Retningslinje for Nettverks- og informasjonsoverføring

Type dokument	Retningslinje
Forvaltes av	Leder av IT-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 5.14, 8.12, 8.21 – 8.23
Referanse NSMs grunnprinsipper for IKT-sikkerhet	2.3.10, 2.5.1-2.5.6, 2.5.8, 2.7.4
Referanse LOV/Regel	Personopplysningsloven, Eksportkontrolloven
Referanse interne dokumenter	Denne retningslinjen er underlagt Politikk for informasjonssikkerhet

1. Formål

Formålet med retningslinjen er å beskytte informasjon mot tap eller misbruk ved overføring mellom interne systemer ved NTNU, elektronisk overføring av informasjon til ekstern part, eller overføring av informasjon til andre medier som kan benyttes til å lagre data (lagringsmedier) som ikke er en del av NTNUs beskyttede IKT-infrastruktur. Med NTNUs IKT-infrastruktur menes alt utstyr, digital informasjon, informasjonssystemer og tjenester som benyttes til informasjonsbehandling og kommunikasjon.

2. Gjelder for

«Retningslinjen for nettverks- og informasjonsoverføring» gjelder for alle som har tilgang til, og/eller bearbeider og forvalter informasjon gjennom NTNUs nettverk.

3. Overordnede prinsipper

a. Det skal implementeres tiltak for å øke evnen til å detektere angrep, samt redusere angrepsflaten i nettverket.
b. Informasjon i transaksjoner til og fra applikasjonstjenester skal beskyttes for å hindre ufullstendig overføring, feilruting, uautorisert meldingsendring, uautorisert utlevering, uautorisert meldingsduplisering eller repetering.
c. Ved bruk av eksterne systemer skal det inngås en databehandleravtale godkjent av virksomhetsstyring.
d. Forskning og kunnskap som kan misbrukes skal underlegges eksportkontroll iht. Eksportkontrolloven og reguleres av «Retningslinjer for kontroll med kunnskapsoverføring»[1].

[1] https://www.regjeringen.no/no/tema/utenrikssaker/Eksportkontroll/om-eksportkontroll/kunnskap/id2500543/

e. Ved verbal kommunikasjon utenfor NTNUs lokaler må deltakere være bevisst sine omgivelser og innhold i kommunikasjon slik at ikke klassifisert informasjon kommer på avveie.

4. Nettverk

4.1 Nettverkskontroller

NTNUs datanett er definert som datanettet som eies og driftes av NTNU på alle Campus. Inkludert i dette er kjernenettverk og alle nettverkskomponenter som er koblet til det. Det inkluderer også alle internettforbindelser inn og ut av NTNU, samt eventuelt leide linjer mellom NTNU og partnere. For å sikre tilgangen til dette nettverket skal følgende kontroller være implementert:

a. Klientnettverk skal ha autentisering både på kablet og trådløst nett. (IEEE 802.1x).
b. Brannmurer skal benyttes for å kontrollere trafikken i nettverket, inkluderer også brannmurer på servere.
c. Logger fra brannmuren skal håndteres etter krav i «Retningslinje for Operativ Sikkerhet».
d. Ekstern tilgang til nettverkssonene Intern, Fortrolig og Strengt fortrolig skal gå via kryptert forbindelse med sikker autentisering som kan realiseres ved hjelp av f.eks. VPN og/eller Microsoft Direct Access. Løsningene må ha to-faktor autentisering for å hindre at man kan logge på bare med brukernavn og passord.

4.2 Sikring av nettjenester

Følgende tiltak skal være implementert for å sikre NTNUs datanett:

a. Nettverksutstyr skal sikres fysisk basert på krav i «Retningslinje for fysisk sikring av IKT-infrastruktur».
b. Nettverkskomponenter skal konfigurasjonsstyres slik at man til enhver tid har et oppdatert nettverk.
c. Det skal etableres redundante forbindelser der kravene til tilgjengelighet krever dette.
d. Kvaliteten på nettverkstjenesten skal være tydelig definert enten det leveres av NTNU IT eller av eksterne leverandører.

4.3 Segregering i nettverk

Segregering av nettverkene er en forutsetning for å kunne oppnå en høyre grad av informasjonssikkerhet. Følgende krav stilles:

a. Brukerutstyr skal isoleres i egne soner. Der det er mulig eller hensiktsmessig bør klienter også skilles fra hverandre for å unngå at klienter infiserer hverandre. (Private VLAN)
b. Nettverket skal kunne isolere brukerutstyr som er kompromittert.
c. Nettverket skal ha egne soner for brukerutstyr med forskjellige sikkerhetsnivå basert på følgende inndeling:
    - Ukjente enheter – ved kun åpen informasjon
    - Private enheter som er registrert – ved opptil intern informasjon
    - Administrerte enheter – ved opptil fortrolig informasjon
    - Administrerte enheter med høyere tilgangsstyring – ved opptil strengt fortrolig informasjon
d. Servere skal plasseres i nettverkssoner basert på klassifisering av informasjon.
e. Det skal være egne nettverkssoner for åpen, intern, fortrolig og strengt fortrolig informasjon.
f. Segregeringen av nettverket skal kontrolleres gjennom brannmurer.
g. Nettverkstrafikk fra servere i intern, fortrolig og strengt fortrolig sone skal bare nå internett via Proxy.
h. Labutstyr skal plasseres i egen sone og skal ikke nås direkte fra internett.

5. Informasjonsoverføring

a. All informasjonsoverføring med informasjon klassifisert som Fortrolig og Strengt Fortrolig skal ha mekanismer for å verifisere integritet.
b. Transaksjoner av informasjon klassifisert som Fortrolig eller Strengt Fortrolig skal krypteres eller sikres på annen måte for å ivareta informasjonssikkerheten[2].
c. Det skal være audit logging av transaksjoner som inneholder personopplysninger og informasjon klassifisert Fortrolig eller Strengt Fortrolig. Loggen skal oppfylle krav til sporing av endringer og innsyn.
d. Ved overføring av avtaleregulert/lovregulert informasjon til en ekstern part skal det alltid foreligge en data- eller informasjonsbehandleravtale

5.1 Elektronisk meldingsutveksling

Ved overføring via e-post eller annet elektronisk meldingssystem gjelder følgende krav:

a. Fortrolig eller Strengt Fortrolig informasjon som overføres via e-post eller andre elektroniske meldingstjenester skal krypteres i henhold til «Retningslinje for bruk av kryptografiske kontroller».

5.2 Konfidensialitets- eller taushetserklæringer

Følgende krav gjelder for konfidensialitets- eller taushetserklæringer ved behandling av klassifisert informasjon:

a. Ved overføring av informasjon klassifisert Intern, Fortrolig eller Strengt Fortrolig til en ekstern part skal det foreligge en signert avtale som ivaretar NTNUs rettigheter og forpliktelser knyttet til informasjonsoverføringen.
b. Medarbeidere i NTNU skal pålegges taushetsplikt for personopplysninger hvor konfidensialitet er nødvendig.
c. Taushetsplikten skal også omfatte annen informasjon med betydning for informasjonssikkerheten.

6. Roller og ansvar

6.1 Leder av IT-avdelingen

a. er ansvarlig for at kravene i «Retningslinje for nettverk og informasjonsoverføring» blir implementert i virksomheten

6.2 Leder av HR- og HMS-avdelingen

a. er ansvarlig for at NTNU har etablert tilfredsstillende taushetserklæringer som ivaretar krav til informasjonssikkerhet i henhold til denne retningslinjen
b. er ansvarlig for at ledere er kjent med, og har tilstrekkelig kompetanse, til å ivareta sitt ansvar i henhold til denne retningslinjen

6.3 Leder av Seksjon for IT-drift

a. er ansvarlig for utarbeidelse av rutiner for som ivaretar informasjonssikkerheten i alle faser av IKT-drift
b. er ansvarlig for at systemene driftes og avvikles i henhold til denne retningslinjen

[2] Retningslinje for bruk av kryptografiske kontroller

6.4 Leder av Seksjon for Digital Sikkerhet

a. er ansvarlig for å stille krav til sikring av informasjon i nettverket eller informasjon som overføres til andre
b. er ansvarlig for å legge føringer for å sikre nettverket
c. er ansvarlig for komme med tiltak for å redusere sårbarheten i nettverket

6.5 Linjeleder

a. er ansvarlig for at taushetserklæringer benyttes i sin enhet i henhold til kravene i denne retningslinjen

6.6 Systemeier

a. er ansvarlig for at systemene der vedkommende er systemeier utvikles, implementeres, driftes og avvikles i henhold til kravene i denne retningslinjen

6.7 Prosjektleder

a. er ansvarlig for at taushetserklæringer benyttes i prosjektet i henhold til kravene i denne retningslinjen
b. er ansvarlig for at informasjon som overføres i prosjektperioden er sikret i henhold til denne retningslinjen