Politikk for Informasjonssikkerhet

Type dokument	Politikk
Forvaltes av	Direktør for organisasjon og infrastruktur
Godkjent av	Direktør for organisasjon og infrastruktur
Gjelder fra	12.06.2023
Neste revisjon innen	12.06.2025
Klassifisering	Åpen
Referanse ISO	27002:2022; 5.1, 5.2, 5.31, 5.35, 5.36
Referanse NSMs grunnprinsipper for IKT-sikkerhet	1.1.1, 1.1.2, 1.3.3a
Referanse LOV/Regel	eForvaltningsforskriften §15 og § 20, personvernforordningen artikkel 5, 24, 32
Referanse interne dokumenter	IKT-reglementet Retningslinjer innenfor informasjonssikkerhet og personvern

1. Formål

Formålet med politikk for informasjonssikkerhet er å sette rammene for arbeidet med informasjonssikkerhet og digital sikkerhet ved NTNU. Politikken skal legge til rette for at arbeidet med å ivareta NTNUs informasjonsverdier, overholder sentrale lover og forskrifter, samt relevante føringer fra myndigheter. Arbeidet med informasjonssikkerhet og digital sikkerhet skal muliggjøre at NTNU kan løse sitt samfunnsoppdrag på en måte som opprettholder tillit i fra ansatte, studenter, partnere og samfunnet for øvrig.

Informasjonssikkerhetsarbeidet ved NTNU overlapper i stor grad arbeidet med digital sikkerhet. Store deler av verdiene som behandles og oppbevares ved NTNU er informasjon, eller områder, systemer og mennesker som oppbevarer eller behandler informasjon. Disse struktureres som enten primærverdi eller sekundærverdi. Primærverdien omhandler informasjon som behandles og forvaltes gjennom NTNUs forskning, utdanning, nyskaping og administrasjon. Sekundærverdier handler om de verktøyene vi benytter, og kompetansen til de som benytter verktøyene. Dette innbefatter ansatte, studenter, lokasjoner, organisasjonsstrukturer, maskinvare, programvare og nettverk.

Politikk for informasjonssikkerhet er underlagt IKT-reglementet og overordnet retningslinjer for informasjonssikkerhet. Sammen utgjør dette styringssystemet for informasjonssikkerhet, som danner grunnlaget for NTNUs arbeid med informasjonssikkerhet, og er en integrert del av NTNUs helhetlige virksomhetsstyring. Styringssystemet gir rammene for en systematisk og helhetlig praksis mellom styrende, gjennomførende og kontrollerende del av arbeidet med informasjonssikkerhet.

2. Gjelder for

NTNUs politikk for informasjonssikkerhet, digital sikkerhet og personvern gjelder for alle som har tilgang til, lagrer, bearbeider eller overfører informasjonsverdier gjennom NTNU eller tilhørende NTNUs virke.

3. Definisjon

Informasjonsverdier er informasjon som kan påføre personer, organisasjoner eller samfunnet skade hvis det kommer på avveie, blir borte eller blir endret på. Informasjonsverdier struktureres som enten primærverdi eller sekundærverdi. Primærverdien omhandler informasjon som behandles og forvaltes gjennom NTNUs forskning, utdanning, nyskaping og administrasjon. Sekundærverdier handler om de verktøyene vi benytter, og kompetansen til de som benytter verktøyene. Dette innbefatter ansatte, studenter, lokasjoner, organisasjonsstrukturer, maskinvare, programvare og nettverk.

Med **informasjonssikkerhet** mener vi at informasjonen er beskyttet mot uønsket innsyn, at den er tilgjengelig når den trengs, og at den er beskyttet mot uønskede endringer. Informasjonssikkerhet handler om hvordan informasjonens konfidensialitet, integritet og tilgjengelighet blir ivaretatt.

Konfidensialitet - Sikkerhet for at nærmere angitt informasjon ikke avsløres for uvedkommende, og at kun autoriserte personer får tilgang til denne.

Integritet - Sikkerhet for at informasjonen og informasjonsbehandlingen er fullstendig, nøyaktig og gyldig, og et resultat av autoriserte og kontrollerte aktiviteter

Tilgjengelighet - Sikkerhet for at en tjeneste oppfyller bestemte krav til stabilitet, slik at aktuell informasjon er tilgjengelig ved behov

Dette er samme definisjoner som brukes i «Nasjonal Strategi for informasjonssikkerhet».

4. Overordnede prinsipper

Overordnede prinsipper definerer rammen for alt arbeid med informasjonssikkerhet, digital sikkerhet og personvern ved NTNU. Ledelsen har gitt følgende overordnede prinsipper:

a. Arbeidet med informasjonssikkerhet skal ligge til grunn for at NTNU kan løse sitt samfunnsoppdrag og opprettholde tilliten i samfunnet.
b. NTNU skal arbeide systematisk, metodisk og målrettet med informasjonssikkerhet for å balansere risiko med åpenhet.
c. NTNU skal beskytte sine informasjonsverdier og digital infrastruktur ved komplementerende sikkerhetstiltak i flere lag som hindrer, eller begrenser skade ved uønskede hendelser for NTNU, partnere, individ eller samfunnet.
d. NTNU skal ivareta konfidensialitet, integritet og tilgjengelighet gjennom sikkerhetstiltak der verdi og tiltak er i balanse ved å være så åpen som mulig, men så lukket som nødvendig.
e. En risikoeier kan ikke akseptere risiko som går utenfor eget risikodomene eller som kan påføre NTNU, individer, samfunnet, partnere eller andre skade.

5. Sikkerhetsmål

Ledelsen ved NTNU har vedtatt følgende mål og prioriteringer for arbeidet med informasjonssikkerhet:

a. NTNU skal ha oversikt over informasjonsverdier som behandles og forvaltes, samt risikoreduserende tiltak iverksatt for å beskytte disse.
b. NTNU skal ha en motstandsdyktig og forsvarbar digital infrastruktur, rigget for å tilstrekkelig beskytte informasjon og infrastruktur, samt oppdage, håndtere og begrense skade ved uønskede hendelser.

c. Alle som har en brukerkonto tilknyttet NTNU skal ha et bevisst forhold til informasjonssikkerhet og personvern, samt bidra til å sikre NTNUs informasjonsverdier gjennom å etterleve prinsipper og krav til informasjonssikkerhet.
d. NTNU skal benytte sikkerhetshendelser, avvik og revisjon til systematisk og kontinuerlig læring, forbedring og målrettede tiltak slik at organisasjonen best kan adressere risiko og det gjeldende trusselbilde.

6. Strategi for informasjonssikkerhet

Strategi beskriver hvordan NTNU skal nå sine mål for informasjonssikkerhet ved å fokusere på tre kjerneområder. Det første er virksomhetens, og lederes implementering av risikostyring i enhetene, det andre er utvikling av sikkerhetskultur, kompetanse og holdninger og det tredje er å opprettholde en robust infrastruktur som ivaretar den digitale sikkerheten:

a. Risikostyring og kontroll med informasjonssikkerheten er et lederansvar og en del av den ordinære virksomhetsstyring og internkontrollen. Ledere skal ha en god risikoforståelse og oversikt over de informasjonsverdier som en er ansvarlig for, slik at de er i stand til å ta informerte valg og gjøre prioriteringer ved innføring av sikkerhetstiltak.
b. Arbeidet med sikkerhetskultur og opplæring skal være en systematisk og kontinuerlig forbedringsprosess. Økt kompetanse skal gjøre ansatte og studenter i stand til å sikre NTNUs informasjonsverdier gjennom en risikobasert tilnærming.
c. NTNU skal sikre informasjonsverdier gjennom en systematisk implementering av kravene i retningslinjene som er utformet iht. kontrollpunkter i ISO 27002:2022. Krav til informasjonssikkerhet og personvern skal ivaretas i design, anskaffelse, utvikling, forvaltning og avhending av informasjonssystemer og digital infrastruktur. NSMs Grunnprinsipper for IKT-sikkerhet versjon 2 brukes som mål for laveste akseptable nivå for grunnsikring av digital infrastruktur. I tillegg brukes hendelser og avvik aktivt for å måle oppnåelse innenfor de ulike kravene.

Arbeidet med informasjonssikkerhet er en kontinuerlig prosess og kan deles i tre deler;

d. *Styrende del* angir prinsipper og mål, retningslinjer, og delegert ansvar innen arbeidet med informasjonssikkerhet. Dette er presisert gjennom styringssystemet for informasjonssikkerhet.
e. *Gjennomførende del* består av opplæring, samt å iverksette kravene i styringssystemet for informasjonssikkerhet. På et overordnet nivå handler dette om å ha oversikt over informasjonsverdier, utføre verdivurdering og etablere eierskap til disse, identifisere risiko for informasjonsverdien og iverksette risikoreduserende tiltak til et akseptert nivå av risiko.
f. *Kontrollerende del* består av hendelseshåndtering, avvikshåndtering, rapportering, revisjon og ledelsens gjennomgang.

Som et breddeuniversitet med teknisk-naturvitenskaplig hovedprofil bidrar NTNU til å utvikle Norge ved å skape verdier og danne det teknologiske grunnlaget for fremtidens verdenssamfunn. NTNUs langsiktige forskningsoppdrag krever tillit til at integriteten av forskningsdata og resultater er ivaretatt og kan etterprøves og bygges videre på i fremtiden. Arbeidet med informasjonssikkerhet skal understøtter dette ved å sørge for at integriteten ivaretas, at informasjon som skal være åpen er tilgjengelig, og informasjon som må være konfidensiell er sikret.

Arbeidet med sikkerhetskultur og opplæring understøtter NTNUs mål innen karriere og kompetanse. NTNU skal bidra til at studentene har kompetanse innen informasjonssikkerhet og personvern gjennom tilbud om opplæring, og ved bruk av teknologi som sørger for at studenter ved NTNU

kommer ut og møter utfordringene i samfunnet med kunnskap og gode vaner om hvordan beskytte informasjonsverdier. Gjennom opplæring av studenter og ansatte bidrar NTNU til å øke samfunnssikkerheten. Ved målrettet opplæring for ledere og andre nøkkelfunksjoner skal NTNU øke bevissthet rundt informasjonssikkerhet og sørge for riktig kompetanse i støttefunksjoner.

For å oppnå en bærekraftig digital campus med gode løsninger for arbeidsplasser, læringsarealer, laboratorier og infrastruktur må man ha tillitt hos de som skal benytte løsningene. Da må informasjonssikkerhet være en innebygget og integrert del i tjenesteutvikling, arealutvikling og digitalisering. Med integrert informasjonssikkerhet og personvern vil man også kunne lykkes med å ta i bruk ny muliggjørende teknologi som effektiviserer undervisning, forskning og administrasjon.

7. Roller og ansvar

Arbeidet med informasjonssikkerhet berører virksomheten på alle nivå. Ansvar og myndighet for informasjonssikkerhet skal følge det ordinære linjeansvaret.
Ledere som har ansvar for mål, arbeidsoppgaver og tjenester og prosesser, skal også ha ansvaret for tilhørende informasjonsbehandling og informasjonssikkerhet. Videre er noen roller presisert gjennom styringssystemet for informasjonssikkerhet og er gitt særskilt ansvar for definerte områder.

7.1. Styret

a. er øverste ansvarlig for informasjonssikkerheten og skal årlig orienteres om arbeidet med informasjonssikkerhet
b. er ansvarlig for at det gjennomføres internrevisjon av informasjonssikkerheten ved NTNU

7.2. Rektor

a. er overordnet behandlingsansvarlig for behandling av personopplysninger ved NTNU
b. skal årlig orientere styret om arbeidet med informasjonssikkerhet og personvern

7.3. Direktør for organisasjon og infrastruktur

a. er ansvarlig for at kravene i politikk for informasjonssikkerhet blir implementert i virksomheten gjennom et fungerende styringssystem for informasjonssikkerhet
b. skal påse at det utvikles handlingsplaner som sørger for et systematisk og kontinuerlig arbeid med informasjonssikkerhet
c. skal sørge for tilstrekkelig finansiering av arbeidet med informasjonssikkerhet
d. er ansvarlig for innsamling og rapportering til ledelsens årlige gjennomgang av arbeidet med informasjonssikkerhet til styret
e. skal påse at relevante parter blir varslet ved alvorlige brudd på informasjonssikkerheten
f. er ansvarlig for å iverksette nødvendige tiltak for å sikre en forsvarlig avviksbehandling ved brudd på informasjonssikkerheten
g. skal sørge for at personvernombudet regelmessig blir invitert til å delta i møter med rektor og dekanmøtene
h. er ansvarlig for at Politikk for informasjonssikkerhet revideres hvert andre år for å sikre ønsket effekt og effektivitet i arbeidet med informasjonssikkerhet

7.4. Prorektorer, avdelingsdirektører og seksjonssjefer i Fellesadministrasjonen

a. er ansvarlig for etterlevelsen av krav til informasjonssikkerhet, herunder krav til behandling av personopplysninger ved enheten
b. er ansvarlig for å følge opp at lovverk og rutiner og godkjenninger følges, og at avvik lukkes
c. er ansvarlig for å holde en løpende og oppdatert oversikt over IKT-systemer som anvendes og behandlinger av personopplysninger ved enheten

d. 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 behandlinger, samt melde avvik ved brudd på informasjonssikkerheten
e. er ansvarlig for at alle ansatte innen enheten har tilgang til tjenester og materiell slik at brukerne kan beskytte NTNUs informasjon og informasjonssystemer
f. er ansvarlig for en systematisk gjennomgang av databehandleravtaler og andre avtaler av betydning for informasjonssikkerhetsarbeidet, og gjennomgang av avvik ved avdelingen på minimum årlig basis
g. er ansvarlig for at internkontrollen i informasjonssikkerhetsarbeidet fungerer ved enheten

7.5. Dekan/museumsdirektør

a. er ansvarlig for etterlevelsen av kravene til informasjonssikkerhet, herunder behandlingen av personopplysninger, ved fakultetet/vitenskapsmuseet
b. er ansvarlig for at alle instituttledere er kjent med gjeldende rutiner og retningslinjer i informasjonssikkerhetsarbeidet
c. er ansvarlig for å fastsette nødvendige lokale rutiner ved behov
d. er ansvarlig for å følge opp at lovverk og rutiner og godkjenninger følges, og at avvik lukkes
e. er ansvarlig for å holde en løpende og oppdatert oversikt over IKT-systemer som anvendes og behandlinger av personopplysninger ved fakultet/vitenskapsmuseet
f. er forskningsansvarlig etter helseforskningsloven for eget fakultet og skal ha oversikt over forskningsporteføljen ved fakultetet
g. 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 behandlinger, samt melde avvik ved brudd på informasjonssikkerheten
h. er ansvarlig for at studentene ved NTNU har nødvendig opplæring i kravene til informasjonssikkerhet
i. er ansvarlig for at alle ansatte innen enheten har tilgang til tjenester og materiell slik at brukerne kan beskytte NTNUs informasjon og informasjonssystemer
j. er ansvarlig for å gjennomføre dialog med respektive underliggende enheter om informasjonssikkerhetsarbeidet, herunder oppfølgingen av rutiner og avvik, på minimum årlig basis
k. er ansvarlig for at internkontrollen i informasjonssikkerhetsarbeidet fungerer ved fakultetet/Vitenskapsmuseet

7.6. Instituttleder

a. er ansvarlig for etterlevelsen av kravene til informasjonssikkerhet, herunder behandling av personopplysninger, ved instituttet
b. er ansvarlig for å holde en løpende og oppdatert oversikt over IKT-systemer som anvendes og behandlinger av personopplysninger ved instituttet
c. er ansvarlig for at ansatte er kjent med relevante lover og regler, samt rutiner for informasjonssikkerhet og forskningsetiske retningslinjer
d. er ansvarlig for at ansatte istandsettes til å ivareta sine plikter til å vurdere risiko ved nye prosjekt og behandlinger, samt melder avvik ved brudd på informasjonssikkerheten
e. er ansvarlig for at internkontrollen i informasjonssikkerhetsarbeidet fungerer ved instituttet/enheten

7.7. Leder av Avdeling for virksomhetsstyring

a. er ansvarlig for at informasjonssikkerhet som en av flere virksomhetsområder inngår i en helhetlig internkontroll

b. skal konsulteres når politikk for informasjonssikkerhet revideres for å sikre en helthetlig og effektiv internkontroll

7.8. Leder av HR- og HMS-avdelingen

c. 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
d. skal konsulteres når politikk for informasjonssikkerhet revideres for å sikre en helthetlig tilnærming til sikkerhet og beredskap ved NTNU

7.9. Leder av IT-avdelingen

a. er ansvarlig for å holde en løpende og oppdatert oversikt over NTNUs IKT-infrastruktur, og at informasjonssikkerheten i og mellom systemene ivaretas
b. er ansvarlig for at alle ansatte og studenter ved NTNU har tilgang til tjenester og materiell slik at brukerne kan beskytte NTNUs informasjon og informasjonssystemer
c. er ansvarlig for forvaltningen av NTNUs elektroniske virksomhetssertifikat
d. skal konsulteres når politikk for informasjonssikkerhet revideres for å sikre ønsket effekt og effektivitet i arbeidet med informasjonssikkerhet

7.10. Leder av Seksjon for digital sikkerhet

a. er ansvarlig for gjennomføring av sikkerhetskrav til NTNUs IKT-infrastruktur
b. skal konsulteres når politikk for informasjonssikkerhet revideres for å sikre en helthetlig tilnærming til sikkerhet og beredskap ved NTNU

7.11. Systemeier

a. alle IKT-systemer ved NTNU skal ha en systemeier
b. er ansvarlig for at IT-systemets utvikling, forvaltning og/eller drift møter kravene til informasjonssikkerhet

7.12. Prosjektleder

a. er ansvarlig for det operative ansvaret og internkontroll ved gjennomføringen av forskningsprosjekt og andre prosjekter, fra planlegging til avslutning, herunder at krav i relevant lovverk og forskningsetiske og interne retningslinjer, etterleves
b. er ansvarlig for å sørge for nødvendige godkjenninger og meldinger, samt ansvar for at avtaler som er påkrevet for ivaretakelse av informasjonssikkerheten og personvernet, inngås
c. er ansvarlig for å sørge for tilgangsstyring dersom det er behov for konfidensialitet, f.eks. ved behandling av personopplysninger, i prosjektet
d. ansvarlig for at relevante og nødvendige dokumentasjonskrav ivaretas i prosjektet

7.13. Prosjektveileder/studentveileder

a. er ansvarlig for at studenter i studentprosjekt er gjort kjent med NTNUs rutiner og retningslinjer og overordnet regelverk innen informasjonssikkerhet og behandling av personopplysninger

7.14. Personvernombudet

a. skal gi råd om hvordan NTNU som behandlingsansvarlige best mulig kan ivareta personverninteressene
b. skal på anmodning gi råd om vurdering av mulige personvernkonsekvenser (DPIA)

c. skal kontrollere gjennomføringen av personvernkonsekvensvurderinger
d. skal kontrollere overholdelsen av regelverket
e. skal holde seg informert om og følge opp avvik ved brudd på personvernet
f. skal være kontaktpunkt for Datatilsynet og de registrerte

7.15. Personvernrådgiver for forskning (Sikt personverntjenester)

a. skal gi råd om hvordan NTNU som behandlingsansvarlige best mulig kan ivareta personverninteressene i forskningsprosjekter
b. skal motta meldinger om behandlinger av personopplysninger i forskningsprosjekter og føre protokoll/oversikt over slike behandlinger i et eget meldingsarkiv

7.16. Alle brukere

a. er ansvarlige for å sette seg inn i relevant lovgivning for informasjonssikkerhet, herunder personopplysningsloven samt helseforskningsloven, åndsverksloven og eForvaltningsforskriften
b. er ansvarlige for å gjøre seg kjent med relevante retningslinjer for informasjons-sikkerhetsarbeidet ved bruk av NTNUs IKT-infrastruktur og i forskningsprosjekter og andre prosjekter
c. er pliktige til å melde avvik (uønsket hendelse) ved brudd på informasjonssikkerheten og behandling av personopplysninger i henhold til gjeldende retningslinje for avviksbehandling når de gjøres kjent med slikt

8. Sentrale lover og forskrifter

a. Personopplysningsloven (og personvernforordningen – GDPR) gir regler for vern av fysiske personer i forbindelse med behandling av personopplysninger, plikter for NTNU som behandlingsansvarlig, bruk av personvernombud og rettigheter for den registrerte
b. Forvaltningsloven (og eForvaltningsforskriften) – krav til saksbehandling, dokumentasjon og forsvarlighet, også krav til internkontroll og informasjonssikkerhet
c. Offentleglova – krav om at NTNU som offentlig virksomhet skal være åpen for innsyn, samtidig unnta for innsyn der loven åpner for eller krever det.
d. Arkivloven - inneholder regler om hvilke dokumenter som skal arkiveres og krav til arkiveringen
e. Helseforskningsloven – krav til organisering, roller og ansvar i helseforskning
f. Helseregisterloven og helsepersonelloven – regler om behandling av pasientdata og taushetsplikt for helsepersonell
g. Forskningsetikkloven – regler om at forskning skal skje i henhold til anerkjente forskningsetiske normer, for forsker og institusjon
h. Åndsverkloven - inneholder regler om immaterielle rettigheter og bruk av bilder
i. Beskyttelsesintruksen og sikkerhetsloven – stiller krav til klassifisering og håndtering av informasjon.
j. Eksportkontrolloven – gir regler om kontroll med og forbud mot eksport av strategiske varer, tjenester og teknologi, herunder forbud mot ulovlig kunnskapsoverføring

I tillegg kan andre lover og forskrifter være relevante: ekomloven, politiregisterloven, behandlingsbiobankloven, pasientjournalloven, mv.