Retningslinje for Operativ sikkerhet

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
Klassifisering	Åpen
Referanse ISO	ISO27002:2022 5.8, 5.21, 5.23, 5.30, 7.5, 7.11, 7.12, 8.6-8.9, 8.12-8.17, 8.19, 8.20, 8.25-8.34
Referanse NSMs Grunnprinsipper for IKT-sikkerhet	1.1.5, 1.2.1-1.2.4,2.1.1-2.1.3, 2.1.5-2.1.9, 2.2.1-2.2.5,2.2.7,2.3.1-2.3.6,2.3.9 ,2.4.3,2.8.3,2.8.4,2.9.1-2.9.4, 2.10.1-2.10.4, 3.1.1, 3.1.3, 3.2.1-3.2.7
Referanse LOV/Regel	
Referanse interne dokumenter	Denne retningslinjen er underlagt IKT-reglementet og Politikk for informasjonssikkerhet

1. Formål

Formålet med denne retningslinjen er å sikre stabil og sikker utvikling og drift av NTNUs informasjonssystemer, samt mulighet til å detektere problemer i IKT-infrastrukturen. Dette skal gjøres ved å øke kvaliteten og sikre tjenestene som NTNU leverer gjennom målrettede tiltak og krav.

2. Gjelder for

Retningslinje for operativ sikkerhet gjelder for alle som har tilgang til, drifter og forvalter NTNUs informasjonssystemer, tjenester og utstyr (NTNUs IKT-infrastruktur).

3. Overordnede prinsipper

a. Systemer direkte tilkoblet fastnettet skal være oppdatert og driftet av NTNU IT eller fagnær IT ved institutt.
b. Systemer som står permanent på fastnettet skal logge til sentral loggløsning.
c. Systemer tilkoblet fastnett som er midlertidig skal ha et definert tidspunkt for avvikling.
d. Systemer i produksjon, test og utvikling skal være tilstrekkelig dokumentert for sikker drift og bruk.
e. Utvikling og test av systemer skal foregå i separate løsninger med egen rutine som beskriver overføring mellom utvikling, test og produksjon.
f. NTNU skal ha et helhetlig system for både aktiv og passiv monitorering av IKT-infrastruktur, systemer og tjenester.
g. NTNU skal iverksette tiltak som detekterer, beskytter mot og støtter sentral håndtering av uønsket programvare og skadevare.
h. Det kan pålegges tiltak og krav utover denne retningslinjen for å ivareta sikkerheten basert på risiko og trusselvurderinger.
i. Passordlevetid på API-er skal endres jevnlig, minimum hvert 2. år.

4. Dokumentasjon

NTNU skal ha en samlet oversikt over alle systemer og tjenester i produksjon, samt en oversikt over alle systemer og tjenester som er i test og/eller utvikling. Denne oversikten skal minimum inneholde programvare, operativsystem og maskinvare, samt klassifisering og systemeier.

4.1 Systemdokumentasjon og driftsprosedyrer

Systemdokumentasjonen skal beskrive hvordan systemet eller tjenesten er implementert, samt inneholde standard driftsrutiner -prosedyrer i tillegg til tilhørende brukerdokumentasjon der det er relevant. NTNU skal ha systemdokumentasjon for alle systemer som er i produksjon, samt alle funksjons- og/eller virksomhetskritiske systemer i test og/eller utvikling.

Følgende krav gjelder:

a. Systemdokumentasjon skal beskrive oppsett av systemer og tjenester som ivaretar NTNUs retningslinjer for informasjonssikkerhet.
b. Systemdokumentasjon for et system skal omfatte signifikante elementer systemet er bygget opp av, og avhengighetsforholdet mellom disse elementene.
c. Systemdokumentasjonen skal jevnlig vedlikeholdes og oppdateres når det utføres endringer.
d. Systemdokumentasjonen skal være av en slik kvalitet at man skal kunne gjenbygge systemet eller tjenesten samt benytte den til feilsøking ved hendelser.
e. Informasjon om system(er) med link til dokumentasjon skal til enhver tid være oppdatert i IT Service Portal.

4.2 Brukerdokumentasjon

a. Brukerdokumentasjon bør beskrive sikker og anbefalt bruk av NTNUs informasjonssystemer som ivaretar NTNUs retningslinjer for informasjonssikkerhet.

5. Sikker utvikling

a. Kravene til informasjonssikkerhet for et IKT-system gjelder uavhengig om systemet utvikles gjennom skreddersøm, eller om det er tilpasninger i et standardisert IKT-system.
b. Rutiner for prosjektering, utvikling og forvaltning av IKT-systemer ved NTNU skal være basert på anbefalt veileder fra Datatilsynet for utvikling av programvare med innebygd personvern iht. sjekkliste.[1]

a. Ledere for avdelinger som prosjekterer, anskaffer, utvikler og/eller forvalter IKT systemer ved NTNU skal kunne dokumentere hvordan de systematisk har tilnærmet seg anbefalingene for sikker utvikling innen hvert av områdene i Datatilsynets veileder for programvareutvikling med innebygd personvern. Alternativt skal det være utviklet og implementert en tilsvarende systematikk for alle punktene som er relevant for eget ansvarsområde.
b. Utvikling, test og produksjon skal foregå i separate, adskilte løsninger.
c. NTNU skal etablere hensiktsmessig fysisk og logisk sikring av utviklingsmiljøer for systemutvikling som dekker hele utviklingsprosessen.
d. Utvikling og test relatert til informasjonssystemer med informasjon klassifisert på nivå 3 eller 4 iht. NTNUs «Retningslinje for klassifisering av informasjon» skal foregå på dedikerte og sikrede nett.

[1] Sjekkliste https://www.datatilsynet.no/regelverk-og-skjema/veiledere/programvareutvikling-med-innebygd-personvern/.

e. Systemer i test eller utvikling skal ikke tilkobles internett dersom det ikke finnes særskilte krav til unntak.
f. Produksjonsdata som inneholder personopplysninger skal ikke overføres til utvikling eller test med mindre man har hjemmel for å gjøre dette.
g. Sensitive data skal ikke overføres til utvikling uten at det er foretatt en risikovurdering og at denne er godkjent av risikoeier.
h. Autentiseringsmekanismer og brukere i test og utvikling skal være adskilt fra produksjon og skal i tillegg være kontrollert og sporbart.
i. NTNU skal føre tilsyn med og overvåke aktivitet forbundet med utkontraktert systemutvikling får å sikre at krav til informasjonssikkerheten ivaretas.

6. Drift og monitorering

6.1 Endringsstyring (Change management)

Endringsstyring er en etablert prosess for å styre endringer i tjenester, systemer og applikasjoner som driftes av NTNU. Prosessen skal baseres på ITIL rammeverket. For å ivareta informasjonssikkerheten skal følgende krav til endringsstyring etterleves:

a. NTNU skal ha endringsstyring på alle systemer i produksjon.
b. NTNU skal registrere endringer som kan påvirke sikkerheten
c. NTNU skal ha rutine som beskriver overføring fra utvikling til test og fra test til produksjon.
d. NTNU skal ha en rutine for endringsstyring av signifikante endringer på IKT-systemer.
e. NTNU bør ha endringsstyring på systemer i test og utvikling.

6.2 Kapasitetsstyring (Capacity management)

For å unngå at ressurser opptas unødvendig stilles det krav til kapasitetsstyring:

a. ved gitte intervaller skal ressursforbruk, systemer og tjenester behovsprøves for å avdekke hva som kan avvikles eller om noe må konsolideres.
b. det skal eksistere prosedyrer for å avvikle system/tjeneste, optimalisering og frigjøring av ressurser, samt rydding og sikker sletting av data

6.3 Konfigurasjonsstyring (Configuration Management)

Det er viktig at komponenter i tjenester og systemer er sentralt konfigurert og oppdatert. Følgende krav stilles:

a. Konfigurasjonsstyringen skal baseres på FitSM for konfigurasjonsstyring.
b. Systemer og applikasjoner i produksjon skal styres via sentrale konfigurasjonsverktøy.
c. Avhending av IT-Utstyr skal følge rutine for avhending av lagringsmedium.

6.4 Teknisk sårbarhetsstyring

For å kunne beskytte informasjon og digital-infrastruktur så skal det etableres en prosess for sårbarhetsstyring. Følgende krav stilles:

a. NTNU skal ha en rutine for teknisk sårbarhet- og angrepsflate monitorering.
b. NTNU skal utføre risikovurdering av sårbarheter (Vulnerability risk assessment) og implementere nødvendige tiltak for å begrense risiko for negativ effekt for organisasjonen.
c. NTNU skal ha rutiner for sikkerhetsoppdatering av operativsystemer, programvare og maskinvare på alt utstyr som er koblet til eller er en del av NTNUs digitale infrastruktur.

d. Systemer direkte tilkoblet fastnettet eller som er permanent tilkoblet NTNUs nettverk skal ha sentral sårbarhetsmonitorering der mulig.

6.5 Beskyttelse mot fysiske hendelser

a. Arealer som inneholder infrastruktur som representerer høy sårbarhet/risiko for tilgjengeligheten til kritiske eller større deler av NTNUs informasjonskilder skal ha fysisk beskyttelse mot naturkatastrofer, sabotasje og ulykker.
b. For arealer som inneholder infrastruktur som representerer høy sårbarhet/risiko for tilgjengeligheten til kritiske eller større deler av NTNUs informasjonskilder skal det være utarbeidet og testet en kontinuitetsplan som inntrer ved kritiske hendelser.
c. Kabler for strøm og data skal beskyttes mot avlytning og skade.

6.6 Beskyttelse mot skadevare

NTNU skal ha tiltak som detekterer, beskytter mot og støtter sentral håndtering av uønsket programvare og skadevare. Følgende krav gjelder:

a. NTNU skal vurdere tiltak mot skadevare fortløpende basert på risiko og sårbarhetsvurderinger, samt trusselbildet mot NTNU.
b. NTNU skal ha oppdatert og sentralt styrt antiskadevare agent på alle klienter, servere og enheter som er permanent tilkoblet nettverket.
c. NTNU krever at enheter som kobler seg til nettverket skal ha installert sikkerhetsoppdateringer og har oppdatert skadevarebeskyttelse.

6.7 Sikkerhetskopiering

Det er krav til at det er etablert sikkerhetskopiering der dette er nødvendig for å ivareta informasjonssikkerheten. Følgende krav stilles:

a. Det skal etableres sikkerhetskopiering basert på systemets klassifisering og eksterne eller interne krav til sikkerhetskopiering.
b. Sikkerhetskopiering må sikres slik at det ikke lagres i samme rom eller i nærheten av systemet det tas sikkerhetskopiering av.
c. Det skal være mulig å foreta kryptert sikkerhetskopiering dersom klassifisering tilsier dette.
d. Løsningen for sikkerhetskopiering må støtte differensierte sikkerhetsnivå.
e. Sikkerhetskopier skal ha tilgangskontroll som følger prinsipper og krav i retningslinje for tilgangskontroll.
f. Tilgang til sikkerhetskopiert data skal loggføres.
g. Sikkerhetskopiering skal fungerer hensiktsmessig og i henhold til driftsrutiner verifiseres regelmessig.
h. Det skal regelmessig gjennomføres test av gjenoppretting i fra sikkerhetskopi.
i. Programvare definert som kritisk for virksomheten iht. “Retningslinje for klassifisering av informasjonsobjekter” skal sikkerhetskopieres for å kunne sikre gjenoppretting.

6.8 Logginnsamling og systemmonitorering (Event management)

Effektiv og sikker drift av IKT-infrastruktur er avhengig av å vite status på systemer, tjenester og infrastrukturen som helhet for å kunne avdekke unormal aktivitet eller avvik i fra normal drift. NTNU skal ha et helhetlig system for både aktiv og passiv monitorering av IKT-infrastruktur, systemer og tjenester. Logg og monitorering er basis for operativ sikkerhet og god tjenestekvalitet.

6.8.1 Logging ved NTNU

a. Alle systemer som permanent står på NTNUs nettverk skal logge til sentral loggløsning.
b. Lokal kopi av loggen skal oppbevares i 7 dager.
c. Logger skal analyseres sentralt for å kunne avdekke feil, tilgjengelighets- og sikkerhetshendelser.
d. Innsamling, prosessering og lagring av system- og applikasjonslogger skal gjøres på en egen sentral plattform. Denne plattformen skal være adskilt i fra andre systemer og være plassert i NTNUs datasenter.
e. Alle systemer/tjenester tilkoblet NTNU sitt fastnett skal sørge for å ha korrekt tid og dato, og benytte NTNUs nettverksbaserte tidsserver.
f. Logger skal lagres kryptert på maskinvare adskilt fra andre IT-systemer med streng tilgangsstyring.

6.8.2 Driftsmonitorering ved NTNU

a. NTNU skal ha sentral driftsmonitorering av systemer og applikasjoner som er i produksjon.
b. Systemer som er i produksjon skal minimum monitorere:
    - ytelse og ressursforbruk (CPU, Disk, Båndbredde etc.)
    - status på tjenester av en slik kvalitet at det kan brukes til å beregne tjenestekvalitet
c. Sentral monitoreringsplattform skal være uavhengig andre systemer.

7. Roller og ansvar

7.1 Leder av IT-avdelingen

a. er ansvarlig for at kravene i «Retningslinje for operativ sikkerhet» blir implementert i virksomheten
b. er ansvarlig for å rapportere på gjennomføringsgrad, effekt og effektivitet i arbeidet med sikker utvikling

7.2 Leder av HR- og HMS-avdelingen

a. er ansvarlig for at ledere er kjent med og har tilstrekkelig kompetanse til å ivareta sitt ansvar i henhold til denne retningslinjen

7.3 Leder av Seksjon for digital sikkerhet

a. er ansvarlig for at enheten har tilstrekkelig med kompetanse og verktøy for å ivareta kravene i «Retningslinje for operativ sikkerhet»
b. er ansvarlig for systemer og rutiner for teknisk sårbarhetsstyring i virksomheten
c. er ansvarlig for å opprette et sentralt loggsystem i virksomheten
d. er ansvarlig for å tilby sentrale løsninger for skadevarebeskyttelse i virksomheten
e. er ansvarlig for sentral sikkerhetsmonitorering og analyse
f. er ansvarlig for å godkjenne endringer som kan påvirke sikkerheten til NTNU
g. kan pålegge organisasjonen ytterlige sikkerhetstiltak utenom det som er nevnt i denne retningslinjen basert på trussel og risikovurdering.

7.4 Leder av seksjon for IT-utvikling

a. er ansvarlig for utarbeidelse av rutiner for som ivaretar informasjonssikkerheten i alle faser av IKT-utvikling

b. er ansvarlig for at medarbeidere har kompetanse til å møte kravene til sikker utvikling iht. denne retningslinjen

7.5 Leder av Seksjon for IT-drift

a. er ansvarlig for at enheten har tilstrekkelig med kompetanse og verktøy for å ivareta kravene i «Retningslinje for operativ sikkerhet»
b. er ansvarlig for sentral driftsmonitorering for virksomheten
c. er ansvarlig for sikkerhetskopiering av fellessystemer og infrastruktur
d. er ansvarlig for å implementere pålagte sikkerhetskontroller i infrastrukturen innen rimelig tid og uten ubegrunnet opphold.

7.6 Leder av seksjon for IT-forvaltning

a. er ansvarlig for utarbeidelse av rutiner for som ivaretar informasjonssikkerheten i alle faser av IKT-forvaltning
b. er ansvarlig for at medarbeidere har kompetanse til å møte kravene til sikker utvikling iht. denne retningslinjen

7.7 Leder av Seksjon for IT-Brukerstøtte

a. er ansvarlig for at enheten har tilstrekkelig med kompetanse og verktøy for å ivareta kravene i «Retningslinje for operativ sikkerhet»

7.8 Leder av Seksjon for Økonomirådgivning

a. er ansvarlig for utarbeidelse av rutiner for som ivaretar krav til informasjonssikkerheten ved inngåelse leverandøravtaler og i avtaleforvaltning

7.9 Systemeier

a. er ansvarlig for krav til regelmessig kvalitetssikring av informasjonssikkerheten i hele IKT-systemets livssyklus
b. er ansvarlig for at systemer og tjenester leveres i henhold til kravene i retningslinjen
c. er ansvarlig for at systemet er registrert i NTNUs sentrale oversikt over IT-systemer – IT-service Portal
d. er ansvarlig for at dokumentasjonen er oppdatert og korrekt
e. ansvarlig for at krav til funksjonalitet og brukergrensesnitt til IT-systemet ikke bryter med kravene til informasjonssikkerhet
f. er ansvarlig for at det finnes relevant opplæringsmateriale for sikker og effektiv bruk av systemet
g. er ansvarlig for at IT-systemet er underlagt internkontroll

7.10 Systemforvalter

a. er ansvarlig for at systemet blir forvaltet iht. de krav til informasjonssikkerhet som systemeier har dokumentert i IT-service Portal og i annen tilgjengelig dokumentasjon knyttet til utvikling, drift og forvaltning
b. skal bistå med råd og innhold til opplæring, samt sørge for at denne er tilgjengelig der relevant
c. skal påse at all utvikling, drift og forvaltning skjer i henhold til gjeldende retningslinjer for disse områdene
d. ansvarlig for akseptansetest før IT-systemet settes i produksjon, herunder utarbeidelse av kriterier, testplan og gjennomføring av akseptansetest

7.11 Systemutvikler

a. er ansvarlig for sikker koding, med et særlig ansvar for å teste, avdekke og rapportere avvik eller mistenkt sårbarhet