Difi
Direktoratet for
forvaltning og ikt

Veileder i kompetanse- og kulturutvikling innen informasjonssikkerhet

Denne veilederen tar for seg hvordan man kan bygge opp et helhetlig opplæringsprogram, og gir råd til hvordan man kan utvikle sikkerhetskulturen. Veiledningsmaterialet er utviklet for deg som arbeider med opplæring innen informasjonssikkerhet, uavhengig av tidligere erfaring. Dette er tredje versjon av veilederen.

Innholdsfortegnelse:

Direktoratet for
forvaltning og IKT (Difi)
infosikkerhet.difi.no
infosikkerhet@difi.no

1 Hva er kompetanse- og kulturutvikling?

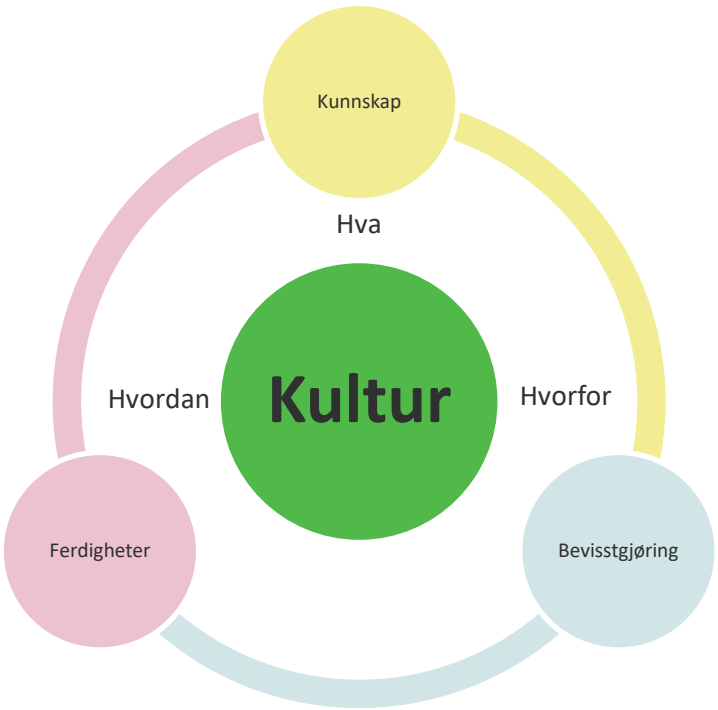
Alle virksomheter har mål de skal nå og oppgaver som skal utføres for å nå disse målene. For å kunne realisere målene, vil det være nødvendig å sikre at alle ansatte har tilstrekkelig kunnskap for å kunne utføre sine arbeidsoppgaver på en god måte. Dette inkluderer kunnskap om informasjonssikkerhet.

Den enkeltes kunnskap, adferd og holdninger er en del av organisasjonens kultur. Den enkeltes kunnskap, adferd og holdninger til informasjonssikkerhet vil være en del av dette – en del av virksomhetens sikkerhetskultur.

Kompetansen den enkelte har og virksomhetens organisasjonskultur vil utvikles kontinuerlig. Dette skjer naturlig i dialog og samhandling med andre. Samtidig vil det også være behov for konkrete tiltak for å heve kompetansen og utvikle organisasjonskulturen i riktig retning. For å sikre tilstrekkelig kompetanse, vil de fleste virksomheter ha behov for opplæringstiltak. Opplæring kan bidra til å

- heve kunnskapsnivået
- bevisstgjøre de ansatte
- trene ferdigheter
- utvikle organisasjonens kultur

Organisasjonens behov avgjør hva opplæringen bør fokusere på. Alle områdene dekkes ikke nødvendigvis av samme opplæringstiltak.



Figuren viser at organisasjonens kultur påvirkes av den enkeltes kunnskap, bevissthet og ferdigheter. Kunnskap viser til hva den enkelte kan, bevisstgjøring innebærer at man forstår hvorfor og ferdigheter innebærer at man vet hvordan. Sammen med de ansattes holdninger utgjør dette organisasjonens kultur.

Direktoratet for
forvaltning og IKT (Difi)
infosikkerhet.difi.no
infosikkerhet@difi.no

1.1 Kunnskap

Alle ansatte må ha tilstrekkelig kunnskap for å kunne utføre sine arbeidsoppgaver på en god måte. Dette inkluderer kunnskap om informasjonssikkerhet.

En utfordring er å identifisere hva den enkelte faktisk bør eller må vite. Behovet for kunnskap vil variere utfra den ansattes arbeidsoppgaver og rolle i organisasjonen. Det er noe kunnskap den enkelte bør ha under huden (taus kunnskap) og noe det holder å kunne slå opp ved behov.

1.2 Bevisstgjøring

Selv om man har kunnskap, betyr ikke det at den enkeltes adferd er i samsvar med kunnskapen. Det er ofte nødvendig med bevisstgjøring i tillegg.

Bevisstgjøring innebærer å bli klar over hvorfor man skal handle på en bestemt måte. Man går inn i retningslinjer, krav og rutiner for å forstå hvorfor de er som de er. Videre ser man på den enkeltes bidrag og betydning i etterlevelsen av krav, og hvilke konsekvenser det vil få dersom regler ikke blir fulgt. Bevisstgjøring er derfor viktig for å sikre etterlevelse av pålegg.

Bevisstgjøring er også viktig for å skape refleksjon. Denne refleksjonen fører til at ansatte tenker over hvilke deler av sikkerhetsarbeidet som fungerer etter hensikten, hvilke områder organisasjonen bør se nærmere på og hvor de eventuelt må endre praksis. Dette gjør at de ansatte forstår at de spiller en viktig rolle i utviklingen av organisasjonskulturen. Bevisstgjøring er derfor sentralt i arbeidet med utvikling av en god sikkerhetskultur.

1.3 Ferdigheter

Selv om en ansatt vet hva og hvorfor (kunnskap og bevisstgjøring) er det de praktiske handlingene, dvs. den enkeltes adferd, som avgjør resultatene. Det er derfor i de fleste sammenhenger viktig å trene på praktiske ferdigheter. Dette kan gjøres på mange måter, og omfanget av trening kan variere. Det kan være alt fra små øvelser hver enkelt kan gjøre i hverdagen, til større øvelser for hele seksjoner eller avdelinger.

Den enkelte virksomhet må vurdere hvilke ansatte som trenger ferdighetstrening på hvilke områder. For mer informasjon om hvordan opplæring kan gjennomføres i virksomheten, se kapittel 3.

1.4 Kulturutvikling

Alle virksomheter har en organisasjonskultur. Dette er et sett med «felles verdier, normer og virkelighetsoppfatninger som utvikler seg i en organisasjon når medlemmene samhandler med hverandre og omgivelsene».1 Organisasjonskultur er forenklet sagt en felles oppfatning i virksomheten - «slik gjør vi det hos oss».

Sikkerhetskulturen er en del av organisasjonskulturen, og handler derfor om hvilke verdier og normer som ligger til grunn for den enkeltes valg for håndtering av informasjon og systemer. Sikkerhetskultur er dermed den felles oppfattelsen i virksomheten som har positive eller negative konsekvenser for sikkerheten.

[1] Henning Bang, Organisasjonskultur, 3. utgave, 2011.

Direktoratet for
forvaltning og IKT (Difi)
infosikkerhet.difi.no
infosikkerhet@difi.no

Kjernen i utviklingen av en sikkerhetskultur er:

- Hva – vite hva en skal gjøre i ulike situasjoner
- Hvorfor – forstå hvorfor
- Hvordan – ha tilstrekkelige ferdigheter til å kunne handle deretter
- Holdning – ta risiko og sikkerhetskrav på alvor, og handle i samsvar med dem

Kulturutvikling er en kontinuerlig prosess. Ledere må ta stilling til om organisasjonen har en velfungerende sikkerhetskultur som skal opprettholdes og forsterkes, eller om det er behov for å endre på den eksisterende kulturen. Små feil, misforståelser og manglende kunnskap og ferdigheter kan korrigeres gjennom opplæring og veiledning, mens endring av kultur er en lengre og tyngre prosess. Endringer kan være nødvendig fordi kulturen ikke er god, eller fordi kravene til virksomheten har endret seg. Det kan også være subkulturer innen organisasjonen som det er nødvendig å ta tak i og utvikle, for å sørge for at organisasjonen har en enhetlig sikkerhetskultur. For at kulturen skal være velfungerende og la seg opprettholde, er det også viktig at rutiner og prosesser støtter opp under effektive samarbeidsformer, og ikke oppleves som en hindring i arbeidet.

I holdnings- og kulturutvikling er bevisstgjøring og refleksjon viktige redskap. Den enkelte må være bevisst hvorfor man skal handle på en viss måte, og så reflektere over egne valg og kravenes hensiktsmessighet. Refleksjonen må foregå både individuelt og kollektivt. Tillit er sentralt for å oppnå kollektiv refleksjon. Det må være lov å tenke høyt uten å ha alle svarene, og man må ha et miljø som verdsetter gode diskusjoner. Har man ikke dette, skapes ikke tilliten som er nødvendig for å utvikle organisasjonens kultur i riktig retning. Tillit er derfor avgjørende i arbeidet med å bygge en god sikkerhetskultur.

Målet er å ha en kultur der de ansatte utfører sine oppgaver i tråd med policyer og retningslinjer, og er bevisst hvorfor de skal handle som de gjør, reflekterer over egne valg, og diskuterer holdninger og adferd. Samtidig skal handlinger, refleksjon og dialog føre til at virksomheten endrer policyer og retningslinjer som ikke er hensiktsmessige. Slik videreutvikles adferd: alle går i samme retning samtidig som refleksjon og dialog fører til nødvendige endringer i virksomheten.

Husk:

- Kun ved å skape et miljø der man kan diskutere rammer, føringer og regler som ligger rundt oss, vil vi kunne skape en god sikkerhetskultur og utvikle organisasjonen videre på dette området. Det er derfor viktig å legge til rette for diskusjoner om sikkerhetsarbeid, krav, føringer etc.

- Sørg for at dere har en prosess for å håndtere alle sikkerhetshendelser og andre sikkerhetsrelaterte tilbakemeldinger som rapporteres fra ansatte. Uten oppfølging skapes det inntrykk av at regler og policyer ikke betyr noe og ikke behøver å følges, eller at tilbakemeldinger ikke tas alvorlig. Da utvikles en negativ sikkerhetskultur.

- Selv om virksomheten ikke har utfordringer med manglende kompetanse eller en dårlig sikkerhetskultur, er det nødvendig å arbeide kontinuerlig for å opprettholde eksisterende nivå.

Direktoratet for
forvaltning og IKT (Difi)
infosikkerhet.difi.no
infosikkerhet@difi.no

2 Hvorfor ha opplæring innen informasjonssikkerhet?

2.1 Ansvar for opplæring

Opplæring er et lederansvar. Det er ledelsen i en virksomhet som har ansvar for at informasjons-sikkerheten ivaretas. Dette innebærer bl.a. et ansvar for å sørge for at medarbeiderne har tilstrekkelig kunnskap om informasjonssikkerhet for å kunne utføre sine oppgaver. I praksis vil det daglige ansvaret for å utføre opplæringsaktiviteter være delegert nedover i virksomheten, og innen informasjonssikkerhet er det gjerne sikkerhetsansvarlig som får ansvaret for å sette i verk opplæringsaktiviteter. Uavhengig av hvem som utfører de daglige aktivitetene er det til syvende og sist ledelsen som er ansvarlig for at informasjonssikkerhet ivaretas i egen organisasjon.

Husk:

- Ledelsen må forstå hvorfor det er viktig å ha opplæring innen informasjonssikkerhet, og støtte opp om opplæringstiltak.

2.2 Internkontroll (styringssystem) for informasjonssikkerhet

Alle offentlige virksomheter skal ha internkontroll for informasjonssikkerhet.[2] Internkontroll handler om å ha tilstrekkelig styring og kontroll slik at virksomheten kan nå sine mål på en kostnadseffektiv måte. Det er lederens ansvar å sørge for at dette er på plass.

Kompetanse- og kulturutvikling er en viktig brikke i internkontrollen. De ansatte må kjenne de aktivitetene i internkontrollen som er vesentlig for dem, og gis nødvendig opplæring. Hva som er vesentlig vil variere ut fra hvilken rolle man har i virksomheten. For eksempel:

- Ledelsen vil ha behov for kompetanse på hvordan internkontrollen fungerer, og hva deres ansvar er.
- De med sentrale roller i internkontroll-aktivitetene, for eksempel ledere på alle nivåer, har behov for grunnopplæring i hva som er deres ansvar, hvordan de kan organisere arbeidet, og hvor de kan få hjelp og støtte.
- De som har ansvaret for å lede gjennomføringen av risikovurderinger på ulike områder har behov for kompetanse på hvordan dette kan gjøres.
- Alle ansatte må ha forståelse for hva informasjonssikkerhet er, og hvilket ansvar de har i forbindelse med dette. I tillegg må de ha kunnskap om retningslinjer og rutiner som angår deres arbeid, og hvor de kan finne øvrig informasjon om internkontrollen.

Tilstrekkelig kompetanse og bevissthet om informasjonssikkerhet hjelper til å underbygge virksomhetens styring og kontroll.

For mer informasjon om internkontroll, se Difis veiledningsmateriale «Internkontroll i praksis - informasjonssikkerhet» (https://internkontroll-infosikkerhet.difi.no/).

[2] Forskrift om elektronisk kommunikasjon med og i forvaltningen (eForvaltningsforskriften) § 15.

Direktoratet for
forvaltning og IKT (Difi)
infosikkerhet.difi.no
infosikkerhet@difi.no

2.3 Lovkrav og standarder

I tillegg til at opplæring er en viktig brikke i virksomhetenes internkontroll, finnes det regelverk som stiller krav til opplæring. Den enkelte virksomheten kan også gjennom avtale ha forpliktet seg til å sikre at ansatte har tilstrekkelig kompetanse.

Virksomheten må selv vurdere hvilke krav som må oppfylles, enten som følge av krav i regelverk eller forpliktelser i avtaler. Under følger eksempler på krav til opplæring man kan være forpliktet til å følge (listen er ikke uttømmende):

Lov/forskrift/standard	**Virkeområde**	**Kravet omhandler**
Personvernforordningen artikkel 24 (personopplysnings-loven § 1)	Helt eller delvis automatisert behandling av personopplysninger og ikke-automatisert behandling av personopplysninger som inngår i eller skal inngå i et register.	Den behandlingsansvarlige skal gjennomføre egnede organisatoriske tiltak for å sikre at behandlingen utføres i samsvar med forordningen.
Sikkerhetsloven § 5, andre ledd, bokstav b	Forvaltningsorganer m.m.	Sørge for at ansatte og engasjerte får tilstrekkelig opplæring i sikkerhetsspørsmål.
Forskrift om sikkerhets-administrasjon § 3-1 (veiledning) og § 3-2 (kompetanse)	Forvaltningsorganer m.m.	Alle ansatte skal: • Før de settes til tjeneste relatert til skjermingsverdig informasjon ha tilstrekkelig kompetanse i sikkerhetstjeneste tilpasset den enkeltes oppgaver • ha gjennomført grunnleggende opplæring i sikkerhet Virksomheten skal ha oversikt over den sikkerhetsfaglige kompetansen og sørge for veiledning av de ansatte.

Direktoratet for
forvaltning og IKT (Difi)
infosikkerhet.difi.no
infosikkerhet@difi.no

NS-ISO/IEC 27001:2013 kapittel 7 (7.2. og 7.3.)	Kan være pålagt å følge gjennom avtale. eForvaltningsforskriften § 15 pålegger forvaltningsorganer som skal kommunisere elektronisk å ha en internkontroll (styring og kontroll) på informasjonssikkerhetsområdet. Internkontrollen skal være basert på anerkjente standarder. Difi anbefaler å basere seg på NS-ISO/IEC 27001:2013 (se bruksområdet «Internkontroll/styringssystem/ ledelsessystem for informasjonssikkerhet» i referansekatalogen for IT-standarder i offentlig sektor: https://www.difi.no/artikkel/2015/10/internkontroll-styringssystem-ledelsessystem-informasjonssikkerhet)	Krav til nødvendig opplæring, herunder krav til kartlegging, dokumentasjon og evaluering av opplæringen. For mer informasjon om de konkrete kravene, se omtalen av krav til kompetanse- og kulturutvikling i NS-ISO/IEC 27001:2013 i Difis veileder «Internkontroll i praksis - informasjonssikkerhet» (https://internkontroll-infosikkerhet.difi.no/hva-sier-isoiec-27001#Kompetanse- og kulturutvikling)

Direktoratet for forvaltning og IKT (Difi)
infosikkerhet.difi.no
infosikkerhet@difi.no

3 Hvordan oppnå helhetlig kompetanseutvikling

Målet er å ha et helhetlig tilbud som bidrar til at ansatte får nødvendig opplæring for å kunne utføre sine daglige oppgaver. De ansatte skal gjennom ulike aktiviteter:

- kjenne til kravene som stilles
- få forståelse for sikkerhetskravene som gjelder i egen organisasjon
- etterleve krav og bidra i utviklingen av organisasjonens sikkerhetskultur

Opplæringstiltak bør sees i sammenheng og være igangsatt på bakgrunn av behov. Opplæringen bør jevnlig vurderes og revideres etter behov.

Det er viktig å ha forankret opplæring- og kompetanseutviklingsaktiviteter i ledelsen. Før du går i gang med planleggingen av ulike aktiviteter bør du derfor ha:

- forankret arbeidet på riktig nivå i organisasjonen
- kartlagt hvem i organisasjonen du bør involvere i arbeidet. Dette kan være HR-avdeling, kommunikasjonsavdeling, driftsavdeling etc.

Noen virksomheter setter i gang en tidsbegrenset opplæringskampanje som har som mål å øke kompetansen og sikre bevisstgjøring av de ansatte innenfor visse temaer. Dette er et godt tiltak, men bør sees i en større kontekst blant annet for å sikre at nødvendig opplæring gis der det er behov over tid. Under følger anbefalinger til hvordan man kan jobbe med opplæring innen informasjonssikkerhet, i følgende steg:

- Kartlegge behov – sette i gang tiltak på relevante områder
- Velge målgruppe og tilpasse tiltak
- Ta i bruk passende virkemiddel
- Tenkte helhetlig – se tiltak i sammenheng
- Måle effekt
- Etablere forvaltningsregime

Tips:

- For å sikre at man tar stilling til alle temaene her kan malen for utvelgelse av opplæringstiltak i kapittel 4 benyttes i arbeidet.
- Difis veileder «La stå!» kan også benyttes i utviklingen av kompetansetiltak: https://www.difi.no/opplaeringstilbud/difis-opplaeringstilbud/la-sta-digital-veileder-utvikling-av-kompetansetiltak

Husk:

- Ledelsens ansvar og ledelsesforankring er viktig. Uten ledelsens støtte er det vanskelig å få gjennomført nødvendige opplæringstiltak blant annet fordi det blir vanskelig å få prioritert nødvendig tid og ressurser til å utføre aktiviteten, og vanskelig å kreve obligatorisk deltagelse i opplæringsarenaer.
- Det kan være krevende å holde på med opplæring. Ikke mist motet, og hør på deltagernes tilbakemeldinger.

Direktoratet for forvaltning og IKT (Difi)
infosikkerhet.difi.no
infosikkerhet@difi.no

3.1 Kartlegge behov – sette i gang tiltak på relevante områder

Det er viktig at virksomhetene har vurdert behovet for opplæring før det igangsettes opplæringstiltak. På den måten vet man at man bruker ressursene sine riktig. Det første man må gjøre er derfor å velge ut hvilke områder og hvilke temaer det skal gis opplæring i basert på et konkret behov. Opplæringstiltak kan være nødvendige blant annet fordi:

a. Risikovurderinger tilsier at opplæring er nødvendig på et område.
   Et eksempel på dette kan være at virksomheten innfører et nytt it-system, og dermed må ha opplæring for de ansatte for å sikre at informasjon blir håndtert riktig.

b. Virksomheten har forpliktelser i henhold til lov eller avtale (se kapittel 2.3.)
   Et eksempel på dette kan være at en virksomhet har avtalt utveksling av opplysninger, og har forpliktet seg til å ha særskilt opplæring i behandlingen av disse.

c. Revisjoner, evalueringer eller undersøkelser har vist at sikkerhetskulturen bør forbedres.
   Et eksempel kan være at undersøkelser har vist at ansatte i liten grad følger interne rutiner på et spesielt område.

Når man velger ut område for opplæring, er det viktig å sette seg noen mål for opplæringen. Uten å ha konkrete og målbare mål for hva man ønsker å oppnå, er det vanskelig å se om tiltaket har ønsket effekt. Et eksempel på et mål er at man ønsker at en større andel dokumenter lagres i det elektroniske saksbehandlingssystemet for å sikre opplysningenes integritet og tilgjengelighet.

Måling av effekten av tiltak omtales i kapittel 3.5.

3.2 Velge målgruppe og tilpasse tiltak

Det er ikke nødvendig å sette i gang opplæringstiltak for ansatte som ikke har behov for det. Når det er konkludert med at det er behov for opplæring, er det derfor viktig å se på målgruppen for opplæringen. Spørsmål man kan stille seg, er for eksempel: Trenger alle ansatte opplæring, eller er det kun visse grupper? Er det kun relevant for nyansatte, eller er det aktuelt å inkludere øvrige ansatte? Hvilke målgrupper som finnes vil variere mellom virksomhetene. Eksempler på målgrupper er:

- Nyansatte
- Ledere
- Systemutviklere
- IT-driftspersonell/brukerstøtte
- Saksbehandlere
- Kundesenter
- Innleid personell

Direktoratet for
forvaltning og IKT (Difi)
infosikkerhet.difi.no
infosikkerhet@difi.no

Tips:

- Vurder nøye hvilke målgrupper du har i din virksomhet og hvilke virkemidler som vil passe for å motivere målgruppene. Samme tilnærming passer ikke for alle.
- Ved bygging av sikkerhetskultur må hele organisasjonen involveres.
- Pass på å ha tydelige og klare budskap.
- Hvis du inviterer til åpne arrangementer, er det viktig å kommunisere på forhånd hvilken målgruppe du ønsker skal delta. Hvis deltagerne føler budskapet ikke treffer dem, kan de i verste fall miste interessen for å lære mer om informasjonssikkerhet. Dette kan føre til at de ikke deltar på fremtidige arrangementer som faktisk er rettet mot dem.
- Ved å trekke inn kommunikasjonsenheten/de som jobber med kommunikasjon tidlig i prosessen, kan du få gode tips og råd til hvordan du kan nå frem til din målgruppe.
- Involver de minst endringsvillige tidlig i prosessen med utvikling av opplæringstiltak. Du kan da få kritikerne til å bli dine beste ambassadører.

3.3 Ta i bruk passende virkemiddel

Det er mange ulike virkemidler som kan benyttes når man skal foreta opplæring. Det er viktig å velge virkemiddel som er egnet for å nå målgruppen, og som er mulig å gjennomføre utfra tilgjengelige ressurser og hjelpemidler. Vurder nøye kapasitet til å planlegge, gjennomføre og evaluere aktiviteten opp mot økonomiske ressurser tilgjengelig.

Det er også lurt å variere bruken av virkemidler. For å nå frem til enkelte målgrupper kan det være aktuelt å bruke flere virkemidler. Samtidig kan et virkemiddel som har fungert godt miste noe av effekten over tid. Det kan derfor være hensiktsmessig å vente en periode før opplæringstiltaket tas i bruk igjen.

Det er viktig å ha et bevisst forhold til om opplæringen skal gi konkret kunnskap, bevisstgjøre ansatte, trene ferdigheter, eller bidra til utviklingen av organisasjonens kultur. Samme virkemiddel er ikke nødvendigvis egnet for å nå alle målsetningene. For eksempel vil dilemmatrening være et bra virkemiddel for å bevisstgjøre ansatte og utvikle organisasjonens kultur, men mindre egnet dersom man skal trene på en bestemt ferdighet.

Eksempler på virkemidler er:

- Aksjon/stunt (f.eks. utdeling av sjokolade til de som har låst pc.)
- Ambassadører (ansatte som får en særskilt rolle i informasjonssikkerhetsarbeidet i en enkelt enhet.)
- Deltagelse i forum eller møter for å utveksle informasjon og skape dialog
- Dilemmatrening (Diskusjoner og/eller refleksjonsøvelser f.eks. gjennom bruk av spill, gruppediskusjoner og rollespill.)
- Egenerklæring
- E-læringskurs
- En-til-en samtaler
- Filmer
- Informasjon på skjermer, plakater, intranett, oppslagstavler o.l.
- Informasjonsskriv, løpesedler ol.

Direktoratet for forvaltning og IKT (Difi)
infosikkerhet.difi.no
infosikkerhet@difi.no

- Klasseromsundervisning/foredrag
- Kurs
- Nanokurs (dvs. kortere e-læringskurs)
- Samtaler i uformelle møteplasser (f.eks. under fredagskaffe og lunsj)
- Øvelser

Tips:

- Ikke gap over for mye i starten. Det kan være lettere å starte i det små med et lite tiltak, som etter hvert kan skaleres opp.
- Ved bruk av tekniske hjelpemidler, f.eks. e-læringskurs, er det viktig å sjekke at de tekniske forutsetningene for opplæringstiltaket er til stede samt teste løsningen godt før utrulling.
- Når du skal rulle ut et opplæringstiltak, kan det være lurt å skaffe noen ambassadører. Dette er personer i organisasjonen som vil kunne spre budskapet og få andre til å delta, reflektere over, og komme med tilbakemeldinger på opplæringen.
- Varier virkemiddelbruken.
- Humor er viktig. Dette kan være et godt virkemiddel for å få til at informasjonssikkerhet blir et tema i kantina. Samtidig må humoren være tilpasset de ansatte. Se an organisasjonen, og ikke overdriv.
- Historier fungerer ofte bedre enn statistikk. Ved å gjøre budskapet personlig og relevant vil flere huske budskapet i ettertid.
- En god måte å bevisstgjøre ansatte på, er å få dem til å forstå hvorfor informasjonssikkerhet er viktig og relevant for den enkelte. Dette kan f.eks. gjøres ved å få de ansatte til å reflektere over spørsmålet «hvorfor er informasjonssikkerhet viktig for meg i min jobb»?
- Egenerklæringer kan være egnet for å få bekreftet gjennomført opplæring og kunne fremlegge dokumentasjon ved en eventuell revisjon. Husk at erklæringene ikke gir informasjon om faktisk forståelse for, og etterlevelse av, krav.

3.4 Tenke helhetlig – se tiltak i sammenheng

3.4.1 Sammenheng mellom opplæringstiltak innen ulike fagområder

Det er vanligvis et behov for å ha opplæring på mange ulike områder, inkludert informasjonssikkerhet. Det kan derfor være lurt å se på all opplæring i virksomheten i sammenheng, slik at man sparer tid og ressurser, får opplæring tematisk i en god rekkefølge, og at ansatte ser sammenhengen mellom de ulike områdene det drives opplæring innen. I tillegg vil enkeltstående tiltak innen et konkret tema kunne gi økt kunnskap blant ansatte innenfor det aktuelle området, men gi mindre bevisstgjøring fordi man ikke ser hvordan det henger sammen med virksomhetens mål og øvrige prosesser.

Ved etablering av et nytt opplæringstiltak bør man derfor undersøke om man allerede har etablert opplæringstiltak eller tatt i bruk virkemidler på andre områder som kan benyttes.

Direktoratet for
forvaltning og IKT (Difi)
infosikkerhet.difi.no
infosikkerhet@difi.no

Tips:

- God ferdighetstrening kombinerer kunnskap, bevisstgjøring og ferdigheter innen informasjonssikkerhet med ferdighetsopplæring i arbeidsprosesser og bruken av IKT-verktøy.
- Bruk gjerne eksisterende fora/møteplasser.
- Ikke legg opplæringsaktiviteter til de travleste periodene i virksomheten.

3.4.2 Legg en plan

Kompetanse- og opplæringsplaner, både for virksomheten generelt og for informasjonssikkerhet spesielt, kan bidra til at opplæringen skjer mer systematisk. Det er den enkelte virksomhet som selv må vurdere hvilket behov for planer som er nødvendig og på hvilket nivå. Planene kan være egne planer eller være en del av øvrige dokumenter. Det viktige er å ta stilling til hvilke kompetansebehov virksomheten har, og arbeide systematisk for å dekke det.

Kompetanseplaner: Med kompetanseplaner menes i denne veilederen oversikt over behov for kompetanse på ulike nivåer (virksomhetsnivå, innen informasjonssikkerhet spesielt eller på individnivå). En kompetanseplan er knyttet opp til virksomhetens strategiske prioriteringer og mål. På virksomhetsnivå kalles det ofte en kompetansestrategi, mens det på individnivå ofte kalles en utviklingsplan.

Opplæringsplaner: Med opplæringsplaner menes i denne veilederen konkrete planer for å utføre opplæring. Hensikten med en opplæringsplan er å dekke behovene i kompetanseplanen.

Kompetanseplaner for opplæring innen informasjonssikkerhet er et nyttig virkemiddel for å oppnå en helhetlig tilnærming til kompetanseheving. Noen virksomheter har generelle kompetanseplaner som skal dekke virksomhetens totale kompetansebehov. Det er da hensiktsmessig å utarbeide kompetanseplaner for informasjonssikkerhet som sees i sammenheng med virksomhetens generelle kompetanseplan.

Opplæringsplaner er nyttige verktøy for å sikre at kompetanseplanens målsetninger oppnås. Virksomheten kan ha felles opplæringsplaner for flere områder. Når man utformer en egen opplæringsplan for informasjonssikkerhet, bør denne sees i sammenheng med den generelle opplæringsplanen. Dermed kan man unngå overlappende aktiviteter eller at ulik opplæring for samme personer legges til samme tidspunkt.

I hvilken grad kompetanse- og opplæringsplaner blir individuelt tilpasset er et spørsmål om kost/nytte. Individuelt tilpassede planer vil normalt kreve en kartlegging av stillinger og funksjoners behov, og individuelle og gruppers kompetansestatus og behov. Dette kan være et krevende arbeid, men kan også bidra til at opplæringstiltak rettes mot riktige målgrupper og individer.

Direktoratet for
forvaltning og IKT (Difi)
infosikkerhet.difi.no
infosikkerhet@difi.no

Kompetanse- og opplæringsplaner innen informasjonssikkerhet bør være en del av virksomhetens internkontrollarbeid. Slik sikrer man at kompetansebehov vurderes samlet, og at opplæringsaktiviteter sees i sammenheng med øvrige aktiviteter. For mer informasjon om internkontroll, se Difis veiledningsmateriale «Internkontroll i praksis - informasjonssikkerhet» (https://internkontroll-infosikkerhet.difi.no/).

Figuren viser hvordan virksomheten kan ha kompetanse- og opplæringsplaner på ulike nivåer som må sees i sammenheng, og som henger sammen med virksomhetens internkontroll.

Tips:

- Husk at opplæring må gjøres jevnlig. Ansatte kommer og går, og kunnskap er ferskvare.
- Eksempel på opplæringsplan: https://www.difi.no/artikkel/2015/06/eksempel-opplaeringsplan-innen-informasjonssikkerhet

3.5 Måle effekt

Når man setter i gang opplæringstiltak, er det viktig å kunne se om opplæringen har hatt ønsket effekt. Opplæringstiltakene som settes i verk bør derfor ha målbare kriterier som kan gi nok informasjon til å vurdere om opplæringen er nyttig og bør videreføres i fremtiden. Ved oppstart av opplæringsarbeid eller i planleggingen av et nytt opplæringstiltak må man derfor se på formålet med opplæringen, og velge måleparametere som gir svar på om målet er oppnådd.

Det er lettere å måle konkrete hendelser, f.eks. deltagelse i opplæringstiltak, fremfor holdninger og adferd. Samtidig er det viktig å se på faktiske holdninger og etterlevelse – den enkeltes adferd – for å sikre at tiltaket har hatt ønsket effekt. Det ideelle er å måle resultater fremfor gjennomførte

Direktoratet for forvaltning og IKT (Difi)
infosikkerhet.difi.no
infosikkerhet@difi.no

aktiviteter. Det er viktig å vurdere både kvantitative og kvalitative målinger, da disse kan gi ulik informasjon. Måling kan gjøres på flere måter, for eksempel

- spørreundersøkelse blant ansatte
- en-til-en samtaler
- antall rapporterte sikkerhetshendelser
- statistiske opplysninger fra bruk av IT-systemer
- fysiske undersøkelser, f.eks. av adgangskontroll og låsing av pc

Ved valg av måleparametere er det lurt å se på hva som finnes fra før, siden det er ressursbesparende å benytte seg av eksisterende data. Ofte eksisterer det allerede tall som kan benyttes, for eksempel antall uønskede hendelser eller antall passordbytter i løpet av et år.

Det anbefales å måle tilstanden før og etter at man setter i gang tiltak. En måling som gjøres før opplæring gjennomføres kalles gjerne en nullpunktsmåling, eller baseline på engelsk. Kun ved å måle både før og etter ser man om opplæringstiltaket har hatt effekt.

Ved måling av effekt over tid, er det sentralt å gjennomføre målingen på tilnærmet samme måte slik at grunnlaget blir sammenliknbart. Dette betyr for eksempel at spørsmål som stilles i et spørreskjema ikke kan endres hvis svarene skal sammenlignes over tid.

Hva man velger å måle vil være avhengig av hva man ønsker å oppnå med opplæringen. Dersom man ønsker å få ned antall hendelser innen et gitt område, kan for eksempel statistikk over antall hendelser være nok. Dersom man ønsker å forbedre sikkerhetskulturen, for eksempel gjennom holdningsendring, kan det være mer hensiktsmessig å gjennomføre anonyme spørreundersøkelser eller en-til-en samtaler.

Hvis du skal samle inn personopplysninger i forbindelse med måling, er det viktig å ta stilling til hva opplysningene skal brukes til før man begynner å måle. En konkret plan bidrar til at man kun samler inn relevant informasjon og får en mer effektiv kontroll med oppfølgningen.

Måling er en viktig brikke i virksomhetens internkontroll. For mer informasjon, se omtalen av måling i Difis veileder «Internkontroll i praksis - informasjonssikkerhet» (https://internkontroll-infosikkerhet.difi.no/systematiske-aktiviteter/maling-evaluering-og-revisjon).

Tips:

- Et godt avvikshåndteringssystem kan gi verdifulle opplysninger om antall avvik, hvilke områder man bør se nærmere på etc. Men husk at antall innmeldte avvik ikke i seg selv nødvendigvis gir god nok informasjon om opplæring har hatt ønsket effekt.
- Hvis du måler folks adferd, er det viktig å bruke informasjonen forsiktig. Bruk helst statiske opplysninger når du kommuniserer resultatene. Og pass på at ingen føler seg hengt ut.
- Vær oppmerksom på hvordan du utformer spørsmål. Vi har en tendens til å svare det vi tror er forventet eller ønsket svar.

Direktoratet for forvaltning og IKT (Difi)
infosikkerhet.difi.no
infosikkerhet@difi.no

3.6 Etablere forvaltningsregime

Det er nødvendig å ha en plan for håndtering av kompetanseplaner og opplæringstiltak i fremtiden. Et forvaltningsregime definerer hvordan de ulike kompetanseplanene og opplæringstiltakene i virksomheten forvaltes: hvordan de brukes, oppdateres og utfases.

Kompetanseplaner er et arbeidsverktøy som kontinuerlig skal være i samsvar med virksomhetenes praksis. Det er derfor viktig å ha avklart hvem som oppdaterer planene ved behov.

De konkrete opplæringstiltakene vil også kreve oppdatering og videreutvikling. Det kan være behov for oppdatering av ulike årsaker, for eksempel at det innføres nye krav, policyer og retningslinjer oppdateres, eller organisasjonen endres. I tillegg vil materiale ikke oppnå samme effekt i lengden dersom mange har sett det før, og det kan derfor være nødvendig å oppdatere materiale eller vente en stund før materialet benyttes igjen.

Ved å ha etablert et forvaltningsregime sikrer man at tiltakene til enhver tid er oppdaterte, relevante og brukes på riktig måte.

Tips:

- Vær tydelig på hvem som har ansvar for å forvalte et opplæringstiltak og opplæringsplan(er).

3.7 Oppsummering

Ved å ha et helhetlig opplæringsprogram for ansatte sikrer man at medarbeiderne har tilstrekkelig kompetanse for å kunne utføre sine arbeidsoppgaver på en hensiktsmessig måte. Ved å se tiltakene i sammenheng sørger man for at opplæringen kan skje mer effektivt og legger til rette for at den enkelte kan se sammenhengen mellom temaene det gis opplæring innen. Dette danner et godt grunnlag for å få medarbeidere som har nødvendig kunnskap og ferdigheter innen informasjonssikkerhet, reflekterer over sine handlinger og er med å danne en god sikkerhetskultur.

Direktoratet for
forvaltning og IKT (Difi)
infosikkerhet.difi.no
infosikkerhet@difi.no

4 Vedlegg – Mal for utvelgelse av opplæringstiltak

Malen kan benyttes som et hjelpemiddel for å sikre at man har tatt stilling til vurderingstemaene som er omtalt i veilederens del 3. Skjemaet kan brukes til å få oversikt over opplæringstiltak man har eller skal igangsette. Skjemaet kan tas inn som et vedlegg til virksomhetens opplæringsplan(er).

Vurderingstema:	**Eksempel 1:**	**Eksempel 2:**	
1. Område (tema for opplæringen)	Bruk av bærbar pc.	Håndtering av utskrifter.	
Tema valgt på bakgrunn av:	Risikovurdering (eventuelt referanse).	Risikovurdering (eventuelt referanse).	
Mål:	Ansatte håndterer bærbare pc-er i tråd med sikkerhetspolicyen.	Alle ansatte bruker sikker utskrift og ingen dokumenter med taushetsbelagte opplysninger ligger på skriveren.	
2. Målgruppe:	Nyansatte	Alle ansatte. Spesielt fokus på nyansatte.	
3. Virkemiddel:	Tema for innlegg på nyansattkurset (20 min presentasjon).	Tema for innlegg på nyansattkurs (20 min presentasjon). Nyhetssak på intranett.	
4. Referanse til kompetanse og/eller opplæringsplan(er):	Opplæringsplan innen informasjonssikkerhet (henvisning/link).	Opplæringsplan innen informasjonssikkerhet (henvisning/link).	
5. Måling (måleparameter):	At nyansatte har fått opplæring: Måles ved å føre deltagerliste på kurset. Håndtering i tråd med instruks: Måles ved å telle antall mistede pc-er i løpet av ett år rapportert inn til IT-drift.	Alle nyansatte har fått opplæring: Måles ved å føre deltagerliste på kurset. Alle ansatte er registrert med sikker utskrift. Fysisk kontroll fire ganger i året av om dokumenter med taushetsbelagte opplysninger ligger igjen på skriverne.	
6. Ansvar for forvaltning:	NN (seksjonssjef, avdelingsleder, ansatt etc.)	NN (seksjonssjef, avdelingsleder, ansatt etc.)	

Direktoratet for forvaltning og IKT (Difi)
infosikkerhet.difi.no
infosikkerhet@difi.no