Retningslinje for Tilgangskontroll

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	ISO27002:2022 5.10, 5.15-5.18, 5.23, 6.5, 6.7, 7.1-7.4, 7.6, 7.8, 8.2, 8.4, 8.5, 8.21
Referanse NSMs grunnprinsipper for IKT-sikkerhet	1.3.1, 1.3.2, 2.2.6, 2.3.7, 2.4.1, 2.6.1-2.6.7
Referanse LOV/Regel	
Referanse interne dokumenter	Politikk for informasjonssikkerhet

1. Formål

Formålet med denne retningslinjen er å sette premisser for tilgangskontroll til NTNU sine informasjonsressurser for å hindre urettmessig tilgang. Retningslinjen er uavhengig av medium og om det gjelder digital tilgangskontroll eller fysisk adgangskontroll til lokasjoner hvor informasjon lagres, prosesseres eller overføres.

2. Gjelder for

Retningslinje for tilgangskontroll gjelder for alle med tilgang og/eller adgang til ett eller flere informasjonssystem som eies, utvikles, driftes eller forvaltes av NTNU.

3. Overordnede prinsipper

a. Adgang og tilgang til NTNUs digitale infrastruktur skal være forankret i et behov for å få utført en pålagt oppgave og tildeles etter minste privilegiums prinsipp (least privilege).
b. NTNU skal ha adgangs- og tilgangskontroll som står i forhold til skaden uautorisert tilgang kan medføre.
c. Adgang og tilgang til NTNUs digitale infrastruktur skal være sporbar.
d. Fjernaksess skal begrenses til godkjente systemer.

4. Implementasjon av tilgangskontroll

4.1 Tilgang til informasjon og informasjonssystemer

a. NTNU skal benytte en sentral identitetsdatabase for digital identitet. En identitetsdatabase er en sentral database som inneholder digitale identiteter fra autorative kilder definert i dette dokumentet. Ved NTNU er følgende systemer autoritative for identitetshåndtering:
    i. FS for identitetshåndtering av studenter

ii. Personal- og lønnssystem for identitetshåndtering av ansatte
iii. Egen sentral database (må opprettes) for eksterne identiteter

b. NTNU skal benytte en sentral database for å tildele identiteter en rolle. BAS skal være autoritativt system for roller og rollebasert tilgangskontroll.
c. Gjestetilgang til NTNUs IKT-infrastruktur skal godkjennes av kontorsjefer eller faggruppeledere.
d. NTNU skal benytte ressursdomener for tilgangskontroll til informasjonsressurser hvor tilgang tildeles basert på gruppetilhørighet av rollen i sentral database (BAS). NTNU skal benytte følgende masterkilder for tilgangskontroll i ressursdomener:
   i. Microsoft Active Directory (WIN-NTNU-NO)
   ii. LDAP (at.ntnu.no)
e. Systemeier definerer hvilke roller eller systemer som skal ha tilgang til informasjonssystemet eller informasjonen som lagres, prosesseres eller overføres via systemet.
f. Krav til logging av adgang og tilgang skal være i henhold til klassifisering av informasjon innenfor de tre områdene konfidensialitet, integritet og tilgjengelighet.

4.2 Brukerforvaltning

Ryddig og systematisk brukerforvaltning er avgjørende for å kunne implementere en sikker rollebasert tilgangskontroll. Feil innen bruker- og identitetsforvaltning vil forplante seg nedover i systemer for adgangskontroll og tilgangskontroll. NTNU definerer derfor følgende prinsipper for hvordan brukerforvaltning skal implementeres i organisasjonen:

a. NTNU skal ha personlige brukerkontoer for alle ansatte, studenter og eksterne. Brukerkonto skal være personlig og ikke deles med andre.
b. NTNU skal ha en rutine for å tildele en person en brukerkonto som sørger for at personens identitet er korrekt før utstedelse av en brukerkonto på NTNU sine systemer.
c. NTNU kan ha egne systembrukere for applikasjoner og tjenester der dette er nødvendig. Disse brukerne skal låses ned til hvilke systemer og tjenester de kan benyttes på.
d. Privilegert tilgang til tjenester, applikasjoner og systemer skal gis etter prinsippet av «need-to-use» basert på tilgang som trengs for å utføre en bestemt funksjon til en gitt rolle. Med privilegerte tilganger menes det her root/tjeneste kontoer på Unix/Linux maskiner, administrator/tjeneste-kontoer på Windows maskiner, systemkontoer i databaser, systemkontoer på nettverksutstyr, applikasjoner og kommunikasjonskanaler mm.
e. Privilegert tilgang skal godkjennes av nærmeste leder gjennom en autorisasjon og skal tidsbegrenses så mye som mulig.
f. Makstid på privilegert tilgang er på 3 år, da må personen re-autoriseres.
g. Midlertidig tilgang skal avgrenses i tid og rom så mye som mulig og gis med en makstid på 1 år.
h. Brukere med privilegerte tilgang på NTNUs tjenester, applikasjoner og systemer skal identifiseres og dokumenteres i en sentral database og knyttes til enten en identitet eller en prosess.
i. Privilegert tilgang skal tildeles en egen brukerkonto som er dedikert til formålet eller oppgaven.
j. Privilegert tilgang på systemer og applikasjoner kan tildeles vanlige brukerkontoer dersom tilgangskontroll til systemet eller applikasjonen benytter multi-faktor autentisering.

4.3 Brukere og autentisering

For å sikre effektiv tilgangskontroll til NTNUs informasjonsressurser stilles følgende krav til de (brukere) som benytter og administrerer disse på NTNUs vegne.

a. NTNU stiller krav til at brukere holder personlige passord eller annet som private kryptografiske nøkler, sertifikater og lignende strengt fortrolig og ikke deler disse med andre.
b. Autentiseringsinformasjon (som passord) skal være unikt for NTNU sine tjenester. Gjenbruk av passord i fra personlige tjenester skal ikke forekomme.
c. Brukere må aktivere sin egen brukerkonto og sette et eget passord før tjenester ved NTNU kan benyttes.
d. Personlige brukere skal sette sine egne passord igjennom https://bas.ntnu.no
e. Passord skal ikke skrives ned eller lagres digitalt på en slik måte at det kan knyttes til en NTNU brukerkonto dersom det kommer på avveie. Unntak er ved bruk av et godkjent passordhvelv (Password manager).
f. NTNU krever at brukere bytter passord hvert andre år eller ved:
    - mistanke om at brukerkonto er på avveie
    - pålegg fra leder for Seksjon for Digital sikkerhet
g. Krav til lengde og kompleksitet av passord ved NTNU:
    - Systembruker: Minimum 30 tegn med høy kompleksitet, dvs store og små bokstaver, tall og spesialtegn.
    - Domeneadministrator: Minimum 20 tegn med høy kompleksitet
    - Systemadministrator: Minimum 20 tegn med medium kompleksitet, dvs store og små bokstaver og tall.
    - Klientadministrator: Minimum 20 tegn med medium kompleksitet
    - Brukere: Minimum 12 tegn med medium kompleksitet

4.4 Autentiseringsmekanismer

Autentiseringsmekanismer er programmer eller rutiner som definerer eller kontrollerer brukeres og/eller brukergruppers tilgang til en maskin eller til en gitt informasjon. For å ha effektiv tilgangskontroll ved NTNU må mekanismer for autentisering av brukere, systemer og tjenester implementeres på en sikker måte for å hindre at autentiseringen kan omgås og dermed gi tilgang til intern, fortrolig eller strengt fortrolig informasjon eller misbruk av NTNUs informasjonsressurser. NTNU stiller følgende krav til autentiseringsmekanismer:

a. All autentisering skal alltid foregå over sikker forbindelse (for eksempel ved bruk av TLS). En sikker forbindelse er en forbindelse der både konfidensialitet og integritet er ivaretatt i kommunikasjonen.
b. Autentiseringsinformasjon skal kun valideres etter at all informasjon er mottatt i systemet og ved autentisering skal ikke systemet gi informasjon om hvilke autentiseringsdata som er korrekt eller feil.
c. Autentiseringsmekanismer skal ha innebygget funksjonalitet som begrenser mulighet for systematisk gjetting av autentiseringsdata.
d. Informasjon som har klassifiseringsnivå 4[1] skal aksesseres med multifaktor iht. sikkerhetsnivå 3[2]. Multifaktor (eller flerfaktor) autentisering er når en bruker må oppgi flere separate uavhengige bevis for sin identitet. Dette kan være for eksempel være en kombinasjon av et passord og engangskode.
e. Tjenester, systemer og applikasjoner skal som standard ikke vise system eller applikasjonsidentifiserende informasjon før autentisering er vellykket.

[1] Retningslinje for klassifisering av informasjon
[2] https://eid.difi.no/nb/sikkerhet-og-informasjonskapsler/ulike-sikkerhetsniva

f. Bannere skal legges til som identifiserer hvem som eier systemet og en advarsel om at det kun er for autentiserte brukere.
g. Autentiseringsmekanismen skal loggføre alle vellykkete og forfeilede forsøk på autentisering.
h. Autentiseringsmekanismer skal logge en sikkerhetsevent dersom et forsøk på eller et vellykket innbrudd forekommer.
i. Logging skal gjøres til en sentral loggtjeneste. Dette gjelder også skybaserte mekanismer.
j. Standard innstilling for autentiseringsmekanismer skal ikke vise passord i klartekst i passordfelt, men med unntak av verifikasjonskode for engangspassord eller andre midlertidige mekanismer.
k. Autentiserte inaktive sesjoner skal som standard alltid utløpe etter en hensiktsmessig gitt tid, men med unntak av sesjoner i fra forhåndsgodkjente lokasjoner eller systemer.
l. Autentiseringsmekanismer skal lagre passord eller annen autentiseringsdata adskilt i fra applikasjon.
m. Standard passord satt av leverandør på utstyr skal alltid byttes før utstyret tas i bruk og kobles til NTNUs infrastruktur.
n. Midlertidige passord eller autentiseringsmekanismer skal genereres unikt for hver tilgang.
o. Midlertidige passord eller autentiseringsmekanismer skal formidles til bruker igjennom en sikker forbindelse hvor mottaker bekrefter at melding er mottatt.

4.5 Programvare for systemdrift og administrasjon

Følgende krav gjelder for programvare som benyttes til administrasjon av tjenester, applikasjoner og systemer slik som verktøy for konfigurasjonsstyring, brukeradministrasjon og andre systemverktøy:

a. Verktøy som brukes for systemadministrasjon skal være identifisert og benytte autentisering
b. Verktøy for systemadministrasjon skal segregeres i fra øvrige applikasjoner.
c. Verktøy for systemadministrasjon skal begrenses til privilegerte administratorkontoer etter prinsipper for privilegert tilgang.
d. All bruk av verktøy for systemadministrasjon skal logges på sentral logg-tjeneste.
e. Alle verktøy for systemadministrasjon som ikke benyttes til drift av tjeneste, applikasjon eller system skal deaktiveres eller avinstalleres hvis hensiktsmessig.
f. Verktøy for systemadministrasjon skal ikke være tilgjengelig for brukere som ikke er autorisert for å drive systemadministrasjon.

4.6 Nettverk, systemer og tjenester på NTNU

Det stilles krav for å få tilgang til, og administrasjon av, nettverk, systemer og tjenester som inngår i NTNUs IKT-infrastruktur. Med NTNUs IKT-infrastruktur menes alt utstyr, digital informasjon, informasjonssystemer og tjenester som benyttes til informasjonsbehandling og kommunikasjon. En skytjeneste er i praksis en forlengelse av NTNUs IKT-infrastruktur.

a. Det skal benyttes tofaktorautentisering for tilgang til eksternt tilgjengelige tjenester i NTNUs IKT-infrastruktur.
b. Nettverk, systemer og tjenester skal ha tilgangskontroll basert på klassifisering for å beskytte informasjon og informasjonsressurser mot uautorisert tilgang.
c. NTNU kan ha systemspesifikke rutiner for hvem som er autorisert for tilgang til gitte nettverk, systemer og tjenester. Disse rutiner skal ta utgangspunkt i klassifisering og defineres av systemansvarlig.
d. NTNU skal ha hensiktsmessig tilgangskontroll til nettverk, systemer og tjenester basert på klassifisering og risiko og sårbarhetsvurdering.

e. Interne systemer skal kun være tilgjengelig og nåes via et Virtual Private Network (VPN) eller lignende løsninger godkjent av seksjon for digital sikkerhet.
f. Applikasjoner skal isoleres fra hverandre der det er mulig.
g. Tilgang til å administrere systemer med sikkerhetsnivå 3[3] eller høyere skal kun gjøres i fra dedikerte arbeidsstasjoner, nettverk eller servere som er godkjent av leder for Seksjon for digital sikkerhet for formålet.

4.7 Tilgangskontroll til kildekode

Det settes krav gjeldene for tilgangskontroll for kildekode og deler av informasjonssystemene som NTNU har utviklet. For kildekoden til sentrale komponenter gjelder dette:

a. Basert på klassifisering skal kildekode og biblioteker ha tilgangskontroll og begrenses til kun autoriserte personer. Dette gjelder spesielt for:
   - kjernesystemer for dataflyt, autentisering og andre kritiske tjenester i NTNU
   - kildekode som er opphavsrett beskyttet
   - kildekode for NTNU som har autentiseringsdata i klartekst eller annen sensitiv informasjon
b. All kildekode som er tilgangskontrollert skal ha:
   - sentral logg av alle endringer
   - sentral logg av all tilgang

4.8 Fysisk sikring av arealer som gir tilgang til NTNUs informasjonsverdier

For å kunne ivareta informasjonssikkerheten skal sikring av fysiske arealer følge kravene under:

a. Områder som inneholder IKT-infrastruktur og/eller informasjon som krever beskyttelse skal inndeles i soner.
b. Sonene skal beskyttes med hensiktsmessige adgangskontroller for å sikre at kun autorisert personell får adgang.
c. Ved vurdering av adgangskontroll og autorisasjon skal det tas hensyn til hvilken informasjon og hvilket utstyr som er plassert i aktuelt område iht. til gjeldende rutine.
d. Alt personell skal kunne tilkjennegi sin identitet når de er i NTNUs områder med adgangsbegrensninger. Referert til tabellen i under betyr det områder med **GUL**, **RØD** og SORT klassifisering til alle tider og for områder med **GRØNN** klassifisering når skallsikringen er aktivisert.

Sikringsnivå	Sikring
SORT Begrensede deler av datarom, datasystemer, arkivrom eller andre rom som gir tilgang til informasjon som det er kritisk for NTNU å beskytte mot uautorisert innsyn eller endring. SORT område skal ligge innenfor RØDT område.	Sort sone skal etableres inne i et område som er definert som rød sone, og som har tilfredsstillende skallsikring. Avlåst hele døgnet. Adgangskort + PIN kode eller nøkkel med svært begrenset tilgang. Eksterne skal kun gis tilgang etter særskilt avtale, opplæring i NTNUs krav til informasjonssikkerhet, signert taushetserklæring og under oppsyn av autorisert NTNU ansatt. Alle skal bære synlig adgangskort. Det stilles krav til alarmsystem til dør, samt bevegelsessensor på innsiden og videoovervåkning av inngang. Rommet skal være tilstrekkelig merket, samt ha instruksjon hvis man ønsker adgang.

[3] Ulike sikkerhetsnivå | eid.difi.no

	Det skal gjennomføres årlig gjennomgang av ROS-analyse for kartlegging av sikringstiltak av arealet. Ved gjennomgang skal følgende revideres: • Adgang ved hendelser som brann, terror, etc • Revisjon av adgang
RØD Avgrensede områder hvor spesiell autorisasjon kreves, datarom/arkiver med fortrolig informasjon, og/eller informasjon som det er viktig for NTNU å beskytte mot uautorisert innsyn eller endringer. RØD sone skal etableres i en GUL sone.	Avlåst hele døgnet. Adgangskort + PIN kode eller nøkkel med begrenset tilgang. Eksterne skal kun gis tilgang etter særskilt avtale og opplæring i NTNUs krav til informasjonssikkerhet. Taushetserklæring skal signeres. Alle skal bære synlig adgangskort. Det stilles krav til alarmsystem til dør. Rommet skal være tilstrekkelig merket. Det skal gjennomføres årlig ROS-analyse for kartlegging av sikringstiltak av arealet. Ved gjennomgang skal følgende revideres: • Adgang ved hendelser som brann, terror, etc • Revisjon av adgang
GUL Arealer der det kan aksesseres informasjon klassifisert som Intern. Kontorer, møterom, kopirom, mv. der det er adgangskontroll hele døgnet.	Lås og personlig nøkkelkort + PIN kode. Eksterne skal kun gis tilgang etter særskilt avtale og signert taushetserklæring. For printerrom der rommet er plassert i grønn sone kan printerrom være gul sone ved utskrift av Fortrolig informasjon. Det kreves da sikker utskriftsfunksjonalitet for printeren/ utskriftssystemet.
GRØNN Offentlig tilgjengelige områder: Vrimleområder, korridorer, kantiner mv. I prinsippet alt åpent.	Skallsikring for bygninger utenom åpningstid og eventuelle ekstra sikkerhetstiltak der det ansees som nødvendig, f. eks videoovervåking mv. Sikringstiltakene baseres på ROS-vurdering og aktiva plassert i lokalene.

5. Roller og ansvar

5.1 Direktør for Organisasjon og infrastruktur

a. skal konsulteres ved endringer på retningslinje for tilgangskontroll

5.2 Leder av Avdeling for virksomhetsstyring

a. er ansvarlig for at arbeidet med tilgangskontroll er underlagt intern/ekstern revisjon for å sikre at det oppnås ønsket effekt med riktig bruk av ressurser (effektivitet)

5.3 Leder av IT-avdelingen

a. skal konsulteres ved endringer på retningslinje for tilgangskontroll
b. er ansvarlig for at prinsipper og krav definert i retningslinje for tilgangskontroll etterleves i IT-avdelingen

5.4 Leder av HR- og HMS-avdelingen

a. skal konsulteres ved endringer av retningslinje for tilgangskontroll
b. er ansvarlig for at linjeledere er kjent med, og har tilstrekkelig kompetanse, til å ivareta sitt ansvar i henhold til retningslinje for tilgangskontroll
c. skal sørge for gode rutiner for forvaltning av roller og identitet og at dette er innarbeidet i relevante prosesser

5.5 Leder av Seksjon for digital sikkerhet

a. er ansvarlig for at retningslinje for tilgangskontroll er i samsvar med nødvendige krav til å ivareta sikker aksess til NTNUs IKT-infrastruktur
b. er ansvarlig for å midlertidig overstyre tildelte aksessrettigheter i situasjoner hvor dette er nødvendig for å ivareta sikkerheten i NTNUs IKT infrastruktur
c. er ansvarlig for å rapportere på effekt og effektivitet knyttet til tiltak som gjennomføres for å beskytte mot uautorisert tilgang til, angrep og/eller trusler mot NTNUs IKT-infrastruktur

5.6 Linjeleder

a. skal sørge for at det utføres korrekt registrering og forvaltning av roller og identiteter innenfor sitt ansvarsområde
b. skal sørge for at det utføres korrigeringer og fjerning av tilgang etter prinsipper og krav nedsatt i denne retningslinjen innenfor sitt ansvarsområde
c. skal sørge for at tilgang til beskyttelsesverdig informasjon forvaltes etter prinsipper og krav nedsatt i denne retningslinjen følges innenfor sitt ansvarsområde

5.7 Systemeier

a. skal konsulteres ved endring av retningslinje for tilgangskontroll
b. er ansvarlig for at prinsipper og krav definert i retningslinje for tilgangskontroll etterfølges og implementeres på systemer denne er ansvarlig for
c. er ansvarlig for å definere hvilke roller som skal ha tilgang til systemet denne er eier av