Digdir

digdir.no

Ledelsens gjennomgang

NIFS-møte 15. februar 2023

Fanny Bøhm-Pedersen, rådgiver

Innhold

- Hvorfor ledelsens gjennomgang?
- Innhold i Digdirs veiledningsmateriell «Internkontroll i praksis – informasjonssikkerhet»
  - Ledelsens styring og oppfølging -> Ledelsens gjennomgang
- Våre tilbud

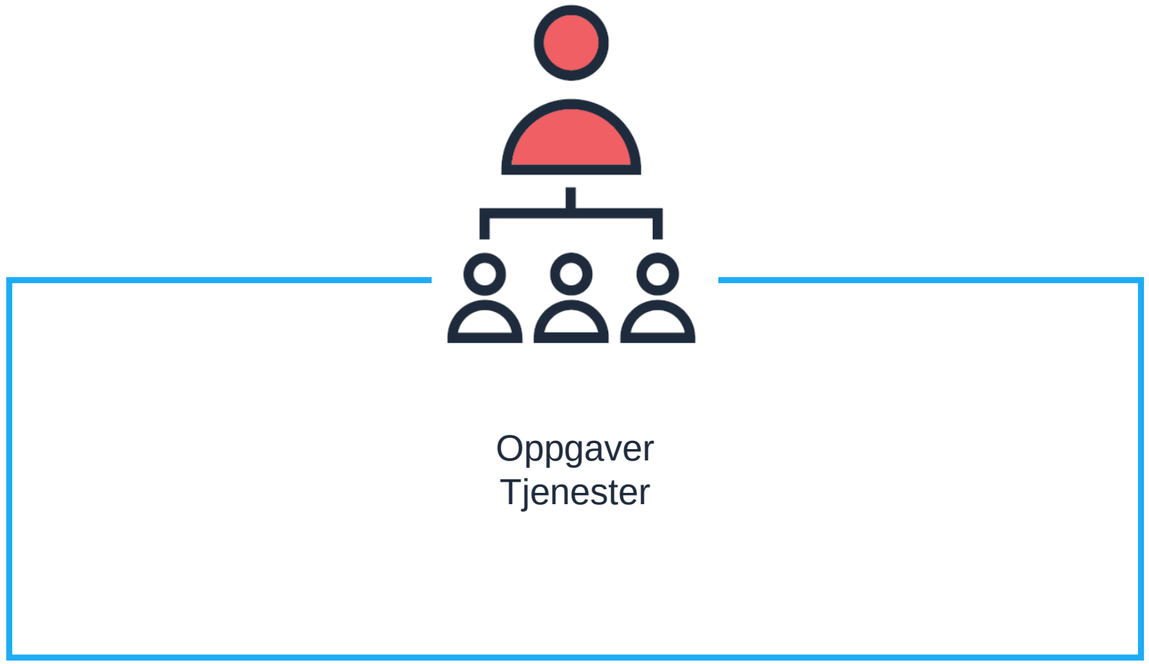
Hvorfor ledelsens gjennomgang?

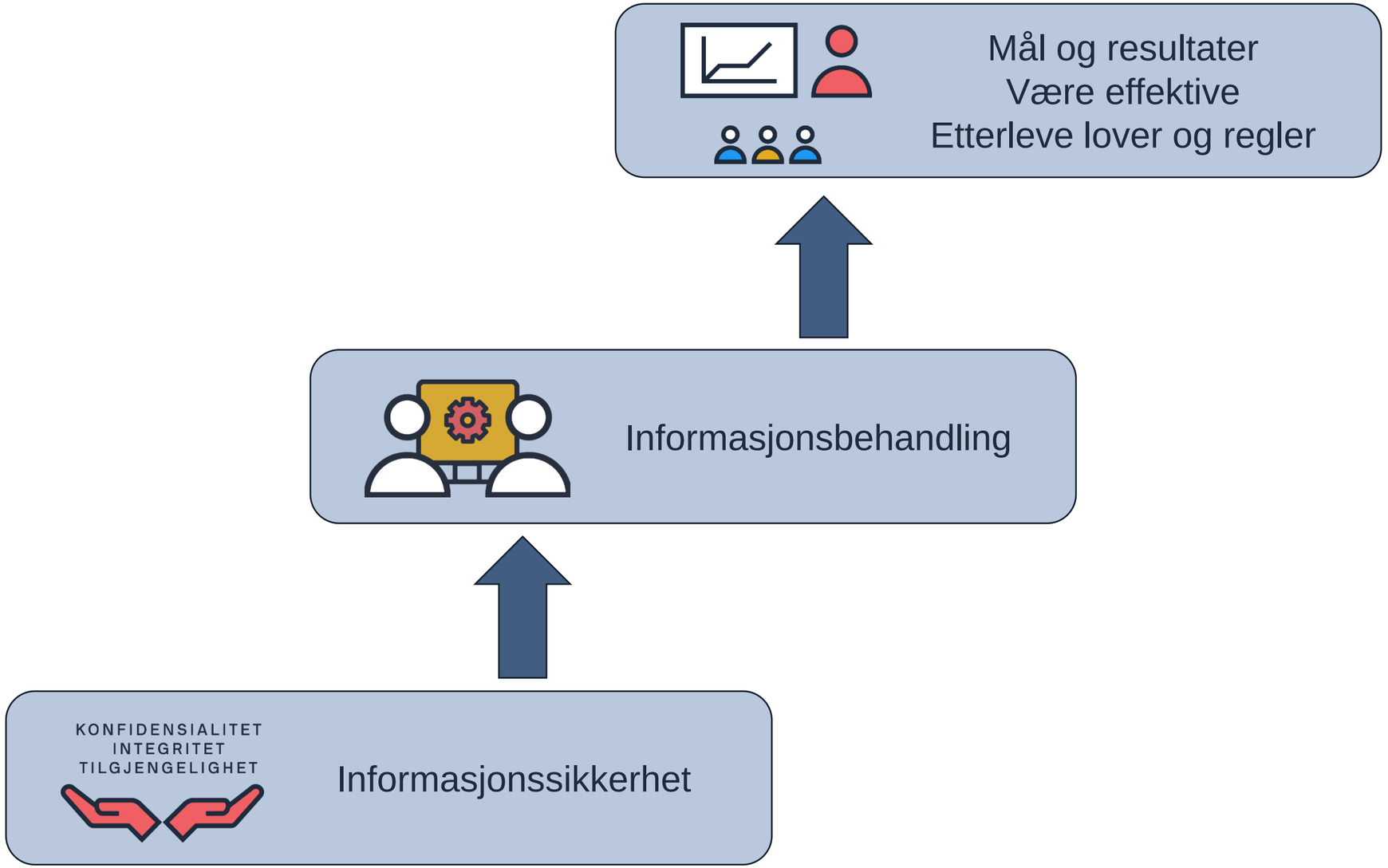
«Ledelsen» - Hvem mener vi?

- Virksomhetsledelsen
  - «Toppledelsen», «ledergruppa», etc.

- «Operative ledere»
  - Linjeledere
  - Ansvarlig for mål og resultater i sin enhet
  - Oppgaveeier/prosesseier → Risikoeier

Leder er ansvarlig for styringen av virksomheten




Mål og resultater
Være effektive
Etterleve lover og regler
Informasjonsbehandling
KONFIDENSIALITET
INTEGRITET
TILGJENGELIGHET
Informasjonssikkerhet

Krav til internkontroll / styring og kontroll

eForvaltningsforskriften § 15 andre ledd

Forvaltningsorganet skal ha en internkontroll (styring og kontroll) på informasjons-sikkerhetsområdet som baserer seg på anerkjente standarder for styringssystem for informasjonssikkerhet. Internkontrollen bør være en integrert del av virksomhetens helhetlige styringssystem. (…)

Kommuneloven § 25-1

Kommuner og fylkeskommuner skal ha internkontroll med administrasjonens virksomhet for å sikre at lover og forskrifter følges.

(...)

Internkontrollen skal være systematisk og tilpasses virksomhetens størrelse, egenart, aktiviteter og risikoforhold.

Bestemmelser om økonomistyring i staten

2.4 Internkontroll

Alle virksomheter skal etablere internkontroll. Virksomhetens ledelse har ansvaret for å påse at internkontrollen er tilpasset risiko og vesentlighet, at den fungerer på en tilfredsstillende måte og at den kan dokumenteres. Internkontroll skal primært være innebygd i virksomhetens interne styring

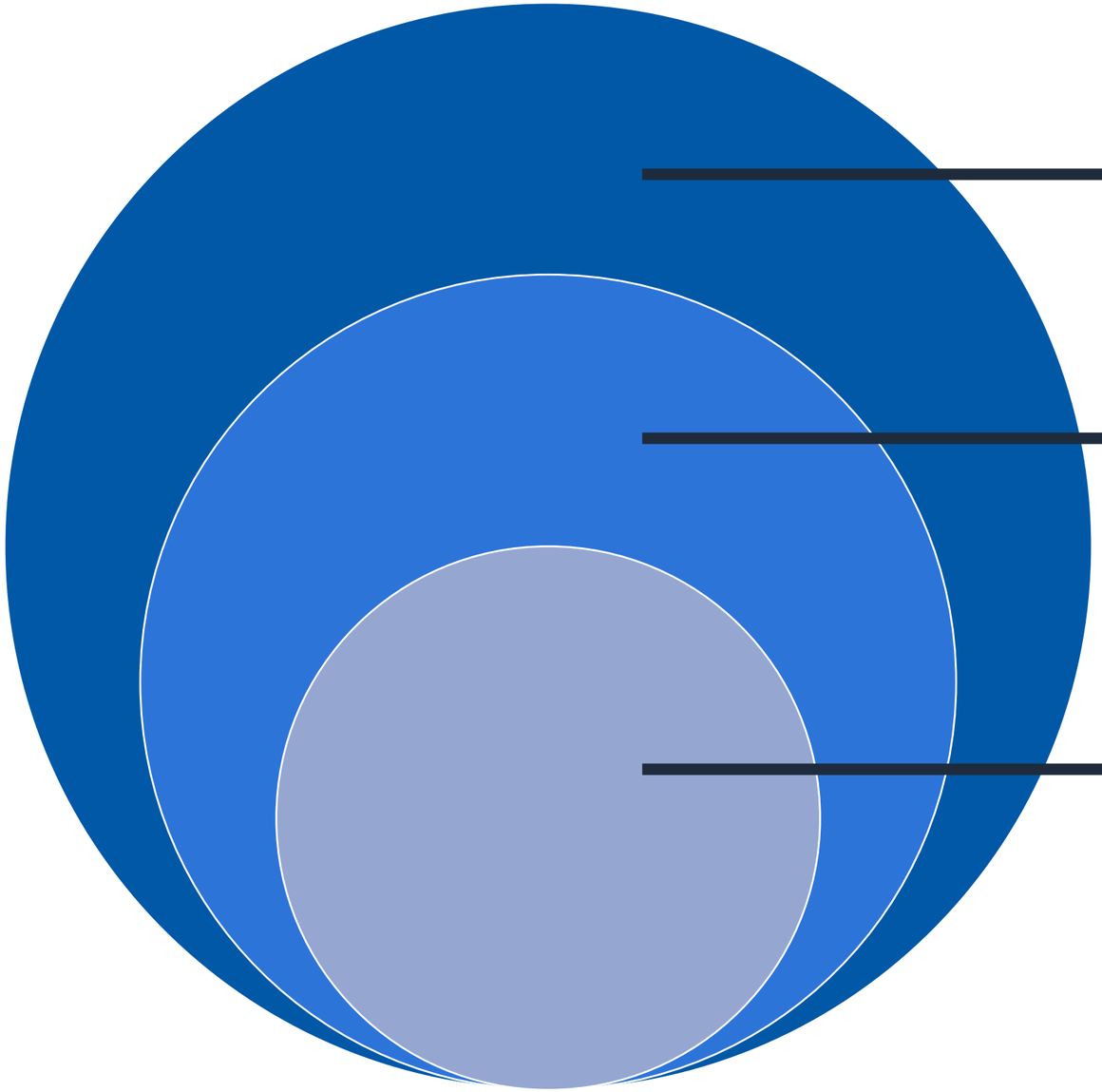
God internkontroll handler i stor grad om systematisk arbeid, god organisering og dokumentasjon, arbeidsmetoder og samhandling som kan forebygge lovbrudd og uønskede hendelser.

Orden i eget hus, KS

Standard og veiledningsmateriell

- ISO/IEC 27001
  - er den anbefalte anerkjente standarden å basere seg på
    - stiller overordnede krav

- Digdirs veiledningsmateriell «Internkontroll i praksis – informasjonssikkerhet»
  - baserer seg på ISO/IEC 27001
  - konkretiserer hvordan kravene kan implementeres og etterleves
  - anbefalt å bruke som referanse og støtte ved analyse av status, etablering og forbedring av internkontroll på informasjonssikkerhetsområdet



Overordnet virksomhetsstyring

Risikostyring i virksomheten

Styring og kontroll med informasjonssikkerhet i virksomheten

Hva kan skje når det går galt?

Vår egen jobb

- feil beslutninger
- brudd på rettssikkerhet
- feil i øk. transaksjoner
- ikke korrekt og forsvarlig saksbehandling
- økonomiske tap
- ineffektivt arbeid
- tapt arbeidstid
- …

Personer og virksomheter

- tap av anseelse, integritet og rettigheter
- økonomiske tap
- ødelagte muligheter, arbeidsforhold, livssituasjon
- bedriftshemmeligheter
- rikets sikkerhet
- liv og helse
- …

Digdir

digdir.no

Innhold i Digdirs veiledningsmateriell «Internkontroll i praksis – informasjonssikkerhet»

[Internkontroll i praksis - Informasjonssikkerhet | Digdir]

Ledelsens styring og oppfølging – «Hjernen»

Ledelsens styring og oppfølging

- Vurdering av risiko
- Håndtering av risiko
- Overvåking og hendelseshåndtering
- Måling, evaluering og revisjon
- Kompetanse- og kulturutvikling

Kommunikasjon

Ledelsens styring og oppfølging

- Ledelsens gjennomgang
  - Minimum en gang årlig

- Ledere på alle nivå
  - Delegere og følge opp gjennom linjen
  - Sikre finansielle rammer
  - Kommunisere viktighet
  - Løfte og håndtere problemstillinger gjennom linjen
  - Beredskap og krisehåndtering

Formålet med ledelsens gjennomgang

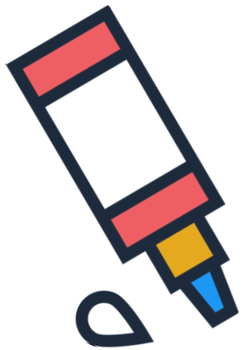
- Avklare status på virksomhetens arbeid med styring av informasjonssikkerhet
- Avklare status på områder og tjenester der virksomhetsledelsen er spesielt opptatt av informasjonssikkerheten
- Reagere og følge opp der det er nødvendig

Behovet for ledelsens gjennomgang varierer

- Omfang og innhold vil variere
- I en etableringsprosess er det større behov for tett kontakt med ledelsen
- Man vil over tid komme inn i en fast rutine og frekvens for virksomhetsledelsens gjennomgang

Underlag til virksomhetsledelsens gjennomgang

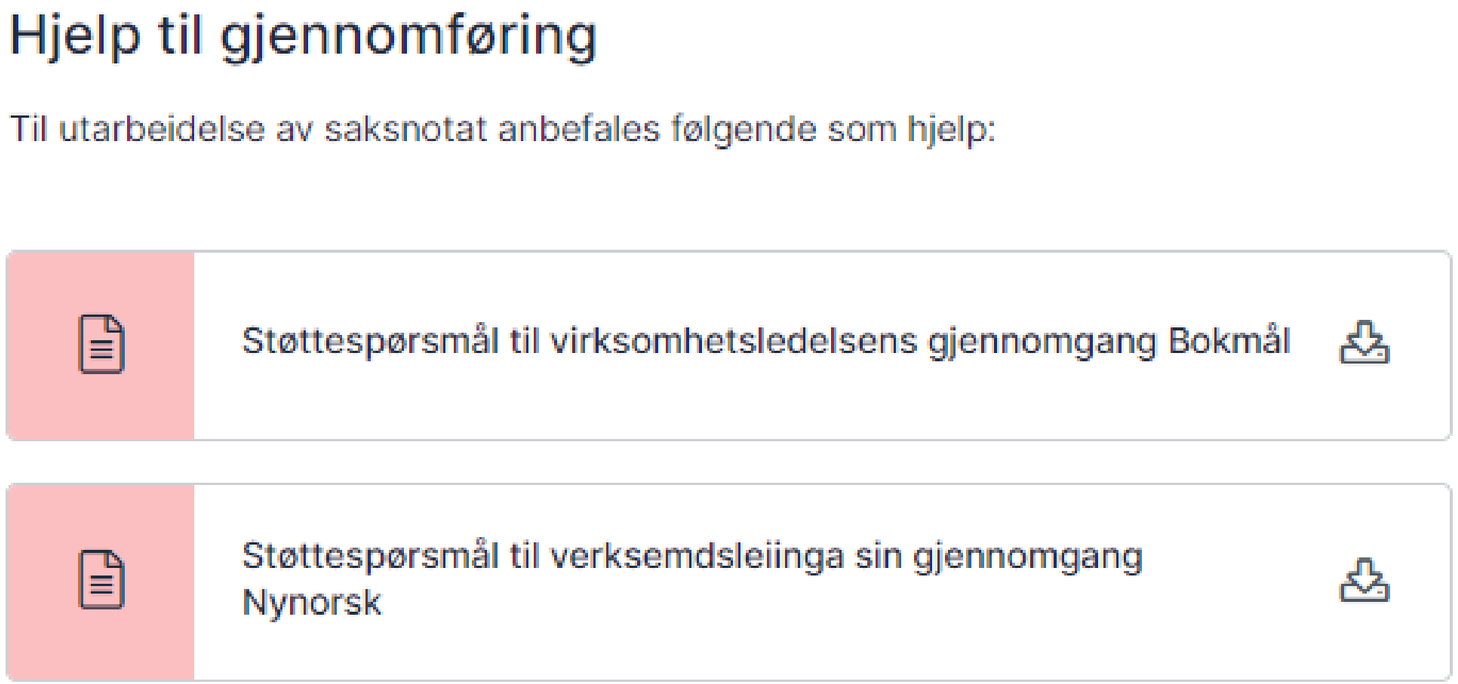
- Fagansvarlig informasjonssikkerhet bør utarbeide et saksnotat for møtet
  - Ledelsen trenger et godt beslutningsgrunnlag med tydelige og begrunnede anbefalinger
  - Gjennomførte styringsaktiviteter og etableringsaktiviteter er en viktig kilde
  - Innholdet vil variere over tid



Innholdet i gjennomgangen

- status på endringer og andre beslutninger fra forrige gjennomgang
- trender i risikobildet både for virksomheten, nasjonalt og internasjonalt
- omtale av særskilte risikoer eller risikoområder av strategisk betydning for virksomheten
- oppsummering av vesentlige avvik i informasjonssikkerheten og arbeidet med styring og kontroll
- vurdering av årsaker til vesentlige avvik
- vurdering av om det helhetlige arbeidet med styring og kontroll fungerer effektivt og gir ønskede resultater
- anbefalte tiltak for forbedring

Mer støtte til saksnotat på Digdir.no



https://www.digdir.no/informasjonssikkerhet/kommunikasjon/3045

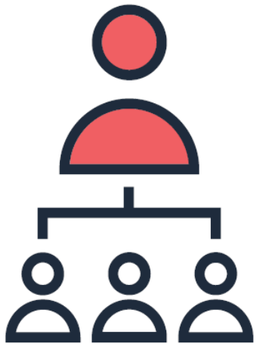
Styringssystem

- ~~Dokumenter~~
- ~~Noe en fagperson tar hånd om~~
- ~~Noe IT-avdelingen har kontroll på~~

- Aktiviteter 👍

~~Ledelsesforankring~~

Ledelsen styrer aktivt



- Ledelsens redskap for å ha styring og kontroll
- Kan ikke ha et «styringssystem» på siden, som noen andre har ansvaret for
- Ledelsen må ha faglig støtte til styringen
  - Eks: fagansvarlig informasjonssikkerhet

Våre tilbud

Digdir

Søk Meny

Hjem › Informasjonssikkerhet › Styring av informasjonssikkerhet › Internkontroll i praksis

Internkontroll i praksis - Informasjonssikkerhet

Internkontroll er leders redskap for å styre risiko på informasjonssikkerhetsområdet. Kjernen i internkontrollen er systematiske aktiviteter som gjennomføres av ledere med ansvar for virksomhetens oppgaver og tjenester.

NIFS

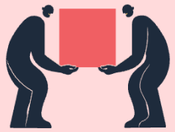
Digdir

Søk Meny

Hjem › Informasjonssikkerhet › Styring av informasjonssikkerhet › Helhetlig styring og kontroll

Helhetlig styring og kontroll av informasjonssikkerhet

For å sikre god styring og kontroll av informasjonssikkerhet må man jobbe helhetlig, og se informasjonssikkerhet som en del av virksomhetsstyringen. Her kan du lese om sammenhengen mellom virksomhetsstyring, informasjonssikkerhet, personvern og sikkerhetsstyring etter sikkerhetsloven.



Hva vil det si?

Å jobbe helhetlig betyr at man skal se sammenhengen mellom viktige områder og aktiviteter i virksomheten.

Hva er felles?

De samme grunnreglene gjelder uavhengig av hvilket fagområde man skal drive styring og kontroll på. Les mer om fellestrekkene her.

Hva er ulikt?

Helheten er ikke den samme for alle, og ulike perspektiver gir ulikt fokus. Les mer om noe av det som må tas hensyn til dersom man skal lykkes med å jobbe helhetlig.

Hvor får du hjelp?

Aktører som veileder innen styring og kontroll

DFØ, Digitaliseringsdirektoratet, KS, NSM og Datatilsynet har alle veiledning som er relevant når man jobber med ulike deler av informasjonssikkerhet.

→

Om denne veiledningen

Denne veiledningen er resultatet av et samarbeid mellom NSM, DFØ og Digitaliseringsdirektoratet. Datatilsynet og KS har også bidratt i arbeidet.

→

Digitaliseringsdirektoratet
Norwegian Digitalisation Agency

Kompetansebeskrivelser

Ansvar, oppgaver og ønsket kompetanse for roller knyttet til styring og kontroll av informasjonssikkerhet

Hjem › Informasjonssikkerhet › Kompetanse- og kulturutvikling

Kompetanse- og kulturutvikling innen informasjonssikkerhet

Her finner du veiledning som kan hjelpe deg når du skal arbeide med kompetanse og kultur innen informasjonssikkerhet i din virksomhet.

Kartlegging av digital sikkerhetskultur

Få veiledning om hvordan du kan kartlegge den digitale sikkerhetskulturen i din virksomhet.

Kompetanse- og kulturutvikling innen digital sikkerhet

Få veiledning om hvordan du kan arbeide med utvikling av kompetanse og kultur knyttet til digital sikkerhet.

Virkemidler

Kompetansebeskrivelser

Les om ansvar, arbeidsoppgaver og kompetansebehov for ulike roller innen styring og kontroll av informasjonssikkerhet.

→

Dilemmatrening innen informasjonssikkerhet

Bruk dilemmatrening for å arbeide med kultur og kompetanse.

→

E-læring for ledere

E-læringskurset "Er det sikkert" forteller om leders ansvar for informasjons-sikkerhet, og hvorfor det lønner seg å ta informasjonssikkerhet på alvor.

→

Hjem › Informasjonssikkerhet › Etterlevelse av fire sikkerhetsstandarder › Etablering av sikkerhetsstandardene

Etterlevelse av fire sikkerhetsstandarder

- Etablering av sikkerhetsstandardene
- Testing av etterlevelsen

Veileder for etablering

Her finner du formålet med hver av fire sikkerhetsrelaterte forvaltningsstandarder og hvordan de bør iverksettes på systemene hvor de skal brukes.

På denne siden

- Anbefalte standarder for sikker datakommunikasjon
  - HTTPS med HSTS
- Anbefalt standard for transportsikring av e-post

Digdir

Søk Meny

Hjem › Informasjonssikkerhet › Etterlevelse av fire sikkerhetsstandarder › Testing av etterlevelsen

Etterlevelse av fire sikkerhetsstandarder

- Etablering av sikkerhetsstandardene
- Testing av etterlevelsen

Veileder for testing av etterlevelse

Her beskriver vi hvordan du kan teste etterlevelse av fire sikkerhetsrelaterte forvaltningsstandarder anbefalt i Referansekatalogen for IT-standarder.

Digitaliseringsdirektoratets tilbud

- Internkontroll i praksis – informasjonssikkerhet
- Helhetlig styring og kontroll av informasjonssikkerhet
- Veiledere og virkemidler til kompetanse- og kulturutvikling innen informasjonssikkerhet
- Kompetansebeskrivelser for roller innen styring og kontroll av informasjonssikkerhet
- Dilemmatrening
- E-læringskurs «Er det sikkert?» på statens læringsplattform

Kontakt oss

Har du kommentarer, innspill eller spørsmål?

 infosikkerhet@digdir.no

 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