# Politikk for informasjonssikkerhet

| | |
|---|---|
| Type dokument | Politikk |
| Forvaltes av | Organisasjonsdirektør |
| Godkjent av | Rektor 20.06.2018 |
| Klassifisering | Åpen |
| Gjelder fra | 20.06.2018 |
| Gjelder til | Frem til revisjon |
| Unntatt offentlighet | Nei |
| Referanse ISO | 27001; 5.1.1, 5.1.2 |
| Referanse LOV/Regel | eForvaltningsforskriften §15 og § 20, personvernforordningen artikkel 5, 24, 32 |
| Referanse interne dokumenter | Politikk for informasjonsvirksomhet er underlagt IKT-reglementet. Politikken er overordnet retningslinjer på informasjonssikkerhetsområdet |

## 1. Formål

Formålet med politikk for informasjonssikkerhet er å ivareta de informasjonsverdier som utvikles, behandles og forvaltes gjennom NTNUs forskning, utdanning, herunder kunstnerisk utviklingsarbeid, formidling, nyskaping og administrasjon, og overholdelse av gjeldende lover og regler. Politikk for informasjonssikkerhet stadfester mål og strategi for informasjonssikkerhet i virksomheten, og setter rammer for arbeidet med ivaretakelse av NTNUs informasjonsverdier og for den digitale sikkerheten i NTNUs IKT-infrastruktur.

Et styringssystem for informasjonssikkerhet skal danne grunnlaget for NTNUs arbeid med informasjonssikkerhet og være en integrert del av NTNUs helhetlige styringssystem. Styringssystemet skal gi rammene for en systematisk og helhetlig praksis mellom styrende, gjennomførende og kontrollerende del av arbeidet med informasjonssikkerhet.

## 2. Hvem NTNUs politikk for informasjonssikkerhet gjelder for

NTNUs politikk for informasjonsvirksomhet gjelder for

- Alle ansatte ved NTNU
- Alle studenter ved NTNU
- Alle som har tilgang til, og/eller bearbeider og forvalter informasjon gjennom NTNUs IKT-infrastruktur

## 3. Sentrale lover og forskrifter på informasjonssikkerhetsområdet

- 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
- Forvaltningsloven (og eForvaltningsforskriften) – krav til saksbehandling, dokumentasjon og forsvarlighet, også krav til internkontroll og informasjonssikkerhet
- Offentleglova – krav om at NTNU som offentlig virksomhet skal være åpen for innsyn, samtidig unnta for innsyn der loven åpner for eller krever det.
- Arkivloven - inneholder regler om hvilke dokumenter som skal arkiveres og krav til arkiveringen
- Helseforskningsloven – krav til organisering, roller og ansvar i helseforskning
- Helseregisterloven og helsepersonelloven – regler om behandling av pasientdata og taushetsplikt for helsepersonell
- Forskningsetikkloven – regler om at forskning skal skje i henhold til anerkjente forskningsetiske normer, for forsker og institusjon
- Åndsverkloven - inneholder regler om immaterielle rettigheter og bruk av bilder
- Beskyttelsesintruksen og sikkerhetsloven – stiller krav til klassifisering og håndtering av informasjon.
- 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.

## 4. Definisjoner

**IKT-infrastruktur:** IKT-infrastruktur: Med NTNUs IKT-infrastruktur menes alt utstyr, digital informasjon, informasjonssystemer og tjenester som benyttes til informasjonsbehandling og kommunikasjon.

**Informasjonssikkerhet:** Informasjonssikkerhet handler om å sikre informasjon ut ifra krav om konfidensialitet, integritet og tilgjengelighet.

**Informasjonsverdier**: Deles inn i to kategorier:

*Primærverdier* handler om hva vi gjør og hvordan, og informasjonen vi benytter:

- forretningsprosesser og aktiviteter
- informasjon

*Sekundærverdier* handler om de verktøyene vi bruker og kompetansen hos de som bruker

verktøyene:

- hardware
- software
- nettverk
- ansatte
- lokasjoner
- organisasjonsstrukturer

**Integritet**: Integritet betyr å sikre at informasjon er korrekt, gyldig og fullstendig og ikke kan endres utilsiktet eller av uvedkommende.

**Internkontroll:** Systematiske styrings- og kontrolltiltak som skal sikre at institusjonens aktiviteter planlegges, organiseres, utføres, sikres og vedlikeholdes i samsvar med krav fastsatt i eller i medhold av lov, og styrende dokumenter.

**Konfidensialitet:** Konfidensialitet betyr å sikre at informasjonen ikke blir kjent for uvedkommende, men at informasjon og informasjonssystemer bare er tilgjengelig for de som har et tjenstlig behov.

**Prosesseier:** En prosesseier er en leder i fellesadministrasjonen, som er ansvarlig for gjennomgående administrative prosesser ved NTNU. Prosesseier har ansvar for felles prosedyrer og retningslinjer samt til enhver tid, styre, forbedre og følge opp de gjennomgående prosessene innen sitt ansvarsområde.

**Risikoeier:** En risikoeier er en leder som er pekt ut som ansvarlig for å nå ett eller flere mål for virksomheten og for å få utført tilhørende arbeidsoppgaver. Risikoeieransvaret følger linjen. I andre kontekster kalles de gjerne mål- og resultatansvarlig, oppgaveeier eller prosesseier.

**Risikostyring:** Risikostyring refererer til et samordnet sett av aktiviteter og metoder som brukes til å lede en organisasjon og å kontrollere de mange risikoene som kan påvirke måloppnåelsen.

**Styringssystem:** Styringssystemet for informasjonssikkerhet ved NTNU følger ISO 27001-standarden, og angir et systematisk arbeid ut fra et sett med styrende dokumenter og prosessbeskrivelser med angitte roller og ansvarsforhold, en aktiv internkontroll og forbedringssløyfer. I praksis fungerer styringssystemet i en tredeling mellom styrende del (ledelseselementet), gjennomførende del (linjen, herunder brukere og prosesseiere) og av kontrollerende del (løpende internkontroll, intern- og ekstern revisjon).

**Systemeier:** En systemeier er en leder som er ansvarlig for å utvikle, forvalte og/eller drifte et informasjonssystem på vegne av NTNU. Systemeier benytter ofte en utpekt systemforvalter som operativt ansvarlig for de oppgaver systemeier har ansvaret for.
En som *oppbevarer* data kan også anses som systemeier. Det vil være i tilfeller der følgende er oppfylt:

- informasjonen tilhører eller er underlagt NTNUs regelverk
- informasjonen benyttes, transporteres eller lagres på
  - IT-systemer
  - personlige enheter
  - annet medium hvor NTNU IT eller linjeleder ikke er systemeier

**Systemeier fellessystem:** En systemeier fellessystem er ansvarlig for å utvikle, forvalte og drifte et informasjonssystem som benyttes av flere risikoeiere i virksomheten

- 

**Tilgjengelighet:** Tilgjengelighet betyr å sikre at informasjon og informasjonssystemer er tilgjengelig ved behov innenfor de tilgjengelighetskrav som er satt.

## 5. Overordnede prinsipper

NTNU skaper, formidler og forvalter informasjonsverdier på vegne av samfunnet, ansatte, studenter og samarbeidspartnere. NTNU skal ivareta konfidensialitet, integritet og tilgjengelighet til informasjonsverdiene i henhold til gjeldende lover, forskrifter, føringer fra myndighetene, samfunnsoppdraget og informasjonseiernes interesser.

NTNU skal ha oversikt over sine informasjonsverdier, og hvilke personopplysninger som behandles. Ved behandling av personopplysninger stiller regelverket (personopplysningsloven) krav til informasjonssikkerheten. Ved behandling av personopplysninger aksepteres ikke brudd på konfidensialiteten og integriteten.

Informasjonssikkerhet er et gjennomgående risikoområde som må håndteres innen alle NTNUs virksomhetsområder. Arbeidet med informasjonssikkerhet skal bygge på prosesser for kontinuerlig forbedring. NTNU skal ivareta informasjonssikkerheten som en integrert del av øvrig virksomhetsstyring og gjennom sitt systematiske kvalitetsarbeid.

Risikostyring og aksept av risiko er et lederansvar. Ved all informasjonsbehandling foreligger det en risiko for brudd på konfidensialitet, integritet og tilgjengelighet. Risikoaksept og tiltak skal stå i forhold til sannsynligheten for og konsekvensen av sikkerhetsbrudd. Restrisiko skal være

akseptert av ledelsen.

Internkontroll og sikkerhetsarbeid skal så langt det er hensiktsmessig være integrert på tvers av internkontrollområder. Det skal gjennomføres sikkerhetsrevisjoner som verifiserer at NTNU og eksterne myndigheters krav til informasjonssikkerhet er ivaretatt og fungerer etter sin hensikt. Sikkerhetsrevisjoner skal gjennomføres hvert andre år.

## 6. Sikkerhetsmål

NTNU har vedtatt følgende mål for informasjonssikkerheten:

- Informasjonssikkerhet skal være en integrert og en naturlig del i alle prosesser, tjenester og systemer ved NTNU.
- Informasjonsverdiene som behandles innen NTNUs virksomhetsområder forskning, utdanning, nyskaping, formidling og administrasjon skal vurderes og håndtereres slik at informasjonen sikres og personvernet ikke krenkes.
- Informasjonsverdienes konfidensialitet, integritet og tilgjengelighet skal ha riktig sikkerhetsnivå basert på klassifisering og risikovurderinger. Registrertes rettigheter, herunder forskningsdeltakeres rettigheter, skal sikres. Offentlighetens rett til innsyn etter offentleglova skal ivaretas.
- Alle ansatte, studenter, og øvrige som har tilgang til, og/eller bearbeider og forvalter informasjon gjennom NTNUs IKT-infrastruktur, skal være kjent med og etterleve NTNUs krav til informasjonssikkerhet.

## 7. Sikkerhetsstrategi

Styringssystemet for informasjonssikkerhet ved NTNU utformes og implementeres etter ISO 27001-standarden. Med hensiktsmessige tilpasninger sikres det at arbeidet med informasjonssikkerhet følger relevante lover og regler og beste praksis på området på en måte som vil fungere for NTNU som organisasjon. Arbeidet med informasjonssikkerhet skal operasjonaliseres gjennom en helhetlig arbeidsflyt mellom en styrende, gjennomførende og kontrollerende del:

*Styrende del* angir krav, føringer, organisering og roller for arbeidet med informasjonssikkerhet. Dette er presisert gjennom de styrende dokumenter for informasjonssikkerhet; IKT-reglementet, Politikk for informasjonssikkerhet og underliggende retningslinjer.

*Gjennomførende del* består av linjelederes, prosesseieres, systemeieres og brukeres gjennomføring av kravene i de styrende dokumentene for informasjonssikkerhet. På et

overordnet nivå handler dette om klassifisering av informasjon, risikovurderinger og risikoreduserende tiltak innenfor de respektive ansvarsområder.

*Kontrollerende del* består av avvikshåndtering, rapportering, intern/ekstern revisjon og ledelsens gjennomgang.

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

1. *Styring og kontroll med informasjonssikkerheten* er et lederansvar og en del av den ordinære virksomhetsstyringen og internkontrollen. Ledere skal ha en god risikoforståelse og oversikt over de informasjonsverdier som enheten håndterer, slik at de er i stand til å ta informerte valg og gjøre prioriteringer ved innføring av sikkerhetstiltak.

2. *Arbeidet med sikkerhetskultur og opplæring* skal være en systematisk og kontinuerlig forbedringsprosess. Økt kompetanse skal gjøre ansatte og studenter i stand til å klassifisere informasjonen de behandler, gjennomføre risikovurderinger og velge nødvendige tiltak for å beskytte informasjonen i arbeidsprosessene.

3. *NTNU skal sikre IKT-infrastrukturen* gjennom en systematisk implementering av kravene i retningslinjene som er utformet iht. kontrollpunkter i ISO 27001, Tillegg A. Krav til informasjonssikkerhet og personvern skal ivaretas i design, anskaffelse, utvikling, forvaltning og avhending av IKT-systemer og infrastruktur.

## 8. Roller og ansvar

Arbeidet med informasjonssikkerhet berører virksomheten på alle nivå. Ansvar og myndighet for informasjonssikkerhet skal følge det ordinære linjeansvaret.

Alle IKT-systemer ved NTNU skal ha en systemeier.

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.

## 8.1. Styret

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

## 8.2. Rektor

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

## 8.3. Organisasjonsdirektør

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

## 8.4. Prorektorer, direktører og avdelingsledere i Fellesadministrasjonen

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

- 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
- er ansvarlig for at alle ansatte innen enheten har tilgang til tjenester og materiell slik at brukerne kan beskytte NTNUs informasjon og informasjonssystemer
- 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
- er ansvarlig for at internkontrollen i informasjonssikkerhetsarbeidet fungerer ved enheten

### 8.5. Dekan/museumsdirektør

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

## 8.6. Instituttleder

- er ansvarlig for etterlevelsen av kravene til informasjonssikkerhet, herunder behandling av personopplysninger, ved instituttet
- er ansvarlig for å holde en løpende og oppdatert oversikt over IKT-systemer som anvendes og behandlinger av personopplysninger ved instituttet
- er ansvarlig for at ansatte er kjent med relevante lover og regler, samt rutiner for informasjonssikkerhet og forskningsetiske retningslinjer
- 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
- er ansvarlig for at internkontrollen i informasjonssikkerhetsarbeidet fungerer ved instituttet/enheten

## 8.7. Leder av Avdeling for virksomhetsstyring

- er ansvarlig for at informasjonssikkerhet som en av flere virksomhetsområder inngår i en helhetlig internkontroll
- skal konsulteres når politikk for informasjonssikkerhet revideres for å sikre en helthetlig og effektiv internkontroll

## 8.8. Leder av HR- og HMS-avdelingen

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

## 8.9. Leder av IT-avdelingen

- er ansvarlig for å holde en løpende og oppdatert oversikt over NTNUs IKT-infrastruktur, og at informasjonssikkerheten i og mellom systemene ivaretas
- 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
- er ansvarlig for forvaltningen av NTNUs elektroniske virksomhetssertifikat
- skal konsulteres når politikk for informasjonssikkerhet revideres for å sikre ønsket effekt og effektivitet i arbeidet med informasjonssikkerhet

## 8.10. Leder av Seksjon for digital sikkerhet

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

## 8.11. Systemeier

- er ansvarlig for at IT-systemets utvikling, forvaltning og/eller drift møter kravene til informasjonssikkerhet

## 8.12. Prosjektleder

- 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
- 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
- er ansvarlig for å sørge for tilgangsstyring dersom det er behov for konfidensialitet, f.eks. ved behandling av personopplysninger, i prosjektet
- er ansvarlig for at relevante og nødvendige dokumentasjonskrav ivaretas i prosjektet

## 8.13. Prosjektveileder/studentveileder

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

## 8.14. Personvernombudet

- skal gi råd om hvordan NTNU som behandlingsansvarlige best mulig kan ivareta personverninteressene
- skal på anmodning gi råd om vurdering av mulige personvernkonsekvenser (DPIA)
- skal kontrollere gjennomføringen av personvernkonsekvensvurderinger
- skal kontrollere overholdelsen av regelverket
- skal holde seg informert om og følge opp avvik ved brudd på personvernet
- skal være kontaktpunkt for Datatilsynet og de registrerte

## 8.15. Personvernvernrådgiver for forskning (Norsk senter for forskningsdata - NSD)

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

## 8.16. Alle brukere

- er ansvarlige for å sette seg inn i relevant lovgivning for informasjonssikkerhet, herunder personopplysningsloven samt helseforskningsloven, åndsverksloven og eForvaltningsforskriften
- 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
- 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