NTNUs IKT-reglement

Type dokument	Reglement
Forvaltes av	Direktør for organisasjon og infrastruktur
Godkjent av	Direktør for organisasjon og infrastruktur
Klassifisering	Åpen
Gjelder fra	25.02.2025
Neste revisjon innen	25.02.2027
Referanse ISO	ISO 27002:2022; 5.4, 6.2, 6.4
Referanse NSMs grunnprinsipper for IKT-sikkerhet	
Referanse LOV/Regel	eForvaltningsforskriften § 20, personvernforordningen artikkel 24, 32, Lov om statens ansatte, Universitets- og høyskoleloven
Referanse interne dokumenter	Politikk for Informasjonssikkerhet og personvern, Retningslinjer innen informasjonssikkerhet og personvern

1. Formål

Formålet med IKT-reglementet er å regulere bruken av NTNUs informasjons- og kommunikasjonsinfrastruktur (IKT-infrastruktur).

2. Hvem NTNUs IKT-reglement gjelder for

IKT-reglementet gjelder for:

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

2.1 Virkeområde

Med NTNUs IKT-infrastruktur menes alt utstyr, digital informasjon, informasjonssystemer og tjenester som benyttes til informasjonsbehandling og kommunikasjon.
Privateid utstyr som koples til datanettet er omfattet av reglementet. Når programvare eller informasjon som eies av NTNU installeres på privat utstyr, er også dette omfattet av reglementet.

3. Overordnede prinsipper

3.1 Tilgang til NTNUs IKT-infrastruktur

Studenter og ansatte skal ha en brukerkonto hos NTNU. Med brukerkonto menes unikt brukernavn, passord og en e-postkasse. Andre kan gis tilgang til IKT-infrastruktur etter tjenstlig behov. Tilgang til de ulike systemer og tjenester autoriseres av systemeier.

3.2 Bruk av IKT-infrastruktur

a. Den som gis tilgang til NTNUs IKT-infrastruktur (heretter kalt bruker) plikter å sette seg inn i IKT-reglementet og å følge det. Brukeren plikter også å sette seg inn i og følge underliggende politikker, retningslinjer og prosedyrer som er tilgjengelig på Innsida[1][2].
b. NTNUs IKT-infrastruktur skal brukes til å utføre oppgaver knyttet til NTNUs virksomhet. NTNUs IKT-infrastruktur skal anvendes på en måte som ikke strider mot lov, forskrift eller NTNUs interne regler.
c. Bruker skal hindre at andre får tilgang til egen brukerkonto. Bruker skal heller ikke søke å skaffe seg tilgang til andres brukerkonto.
d. Bruker skal hindre at uønskede personer får tilgang til NTNUs IKT-infrastruktur, herunder tilgang til rom hvor IKT-utstyr er tilgjengelig. Bruker skal ikke uten tillatelse endre, modifisere eller på annen måte forårsake at IKT-infrastrukturen virker på en annen måte enn forutsatt.
e. Bruker skal ikke benytte NTNUs IKT-infrastruktur på en måte som kan utsette NTNU for tap av omdømme.
f. NTNUs IKT-infrastruktur skal kun benyttes til å understøtte aktiviteter som bidrar til å oppnå universitets formål og oppgaver knyttet til forskning, utdanning, herunder kunstnerisk utviklingsarbeid, nyskaping, formidling og administrasjon.
g. Bruker skal påse at den enkeltes personvern overholdes og ikke krenkes.
h. Bruker plikter å respektere opphavsrett eller lignende rettigheter til programvarer, tjenester og annen digital informasjon som bilder, musikk, og film etc.
i. Lisensiert programvare, tjenester, åndsverk eller andre rettighetsbelagte data skal bare benyttes i henhold til bruksavtale, og bruker plikter å sette seg inn i de reglene som gjelder for bruken. Bruker kan holdes ansvarlig for brudd på vilkårene.
j. Publisering av andres verk, informasjon eller data må bare gjøres etter avtale med rettighetshaveren.
k. Ved lengre fravær, skal bruker legge inn fraværsmelding slik at virksomhetsrelatert epost ikke blir liggende uhåndtert i e-postkassen.
l. Bruker plikter straks å rapportere forhold som kan ha betydning for IKT-infrastrukturens sikkerhet eller integritet (avvik) til IT-avdelingen, ved Seksjon for digital sikkerhet.
m. Behandle all informasjon forsvarlig iht styringssystemet for informasjonssikkerhet og personvern

[1] https://i.ntnu.no/wiki/-/wiki/Norsk/Politikk+for+informasjonssikkerhet
[2] https://i.ntnu.no/wiki/-/wiki/Norsk/Informasjonssikkerhet+-+retningslinjer

3.3 Avslutning av ansettelsesforhold eller studier, mv.

I god tid innen opphør av ansettelsesforhold eller avslutning av studier ved NTNU, skal brukeren rydde sin konto. Filer som tilhører saker som en ansatt har hatt til behandling, skal forelegges brukers/den ansattes overordnede til vurdering. Filene skal ikke slettes før brukers fakultet eller enhet har godkjent dette. Den ansatte skal sørge for at filer som ikke tilhører bestemte saker, forelegges nærmeste overordnede som avgjør om filene skal slettes eventuelt arkiveres.

3.4 Avslutning av bruker og e-postkasse mv.

a. Når arbeidsforhold, studierett eller annen form for tilknytning til NTNU opphører, stenges brukertilgangen til NTNUs IKT- infrastruktur. Varsel om dette gis per e-post en måned i forveien. For brukere tilknyttet Gjestetjenesten tilpasses varselet etter lengden på oppholdet.
b. Ved avskjedigelse eller suspensjon skal tilganger til IKT-infrastruktur trekkes med umiddelbar virkning. Er det behov for å hente ut personlig informasjon eller annen relevant informasjon skal dette skje etter avtale med nærmeste leder og gjøres under oppsyn.
c. Innhold i e-postkasse og personlige lagringsområder slettes permanent senest seks måneder etter at tilgangen stenges. For studenter, slettes de personlige lagringsområdene to måneder etter at studieretten opphørte.
d. Ved dødsfall blir brukerkonto sperret. E-postkassen og det private hjemmeområdet og dets innhold slettes etter seks måneder med mindre offentlige myndigheter eller andre har fremlagt særskilt hjemmel for innsyn.

3.5 Tilbakelevering av materiell til NTNU

a. Materiell tilhørende NTNU skal leveres tilbake. Alle kopier av programvare, dokumentasjon og data eid av, eller utlånt fra NTNU, skal slettes på privat utstyr.
b. Retten til å knytte opp private maskiner til NTNUs nettverk opphører ved avslutning av ansettelsesforhold eller studier.

3.6 Identifikasjon og tilgangsstyring

a. Tilgang til NTNUs IKT-infrastruktur skal være knyttet til en rolle og med påfølgende rettigheter.
b. Den som skal ha tilgang til NTNUs IKT-infrastruktur skal identifisere seg ved hjelp av godkjent digital identitet(er)som er knyttet til rollen.

3.7 Endring av rolle eller avslutning av forholdet til NTNU

a. Ved endring av rolle i tilknytningen til NTNU skal endringer av rettigheter i IKT-infrastrukturen endres tilsvarende. Når forholdet til NTNU avsluttes (studenter uteksamineres, ansatte slutter) skal tilganger og rettigheter trekkes tilbake. Etter en karantenetid skal persondata slettes.
b. Den som benytter den digitale identiteten har selv ansvar for å ta vare på personlige data, samt overlevere NTNUs data i henhold til dette IKT-reglementet og gjeldende avtale som gir tilgang til NTNUs IKT-infrastruktur.

3.8 Kontroll med bruken av NTNUs IKT-infrastruktur

a. All bruk av NTNUs IKT-infrastruktur etterlater elektroniske spor. NTNU samler inn, analyserer og oppbevarer elektroniske spor for å administrere IKT-infrastrukturen, sikre effektiv og kostnadsbærende drift, og for å beskytte NTNUs IKT-infrastruktur mot trusler og misbruk. Innsamling, lagring og bruk av elektroniske spor skal gjøres i henhold til gjeldende lovverk.
b. NTNUs IKT-infrastruktur er tilrettelagt med løsninger for registrering av aktiviteter (logging) og sikkerhetskopiering blant annet for å kunne dokumentere lovbrudd eller avvik fra interne regler og rutiner, men også for å kunne avdekke/oppdage brudd på sikkerheten i IKT-infrastrukturen.
c. IT-avdelingen har hovedansvar for kontroll med tilgang til NTNUs nettverk og generelle IKT-tjenester.

3.9 Innsyn

a. NTNU har som arbeidsgiver innen rammen av regelverket[3], rett til innsyn i arbeidstakers e-postkasse og brukerkonto mv. Arbeidstaker så langt mulig skal varsles og få anledning til å uttale seg før innsyn gjennomføres, og arbeidstaker skal som hovedregel ha rett til å være til stede under innsynet. Arbeidstaker har rett til å la seg bistå av tillitsvalgt eller annen representant.
b. Dersom innsyn er foretatt uten forutgående varsel, skal arbeidstaker etterpå få skriftlig underretning om innsynet. Beslutning om og gjennomføring av innsyn skal dokumenteres i NTNUs sak- og arkivsystem.
c. Innsynet må gjennomføres på en slik måte at dataene så langt som mulig ikke endres og at frembrakte opplysninger kan etterprøves.
d. NTNU har bare rett til å gjennomsøke, åpne eller lese e-post i arbeidstakers e-postkasse eller hjemmeområde, mv. i følgende tilfeller:
    i. Når det er nødvendig for å ivareta den daglige driften eller andre berettigede interesser ved virksomheten.
    ii. Når det er begrunnet mistanke om at arbeidstakers bruk av e-postkassen medfører grovt brudd på de plikter som følger av arbeidsforholdet, eller kan gi grunnlag for oppsigelse eller avskjed[4].
e. Dersom innsyn i e-postkassen viser at det ikke foreligger dokumentasjon som arbeidsgiver har rett til innsyn i, skal e-postkassen og dokumenter i denne straks lukkes. Eventuelle kopier skal slettes.
f. Beslutning om innsyn i ansattes e-postkasse fattes av øverste leder ved enheten (dekan eller avdelingsdirektør). Det samme gjelder ved dødsfall der innsyn er nødvendig for å finne frem virksomhetsrelatert e-post og annet knyttet til brukerkonto.

[3] https://lovdata.no/dokument/SF/forskrift/2018-07-02-1108
[4] https://www.datatilsynet.no/personvern-pa-ulike-omrader/personvern-pa-arbeidsplassen/innsyn-epost-filer/?print=true

g. NTNU kan gi innsyn i informasjon, logger og sikkerhetskopier til offentlige myndigheter når dette har hjemmel i lov eller forskrift, samt ved fremleggelse av rettslig beslutning.

3.10 Reaksjoner og sanksjoner ved brudd på IKT-reglementet

a. Brudd på IKT-reglementet og/eller underliggende politikkdokument, retningslinjer, prosedyrer, og rutiner kan føre til reaksjoner eller sanksjoner mot brukeren.
b. Brukeren er ansvarlig for å sette seg inn i hvilke styrende dokumenter og instruksjoner som er gjeldende for sin bruk av IKT-infrastrukturen. Oversikt over relevante dokumenter er tilgjengelig på NTNUs nettsider.[5]
c. Utstyr eller programvare som forårsaker skade på NTNUs IKT-infrastruktur, på NTNUs informasjon/data, andre brukeres informasjon/data, som på annen måte skaper forstyrrelser i IKT-infrastrukturen eller er til hinder oppnåelse av NTNUs formål med IKT-infrastrukturen, kan umiddelbart og uten forvarsel fjernes fra IKT-infrastrukturen.
d. Ansatte som begår brudd på IKT-reglementet, kan få arbeidsrettslige reaksjoner i form av en advarsel eller sanksjoner i form av suspensjon etter lov om statsansatte § 29.
e. Studenter som begår brudd på IKT-reglementet, kan utestenges helt eller delvis fra NTNUs IKT-infrastruktur etter universitets- og høyskoleloven. Utestenging ut over 14 virkedager anses som et enkeltvedtak for en student, og må følge saksbehandlingsreglene i forvaltningsloven.
f. Beslutning om reaksjoner og sanksjoner mot ansatte besluttes av øverste leder ved grunnenheten, eller dekan dersom bruker er student. Beslutningen skal skje i samråd med systemeier.
g. Klage på vedtak truffet med hjemmel i lov om statsansatte eller universitets- og høyskoleloven følger lovens regler om klage.
h. Gjestebrukere som begår brudd på IKT-reglementet, følges opp av ansvarlig oppdragsgiver. Konsekvensene av brudd reguleres av oppdragsavtalen eller tjenesteavtalen, ev. av avtalerettslige regler.

4. Roller og ansvar

Ansvar for IKT-reglementet har blitt delegert fra Styret til Direktør for organisasjon og infrastruktur gjennom Rektor[6].

4.1 Direktør for organisasjon og infrastruktur

a. Reviderer IKT-reglementet hvert annet år.
b. Skal fremlegge IKT-reglementet for rektor for fastsettelse ved revisjoner eller endringer som vil kunne påvirke brukernes rettigheter og plikter.

4.2 Leder av IT-avdelingen

a. Leder av IT-avdelingen iverksetter utestengning av tilgang til NTNUs IKT-infrastruktur.

[5] Informasjonssikkerhet for ansatte - NTNU
[6] Delegasjonreglement Del 1, pkt 4.1 og Del 2 pkt 3.1

4.3 Ansettelsesmyndigheten

a. Fatter beslutning om sanksjoner mot ansatte i henhold til Lov om Statens ansatte[7] og Personalreglement for hhv vitenskapelig personale og teknisk-administrativt personale[8].

4.4 Dekan/Museumsdirektør/Avdelingsdirektør

a. Er ansvarlig for at studenter er gjort kjent med IKT-reglementet, og at dette aksepteres skriftlig (elektronisk) før de får tilgang til NTNUs IKT-infrastruktur.
b. Fatter beslutning om utestenging inntil 14 dager av NTNUs IKT-infrastruktur som sanksjon mot student ved brudd på IKT-reglementet.
c. Fatter formelt vedtak om utestenging utover 14 dager av NTNUs IKT-infrastruktur som sanksjon mot student ved brudd på IKT-reglementet.
d. Fatter formell beslutning om innsyn i brukers e-postkasse, mv.

4.5 Linjeleder

a. Er ansvarlig for at ansatte er gjort kjent med IKT-reglementet, og at dette aksepteres skriftlig (elektronisk) før de får tilgang til NTNUs IKT-infrastruktur.
b. Følger opp at avvik innen informasjonssikkerhet og personvern meldes i avvikssystemet iht. «Retningslinje for avviksmelding og avvikshåndtering innenfor informasjonssikkerhet og personvern».

4.6 Brukere

a. Brukere er ansvarlig for å sette seg inn i IKT-reglementet og øvrige regler for bruken av NTNUs IKT-infrastruktur, og følge dette.
b. Brukere skal sørge for at brudd på retningslinjer innen informasjonssikkerhet og personvern meldes uten ugrunnet opphold til nærmeste leder og/eller i NTNUs avvikssystem.

[7] https://lovdata.no/dokument/NL/lov/2017-06-16-67
[8] https://innsida.ntnu.no/wiki/-/wiki/Norsk/Personalreglement