Retningslinje for arbeid med sikkerhetskultur og opplæring innen informasjonssikkerhet

Type dokument	Retningslinje
Forvaltes av	Leder av HR- og HMS-avdelingen
Godkjent av	Direktør for Organisasjon og infrastruktur
Gjelder fra	12.06.2023
Neste revisjon innen	12.06.2025
Unntatt offentlighet	Nei
Referanse ISO	ISO 27002:2022; 6.3
Referanse LOV/Regel	Arbeidsmiljøloven § 4-2
Referanse interne dokumenter	Politikk for informasjonssikkerhet

1. Formål

Formålet med denne retningslinjen er å definere ansvar, målgrupper og arenaer for aktiviteter knyttet til målrettet opplæring, kompetansehevende tiltak, og utvikling av bevissthet rundt informasjonssikkerhet i organisasjonskulturen. En organisasjonskultur innebærer en sikkerhetskultur der felles innarbeidede verdier og normer påvirker medarbeideres tanker og forventninger til sikkerhet.

2. Gjelder for

Retningslinjen for arbeid med sikkerhetskultur og opplæring gjelder for alle som har tilgang til, og/eller bearbeider og forvalter informasjon gjennom NTNUs IKT-infrastruktur.

3. Overordnede prinsipper

a. Som førende for arbeidet med sikkerhetskultur og opplæring ved NTNU ligger den til enhver tid gjeldende handlingsplan for informasjonssikkerhet i statsforvaltningen. I gjeldende handlingsplan beskrives *Kunnskap, kompetanse og kultur* som et eget tiltaksområde.
b. Til grunn for arbeidet med sikkerhetskultur og opplæring skal også NTNUs overordnede risikobilde for samfunnssikkerhet ligge, hvor informasjonssikkerhet er kartlagt som et eget risikoområde.
c. Arbeidet med sikkerhetskultur og opplæring skal være en systematisk og kontinuerlig forbedringsprosess.

d. Innholdet i alt utviklingsarbeid og opplæring skal understøtte hovedbudskapet om at informasjonssikkerhet dreier seg om samspill imellom mennesker og informasjonssystemer.
e. All opplæring skal bidra til å skape økt risikoforståelse, samt styrke evnen og lysten til å handle riktig.

4. Arbeidet med sikkerhetskultur og opplæring

Målbildet for arbeid med sikkerhetskultur og opplæring er NTNUs vedtatte mål for informasjonssikkerhet[1]. Arbeidet med å nå dette målbildet innebærer en systematisk og kontinuerlig forbedringsprosess, hvor risikostyring og innebygd informasjonssikkerhet ivaretas gjennom lederes og medarbeideres aktive risikobevissthet og risikoforståelse. Innebygd informasjonssikkerhet er et overordnet prinsipp i arbeidet med informasjonssikkerhet og oppnås når informasjonssikkerhet er:

a. Innarbeidet i virksomhetsstyring og understøtter virksomhetens mål
b. Innarbeidet i virksomhetens prosesser og prosjekter fra starten av
c. Tatt hensyn til i hele livssyklusen til IKT-løsninger
d. Et tema alle ansatte kjenner til og vet hva innebærer for sine arbeidsoppgaver

Fasene i forbedringsprosessen består av planlegging, gjennomføring, evaluering og revidering. Dette arbeidet skal i hovedsak utvikles og drives sentralisert, i tråd med annet kvalitets- og utviklingsarbeid ved NTNU. Linjens ansvar er å delta i de utviklings- og opplæringstiltak som gjøres tilgjengelige. Linjen har også ansvar for å følge opp særskilt risikofylte områder ved sin enhet med lokale målrettede opplæringstiltak. Innholdet i opplæringen skal bygge på de identifiserte krav til informasjonssikkerhet for de klassifiserte informasjonselementene i de aktuelle systemer, tjenester og prosesser for målgruppene til de ulike opplæringsmodulene.

4.1. Sikkerhetsklima

Sikkerhetsklima dreier seg om den synlige vektleggingen av sikkerhet. Sikkerhetsklima innebærer blant annet lederens prioritering av sikkerhet, vektlegging av sikkerhetssystemer og graden av risikotoleranse og brukes for å ha oversikt og kontroll på egen sikkerhet.
Ledere skal gjennom systematisk kartlegging av sikkerhetsklima bistå i å avdekke områder for nødvendig opplæring og kompetansehevende tiltak for å skape et kontinuerlig arbeid med utvikling av enhetens sikkerhetskultur. Sikkerhetsklima skal rapporteres til kontrollerende del i styringssystemet.

4.2. Handlingsplan

Med bakgrunn i risikobildet og analyse av NTNUs sikkerhetsklima skal det etableres en sentral handlingsplan på virksomhetsnivå for arbeidet med sikkerhetskultur og opplæring i et flerårsperspektiv. Handlingsplanen skal ha tydelige effekt- og resultatmål for hele NTNU. Handlingsplanen skal inneholde en opplæringsplan og en kommunikasjonsplan for den aktuelle perioden. Handlingsplan skal rapporteres til kontrollerende del i styringssystemet.

[1] Politikk for informasjonssikkerhet

4.3. Opplæringsplan

Opplæringsplanen skal inneholde målgruppeorienterte, modulbaserte opplæringstilbud til alle ansatte, og med målbar operasjonalisering av hvordan målene i handlingsplanen skal nås. Opplæringsplanen skal i sum over tid treffe innenfor de tre kategoriene tiltak definert i Politikk for informasjonssikkerhet:

a. Lederes implementering av risikostyring i enhetene
b. Utvikling av sikkerhetskultur, kompetanse og holdninger
c. Utvikling av en robust infrastruktur som ivaretar den digitale sikkerheten

Opplæringsmodulene og kursene skal også integreres i NTNUs øvrige opplæringsprogram for ledere og ansatte.

4.4. Kommunikasjonsplan

Kommunikasjonsplanen skal i sin strategiske målsetting og oppbygging følge en kommunikasjonsmodell som over tid bidrar til

a. bevissthet og oppmerksomhet for informasjonssikkerhet
b. et ønske om å støtte og delta i endringsprosessen
c. kunnskap om hvordan sikre NTNUs informasjonsverdier
d. evne til å ta imot ny kunnskap og ta i bruk nye arbeidsmetoder
e. forankring av ny praksis og sikre etterlevelse

Kommunikasjonen som følger opplæringsplanen, skal være i takt med økt risikoforståelse og modenhet for innholdet i opplæringen. Dette for å sikre at kommunikasjonen bygger opp om, og gir støtte til opplæringen som gjennomføres, og for å sikre at ansatte innenfor de tjenester og prosesser som styringssystemet møter opplever sammenheng mellom tilgjengelig informasjon og opplæring.

For alle målgrupper skal det i hovedsak benyttes etablerte møtearenaer og kanaler til informasjon og kommunikasjon om informasjonssikkerhet. I tillegg vil det produseres tilpasset og målgruppespesifikk informasjon på Innsida, i fakultetskanaler og administrative avdelingskanaler, samt skriftlig informasjon som benyttes som supplement ved behov.

4.5. Evaluering

Handlingsplanens innhold, operasjonalisering og måloppnåelse skal ved endt periode evalueres. Læringspunkter tas med i utforming av etterfølgende opplæringsplan og kommunikasjonsplan for slik å sørge for kontinuerlig forbedring og målrettet utvikling. Evalueringen rapporteres inn til kontrollerende del i styringssystemet.

5. Roller og ansvar

5.1. Direktør for organisasjon og infrastruktur

a. Skal påse at det utvikles handlingsplaner som sørger for et systematisk og kontinuerlig arbeid med sikkerhetskultur og opplæring innen informasjonssikkerhet

5.2. Leder av HR- og HMS-avdelingen

a. er ansvarlig for organisasjonsutvikling og endringsledelse i arbeidet med informasjonssikkerhet; herunder påse at ledere er kjent med, og har tilstrekkelig kompetanse og risikoforståelse, til å ivareta sitt ansvar for å utøve risikostyring innen området informasjonssikkerhet
b. er ansvarlig for kartlegging av sikkerhetsklima, med spørreundersøkelse til ledere, med frekvens hvert annet år
c. er ansvarlig for at det utarbeides overordnet handlingsplan for arbeid med sikkerhetskultur og opplæring med tilhørende opplærings- og kommunikasjonsplan for ledere og øvrige ansatte
d. er ansvarlig for evaluering av arbeidet med sikkerhetskultur og opplæring, at informasjon og opplæring på sikkerhetsområdet er konsistent, er i samsvar med overordnede prinsipper og at det dekker relevante arbeidsprosesser
e. er ansvarlig for at arbeidet med sikkerhetskultur og opplæring følger opp fokusområder fra ledelsens gjennomgang og andre kontrollaktiviteter
f. er ansvarlig for å rapportere på gjennomføringsgrad, effekt og effektivitet i arbeidet med opplæring og bevisstgjøring

5.3. Dekan/Instituttleder/Linjeleder

a. er ansvarlig for at ansatte i enheten har tilstrekkelig opplæring innen informasjonssikkerhet, og kan ivareta sin plikt til å vurdere risiko ved nye prosjekt og ved all informasjonsbehandling, samt melde og håndtere avvik ved brudd på informasjonssikkerheten

5.4. Leder av HMS og Beredskaps-seksjonen

a. skal konsulteres i planlegging av kontinuitet og beredskapsarbeidet for å sikre at arbeidet gjennomføres i henhold til Politikk for beredskap

5.5. Leder av Seksjon for digital sikkerhet

a. skal konsulteres i arbeidet med utvikling av kommunikasjon og opplæringsmateriale for å sikre faglig relevant innhold og oppdatert risiko- og trusselbilde

5.6. Systemeier

a. er ansvarlig for at opplæringsmateriale knyttet til bruk av IKT-systemer utvikles og kommuniseres i henhold til gjeldende retningslinje