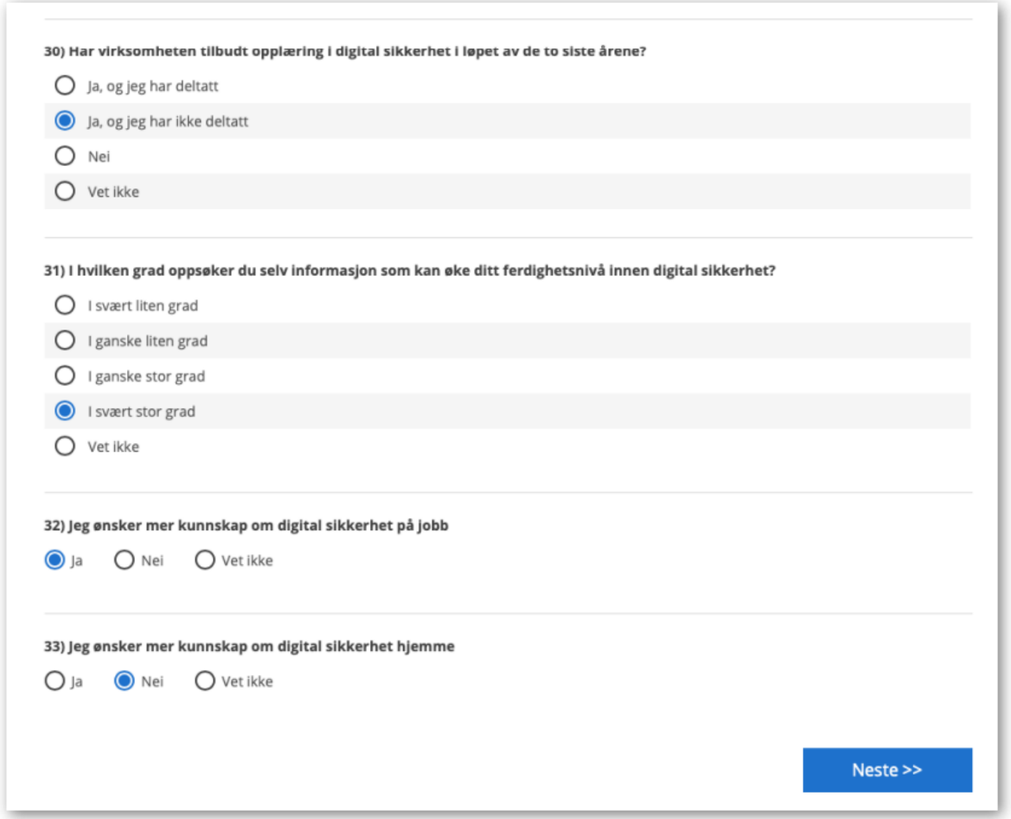
https://www.digdir.no/ik

Planlegging av sikkerhetsmåneden

Veileder for kartlegging av digital sikkerhetskultur

Når du skal gå i gang med å utvikle kompetanse og kultur innen digital sikkerhet i virksomheten, anbefaler vi at du starter med å kartlegge den digitale sikkerhetskulturen.

1. Avholde oppstartsmøte
2. Klargjøre spørsmålssettet
3. Informere om kartleggingen
4. Sende ut spørreundersøkelse
5. Purre
6. Sette sammen analyseteam
7. Analyse og syntese
8. Legge frem resultatene til ledelsen
9. Kommunisere resultatene til de ansatte



Figur 3 Eksempel spørsmål.

https://www.digdir.no/informasjonssikkerhet/veileder-kartlegging-av-digital-sikkerhetskultur/2142

Digdir

Kompetansebeskrivelser

- få oversikt over hvilken kompetanse dere har behov for
- legg en plan for strategisk kompetanseheving i virksomheten

- **Ansvar og oppgaver**: Hvilket ansvar og hvilke arbeidsoppgaver som kan ligge til rollen.
- **Ønsket kompetanse:** Hvilken kompetanse vedkommende bør ha for å utføre disse oppgavene.
- **Tema til intervju/medarbeidersamtale:** Aspekter man kan ha fokus på når man intervjuer nye kandidater, eller vurderer kompetansen til ansatte i virksomheten.

https://www.digdir.no/1107

Fagansvarlig informasjonssikkerhet >

Rådgiver informasjonssikkerhet >

Risikoeier

Toppleder

Øvrig ledergruppe

IT-leder

Systemeier

Alle ansatte

Rolle: Fagansvarlig informasjonssikkerhet

Fagansvarlig informasjonssikkerhet har som hovedansvar å være pådriver og støtte til ledelsen og organisasjonen for øvrig i informasjonssikkerhetsarbeidet.

Ansvar og oppgaver

Hvilken stilling den fagansvarlige har i virksomheten, vil variere avhengig av virksomhetens organisering og behov. Dersom fagansvarlig har en stilling som leder i virksomheten, vil oppgavene og ansvaret komme i tillegg til oppgaver og ansvar vedkommende har som følger stillingsbeskrivelsen.

Fagansvarlig informasjonssikkerhet skal bistå virksomhetsledelsen i utføringen av alle delaktivitetene under ledelsens styring og oppfølging.

I tillegg skal fagansvarlig informasjonssikkerhet være en nøkkelressurs i virksomhetens kontinuerlige internkontrollarbeid på informasjonssikkerhetsområdet, blant annet ved å bistå i arbeidet med risikovurdering og -håndtering, og måling, evaluering og revisjon. Fagansvarlig har ofte ansvaret for å planlegge og gjennomføre opplæring og bevisstgjøringsaktiviteter innen informasjonssikkerhet i virksomheten.

Ønsket kompetanse

Fagansvarlig informasjonssikkerhet er ikke en IKT-teknisk rolle. Den krever imidlertid god forståelse for IKT-relaterte risikoer, og andre typer informasjonssikkerhetsrisikoer. I tillegg må fagansvarlig informasjonssikkerhet ha god forståelse for

Målgrupper og 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

[Internkontrollveilederen - Målgrupper og temaer for opplæring (bokmål)]

Digdir

Veileder i kompetanse- og kulturutvikling innen digital sikkerhet

Denne veilederen omhandler arbeid med utvikling av kompetanse og kultur knyttet til digital sikkerhet. Vi anbefaler at du har startet med å kartlegge den digitale sikkerhetskulturen i virksomheten.

Innhold

https://www.digdir.no/informasjonssikkerhet/veileder-i-kompetanse-og-kulturutvikling-innen-digital-sikkerhet/2141

Gjennomføring av sikkerhetsmåneden

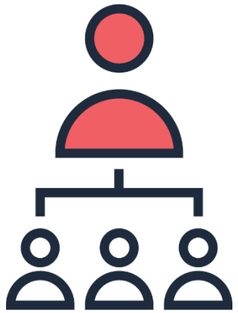
Dilemmatrening innen informasjonssikkerhet

Dilemmatrening er eit verktøy for kompetanse- og kulturutvikling. For å hjelpe verksemder med å auke kompetansen og utvikle kulturen innan informasjonssikkerheit, har vi utvikla ei dilemmatrening.

https://www.digdir.no/2057

Fire historier om styring av informasjonssikkerhet

Turid Topplеder



Linus Linjeleder

Fridtjof Fagansvarlig

Trine Tiltaksleverandør

https://www.digdir.no/informasjonssikkerhet/fire-historier-om-styring-av-informasjonssikkerhet/2647

Er det sikkert? Et e-læringskurs i informasjonssikkerhet for ledere

Dette e-læringskurset gir økt forståelse for leders ansvar for informasjonssikkerhet og hvorfor det lønner seg å ta informasjonssikkerhet på alvor. Kurset gir informasj
hva informasjonssikkerhet er og hvordan dere kan j
systematisk med informasjonssikkerhet. Kurset er la
toppledere, men egner seg også for ledere på alle ni

●●●●●○ (193)

Tema: Digitalisering og IKT | Difi

https://laeringsplattformen.difi.no/kurs/991825827/er-det-sikkert-et-e-laeringskurs-i-informasjonssikkerhet-ledere

Hvordan kan Digdir bistå?

Gjennomføring av dilemmatrening

Foredrag for ledergrupper

Presentasjoner for fagpersoner

Presentasjoner for ansatte

Svare på spørsmål

Støtte i bruk av veiledningsmateriellet

Hva ønsker dere?

infosikkerhet@digdir.no

https://www.digdir.no/infosikkerhet

digdir.no

Digitaliseringsdirektoratet

postmottak@digdir.no

22 45 10 00

Postboks 1382 Vika, 0114 Oslo

Besøksadresser:

Industriveien 1, 8900 Brønnøysund

Skrivarevegen 2, 6863 Leikanger

Grev Wedels Plass 9, 0151 Oslo