NTNU
Norges teknisk-naturvitenskapelige
Universitet

Prinsipper for informasjonssikkerhet ved NTNU

Innledning

Det overordnede dokumentet *Policy for Informasjonssikkerhet ved NTNU* beskriver hvilket formål NTNUs ledelse har med sitt arbeid for informasjonssikkerhet og hvilke konkrete mål som settes for denne sikkerheten. Dokumentet finnes også som vedlegg til dette dokumentet.

Dette dokumentet – *Prinsipper for informasjonssikkerhet ved NTNU* beskriver ansvar og roller i forhold til informasjonssikkerhet og fastlegger de overordnede prinsippene for ivaretakelse og vedlikehold av informasjonssikkerheten ved NTNU.

Rutiner for implementering av prinsippene er gitt i egne dokumenter. I prinsippdokumentet er de overordnede rutinene og andre interne styrende og utførende dokumenter for informasjonssikkerhet referert i *kursiv*.

Dokumentet inneholder ikke et eget avsnitt med referanser. Alle referanser er i stedet samlet i et eget dokument, *Referanser for informasjonssikkerhet ved NTNU*. Dette er gjort for å lette vedlikeholdet av prinsippdokumentet. Referansedokumentet vil inneholde en oppdatert liste over rutinene for implementering av sikkerhetsprinsippene, referanser til offentlige lover og forskrifter og en liste over andre dokumenter som er viktig for arbeidet med informasjonssikkerhet ved NTNU. For dokumenter som er tilgjengelig på nett oppgis nettreferansen.

NTNUs interne styrende og utførende dokumenter for informajsonssikkerhet finnes via NTNUs webside for sikkerhet. Kapittel/punkt 10 - Referanser inneholder nettadresse til NTNUs websider for sikkerhet, Policydokumentet, Prinsippdokumentet og Referansedokumentet.

1 Risikostyring

Risikovurdering

1.1 NTNU skal ha en tilnærming til informasjonssikkerhet basert på risikovurderinger.

1.2 NTNU skal løpende analysere risikoer og vurdere behovet for beskyttelsestiltak som beskrevet i NTNUs rutiner for risiko og sårbarhetsanalyse.

1.3 Risikovurderingen skal identifisere risiko og prioritere tiltak i forhold til kriterier for akseptabel risiko som er fastsatt av NTNU.

1.4 Risikovurderinger skal gjennomføres ved endringer som har betydning for informasjonssikkerheten.

Håndtering av risiko

1.5 Ved identifisering av uakseptabel risiko, iverksettes tiltak for å redusere risiko til et akseptabelt nivå.

1.6 Tiltak skal vurderes med hensyn til effektivitet, kostnad, praktisk gjennomførbarhet og med utgangspunkt i NTNUs rolle som utdannings- og forskningsinstitusjon.

2 Sikkerhetsorganisasjon - ansvar og roller

2.1 Rektor har som øverste faglige og administrative leder ansvaret for informasjonssikkerheten ved NTNU.

2.2 Som eier av policyen og prinsippene for informasjonssikkerhet er rektor ansvarlig for å oppdatere dokumentene og føre tilsyn med at tilhørende rutiner og standarder følges opp i organisasjonen som helhet.

2.3 Direktør for organisasjon og informasjon er delegert rollen som NTNUs sentrale informasjonssikkerhetsansvarlige [1].

2.4 Direktør for organisasjon og informasjon har ansvar for å revidere policyen og prinsippene, minimum hvert annet år eller ved endringer i trusselbildet. Revisjonen skal utføres etter prinsipper fra ISMS[2] beskrevet i ISO/IEC 27001 (PDCA[3] modellen).

2.5 Ansvar for utarbeidelse og vedlikehold av underliggende rutiner kan delegeres.

2.6 Leder for NTNUs fakulteter og andre faglige enheter som VM og BIBSYS er ansvarlig for å påse at kravene til informasjonssikkerhet følges ved enheten.

2.7 Rollen som informasjonssikkerhetsansvarlig for faglige enheter kan delegeres. Enheten skal dokumentere egen sikkerhetsorganisasjon. Leder har ansvar for at alle enhetens brukere får nødvendig opplæring og har tilgang til tjenester og materiell slik at brukerne kan beskytte NTNUs informasjon og informasjonssystemer.

2.8 Ledere ved NTNUs faglige enheter er ansvarlig for å anskaffe, utvikle, vedlikeholde og kvalitetssikre systemer og rutiner for forsvarlig håndtering og sikring av alle typer informasjon innenfor sine respektive ansvars- og arbeidsområder.

2.9 Personalsjefen har overordnet ansvar for utvikling og kvalitetssikring av institusjonelle prosesser, systemer og rutiner på personalområdet og er ansvarlig for å føre tilsyn med at gjeldende lovgivning og interne rutiner på området følges opp i organisasjonen som helhet.

2.10 Studiedirektøren har overordnet ansvar for utvikling og kvalitetssikring av institusjonelle prosesser, systemer og rutiner innenfor studieområdet og er ansvarlig for å føre tilsyn med at gjeldende lovgivning og interne rutiner på området følges opp i organisasjonen som helhet.

---

[1] Rollen betegnes ofte som CSO (Chief Security Officer), eller der ansvaret bare omfatter Informasjonssikkerhet som CISO (Chief Information Security Officer)

[2] ISMS – Information Security Management System

[3] PDCA - The *plan, do, check, act* (*PDCA*) methodology of quality.

2.11 Økonomidirektøren har overordnet ansvar for utvikling og kvalitetssikring av institusjonelle prosesser, systemer og rutiner innenfor området regnskap og økonomi og er ansvarlig for å føre tilsyn med at gjeldende lovgivning og interne rutiner på området følges opp i organisasjonen som helhet.

2.12 IT - direktøren. har overordnet ansvar for informasjonssikkerhet knyttet til sentrale og virksomhetsomfattende IT – systemer og IT – infrastruktur og er ansvarlig for å føre tilsyn med at gjeldende lovgivning og interne rutiner på området følges opp i organisasjonen som helhet.

2.13 Eiendomssjefen har overordnet ansvar knyttet til bygningsmessig infrastruktur.

2.14 HMS – sjefen har overordnet ansvar for informasjonssikkerheten knyttet til informasjon av helsemessig karakter.

2.15 Arkivleder har overordnet ansvar for informasjonssikkerheten knyttet til utvikling og kvalitetssikring av institusjonelle systemer og rutiner innenfor arkivområdet og er ansvarlig for å føre tilsyn med at gjeldende lovgivning og interne rutiner på området følges opp i organisasjonen som helhet.

2.16 Ledere ved NTNUs faglige enheter er ansvarlig for at informasjon av vitenskapelig /faglig karakter innenfor eget ansvarsområde håndteres i henhold til gjeldende forskningsetiske standarder og i samsvar med bestemmelsene om personvern i Personopplysningsloven. Forskningsprosjekter og studentprosjekter som omfattes av Lov om medisinsk og helsefaglig forskning skal forhåndsgodkjennes av regional komité for medisinsk og helsefaglig forskningsetikk (REK). Norsk samfunnsvitenskapelig datatjeneste (NSD) er personvernombud for forsknings- og studentprosjekter som behandler personopplysninger og som ikke faller inn under Lov om medisinsk og helsefaglig forskning. Disse prosjektene er meldepliktige til NSD.

2.17 Ledere ved NTNUs faglige enheter er ansvarlig for å føre tilsyn med at gjeldende lover og NTNUs egne rutiner vedrørende kommersialisering av forskningsresultater og ivaretakelse av de vitenskapelig ansattes intellektuelle rettigheter (IP) blir fulgt.

2.18 Ansatte, studenter og andre personer tilknyttet NTNU plikter å overholde *Policy for Informasjonssikkerhet ved NTNU* og *Prinsipper for Informasjonssikkerhet ved NTNU* med tilhørende rutiner.

Systemeier

2.19 Systemeier har ledelses- og prosessansvar - herunder ansvar for utvikling og vedlikehold av informasjonssystemet eller infrastrukturen og for kontroll av produksjon og informasjonssikkerhet Termen ”eier” betyr ikke at personen eller enheten har en juridisk eiendomsrett. Systemeier skal være ansatt ved NTNU.

2.20 Den enkelte enhetsleder er ansvarlig for å utpeke systemeier og/ eller prosesseier for egne/interne systemer innen eget ansvars- og virksomhetsområde. For sentrale prosesser og virksomhetsovergripende systemer har leder av sentraladministrativ enhet dette ansvaret etter pålegg fra direktør for organisasjon og informasjon, jfr. også 2.9 – 2.15.

Den enkelte enhetsleder har innenfor sitt ansvars- og virksomhetsområde ansvaret for kvalitetssikringen av bruken av de sentrale systemene innenfor de rammene som er gitt av systemeier.

2.21 Systemeier er ansvarlig for krav til anskaffelse, utvikling og vedlikehold av informasjonssystemer. Systemeieren er også ansvarlig for å spesifisere sikkerhetskrav for informasjonen og informasjonssystemet og informasjonen som behandles av systemet.

2.22 Systemeiere er ansvarlig for å påse at dokumentasjon for sikkerhetskrav, tilgangskontroll og autorisert bruk for informasjonssystemet og informasjonen forefinnes og vedlikeholdes. (se 6.5)

Systemansvarlige

2.23 Systemansvarlige er personer som har ansvar for drift av informasjonssystemer eller infrastruktur. Det enkelte informasjonssystem eller infrastruktur kan ha en eller flere systemansvarlige. Ansvaret innbefatter implementasjon og drift av de systemer og de prosesser som inngår i forvaltningen av informasjonen som er betrodd NTNU.

2.24 Den systemansvarlige skal sørge for at sikkerheten i sitt informasjonssystem holder det nivået som systemeieren krever for å tillate behandling av sin informasjon. Dette innebærer også vedlikehold av systemet og implementering av tiltak slik at endringer i trusselsituasjon eller system ikke fører til at sikkerhetsnivået ikke tilfredsstiller kravene til informasjonssikkerhet.

2.25 Systemansvarlige har varslingsplikt overfor systemeiere dersom sikkerheten i systemet endres slik at det ikke tilfredsstiller sikkerhetskravene.

2.26 Den systemansvarlige er ansvarlig for å ha – eller å kunne framlegge informasjon om sikkerheten i systemet når systemeieren skal velge system, sikkerhetsnivå og krav til tiltak for å beskytte sin informasjon.

3 Klassifisering og kontroll

3.1 Informasjon og informasjonssystemer skal klassifiseres med hensyn til akseptabelt sikkerhetsnivå, tilgangsbegrensning og akseptabel bruk.

Klassifisering av informasjon

3.2 Bruker er ansvarlig for klassifisering av all informasjon brukeren behandler.

3.3 Leder ved NTNUs enheter har det overordnede ansvaret for klassifisering av informasjon ved sin enhet. Systemeier avgjør lagringsmåte og har ansvar for administrasjon av tilgangsrettigheter.

3.4 Informasjon skal klassifiseres i en av følgende kategorier:

- **Strengt fortrolig**
  - Informasjon som ut fra Beskyttelsesinstruksen er gradert *Strengt fortrolig* og *Fortrolig*. Slik informasjon skal behandles etter Beskyttelsesinstruksen.
- **Fortrolig**
  - Informasjon som er omfattet av lovbestemt og avtalemessig taushetsplikt:
    - Sensitive personopplysninger ut fra Personopplysningsloven, Helseregisterloven og Helseforskningsloven. Nærmere inndeling beskrives i dokumentet *Behandling av personopplysninger ved NTNU*.
    - Forvaltningslovens bestemmelser om taushetsplikt.
    - Konfidensialitetsklausuler; informasjon av sensitiv art hvor uautorisert tilgang til informasjonen kan medføre betydelig skade for enkeltpersoner, NTNU, kontraktsparten eller deres interesser.
- **Intern**
  - Informasjon der det er fastsatt utsatt innsynsrett eller som er unntatt fra innsynsrett etter Offentlighetslovens kapittel 2 og 3.
  - Informasjon som NTNU forvalter for samarbeidspartnere og andre der informasjonseier har pålagt NTNU unntak fra innsynsrett i henhold til konfidensialitetsklausul og der det ikke kreves beskyttelsestiltak som for klassen *Fortrolig.*
  - Personopplysninger som er å anse som grunnopplysninger iht. dokumentet *Behandling av personopplysninger ved NTNU*.

- **Åpen**
  - Annen informasjon er åpen.

Klassifisering av informasjonssystemer

3.5 Begrepet informasjonssystemer omfatter informasjonen selv og infrastrukturen for informasjonsbehandling. Begrepet infrastruktur for informasjonsbehandling omfatter i dette dokumentet alle former for utstyr og rutiner som benyttes til elektronisk eller papirbasert bearbeiding og lagring av informasjon, og de metoder som gjør slik informasjon tilgjengelig.

3.6 Alle informasjonssystemer skal klassifiseres iht. sikring av konfidensialitet, integritet og tilgjengelighet. Følgende kategorier skal benyttes: *Høy*, *Medium*, *Lav*.

3.7 Systemeier skal gjennomføre klassifisering iht. gjeldende rutine.

Fysisk sikkerhet/soneinndeling

3.8 NTNUs lokaler skal sikres med tilstrekkelige sikringssystemer inkl. relevant sporbarhet/logging av tilgang.

3.9 Alt personell skal kunne tilkjennegi sin identitet når de er i NTNUs områder med tilgangsbegrensninger. Referert til tabellen under punkt 3.11 betyr det områder med *Rød*, *Gul* og *Blå* sikkerhetsgradering til alle tider og for områder med *Grønn* sikkerhetsgradering når skallsiktingen er aktivisert.

3.10 Områder som inneholder infrastruktur for informasjonsbehandling og informasjon som krever beskyttelse skal inndeles i soner. Sonene skal beskyttes med hensiktsmessige adgangskontroller for å sikre at kun autorisert personell får adgang. Ved vurdering av adgangskontroll og autorisasjon tas hensyn til hvilken informasjon og hvilket utstyr som er plassert i aktuelt område iht. til gjeldende rutine.

3.11 Følgende soneinndeling skal benyttes:

Sikrings-nivå	Type informasjon/ informasjons-systemer	Område	Sikring
Rød	Informasjon klassifisert som: *Strengt fortrolig* og *Fortrolig* Informasjonssystem klassifisert som: *Høy*	Avgrensede områder hvor spesiell autorisasjon kreves, datarom/serverom/arkiver med fortrolig informasjon og lignende. Rom med infrastruktur som representerer høy sårbarhet/risiko for kritiske eller større deler av NTNUs virksomhet.	Avlåst hele døgnet. Adgangskort eller nøkkel med svært begrenset tilgang.
Gul	Informasjon klassifisert som: *Fortrolig* Informasjonssystem klassifisert som: *Medium*	Tekniske rom med infrastruktur som representerer høy sårbarhet/risiko for avgrensede deler av NTNUs virksomhet, printerrom, arkivrom, møterom og kontorlokaler der det kan finnes informasjon klassifisert som *Fortrolig*.	Avlåst hele døgnet. Tilgang med nøkkelkort eller nøkkel. For printerrom der selve rommet er plassert i blå eller grønn sone kan printeren være gul sone ved utskrift av fortrolig informasjon. Det kreves da sikker utskriftsfunksjonalitet for printeren/utskriftssystemet.
Blå	Informasjon klassifisert som: *Intern* Informasjonssystem klassifisert som: *Medium*	Kontorer, datasaler, møterom m.v. der det er adgangskontroll hele døgnet. Arealer der det kan finnes informasjon klassifisert som *Intern*	Personlig nøkkelkort, lås, tilgang via resepsjon
Grønn	Informasjon klassifisert som: *Åpen* Informasjonssystem klassifisert som: *Lav*	Offentlig tilgjengelige områder: Vrimleområder, korridorer, kantiner m.v. I prinsippet alt åpent.	Skallsikring for bygninger utenom åpningstid og eventuelle ekstra sikkerhetstiltak f.ex. vakt på bibliotek, Videoovervåking m.v. Sikringstiltakene baseres på ROS-vurdering og aktiva plassert i lokalene

3.12 For informasjon klassifisert som *Fortrolig* og informasjonssystemer klassifisert som *Medium* velger systemeier plassering i fysisk sone ut fra valgmuligheten i tabellen. Systemeier kan også velge plassering i sone med høyere sikkerhetskrav enn angitt i tabellen.

3.13 Hvert område med sikkerhetsgradering *Rød* og *Gul* skal ha en sikkerhetsansvarlig for området. Enheten med ansvar virksomheten knyttet til informasjonssystemer og infrastruktur for informasjonsbehandling i området er ansvarlig for at det utpekes en sikkerhetsansvarlig.

3.14 Ved tildeling og kontroll av adgang til områder med *Rød* og *Gul* sikkerhetsgradering følges gjeldende rutiner – se *Rutiner for regulering av tilgang til sikrede områder.*

3.15 Stasjonært utstyr kan kun tas ut av områder med *Rød* og *Gul* sikkerhetsgradering etter fullmakt eller godkjenning fra sikkerhetsansvarlig for området.

Sikring av IT-utstyr og datamedier

3.16 Med IT-utstyr og datamedier forstås alt utstyr for (maskinell) behandling, lagring og transport av informasjon. Både stasjonært utstyr som arbeidsstasjoner, tjenermaskiner og kommunikasjonsutstyr og bærbart som bærbare datamaskiner, mobiltelefoner og bærbart lagringsmedium som for eksempel minnepinner og CD/DVD-plater.

3.17 Alt IT-utstyr som lagrer informasjon klassifisert som *Intern* og/eller *Fortrolig* (se 3.4) skal passordbeskyttes. Videre skal alt IT-utstyr som tilkobles NTNUs nett passordbeskyttes.

3.18 Informasjon klassifisert som *Fortrolig* på bærbare maskiner og flyttbare datamedier skal krypteres. Styrken på krypteringen skal tilfredsstille sikkerhetskravene satt til beskyttelse av informasjonen.

3.19 IT-utstyr og datamedier som tas ut av lokalene – inklusive bærbart IT-utstyr skal ikke være ubevoktet på offentlige steder. Slikt utstyr skal håndteres som håndbagasje under reiser.

3.20 Ved gjenbruk og kassering av IT-utstyr og datamedier skal relevante rutiner for dette følges, se *Rutine for gjenbruk og kassasjon av IT-utstyr og datamedier*. Lisensiert programvare og data fjernes på en sikker måte slik at kravet til informasjonssikkerhet er tilfredsstilt.

4 Informasjonssikkerhet knyttet til ansatte, innleid personell, studenter og tredjeparter

For alle gjelder

4.1 For tilgang til NTNUs IT-systemer kreves aksept av *NTNUs IT-reglement* og *Datadisiplinerklæring ved NTNU*. Den på NTNU som inngår kontrakt eller avtale er ansvarlig for dette.

4.2 Taushetserklæring[4] skal signeres av alle som kan få kjennskap til fortrolig og/eller intern informasjon.

4.3 Alle brukere av NTNUs informasjonssystemer skal få tilstrekkelig opplæring og oppdatering i NTNUs prinsipper for informasjonssikkerhet og tilhørende rutiner herunder sikkerhetsansvar og roller.

4.4 Brudd på prinsippene for informasjonssikkerhet og tilhørende rutiner vil kunne medføre sanksjoner iht. Tjenestemannsloven og/eller gjeldende regler ved NTNU.

4.5 Sjekk av bakgrunnen til alle som innstilles til stillinger ved NTNU og for innleid personell skal foretas iht. relevante lover og regler.

Avslutning eller endring av tilsettings-, tilknytnings- eller studieforhold gjelder

4.6 Ansvar for gjennomføring av rutiner ved avslutting eller endring av ansettelses-, tilknytnings- eller studieforhold skal være klart definert. Det skal foreligge dokumenterte rutiner med tilpassede rundeskjema for slike avslutnings- og endringsprosesser.

4.7 NTNUs eiendeler[5] leveres inn ved opphør av behov for bruk av eiendelene. Ved tilbakeleveringen følges rutinene for aktuell enhet med relevant rundeskjema.

4.8 Eierforholdet til informasjon avklares. Informasjon eid av NTNU skal dokumenteres og overleveres NTNU.

4.9 NTNU endrer eller stenger tilgangsrettigheter ved opphør eller endring av ansettelses-, tilknytnings- eller studieforhold.

5 Kommunikasjons- og driftsadministrasjon

Operasjonelle rutiner og ansvarsområder

5.1 Rutiner for administrasjon og drift av all infrastruktur og IT-utstyr som brukes til behandling av NTNUs informasjon eller kobles til NTNUs nettverk skal være etablert. Dokumentasjonen skal holdes oppdatert og revideres etter vesentlig endring. Driftsdokumentasjonen skal være tilgjengelig for de som har behov for det og som er autorisert for slik tilgang.

5.2 Rutiner for endringsadministrasjon og endringskontroll skal være etablert og dokumentert.

---

[4] *Standard taushetserklæring ved NTNU*, eventuelt med tillegg tilpasset arbeidsoppgaver og systemtilganger

[5] Eiendeler inkluderer programvare, dokumenter (alle lagringsmedia) og utstyr

5.3 Organisering av IT-tjenesten er ikke homogen for NTNU. Med begrepet IT-tjenesten – eller IT-tjenesten ved enhet forstås den/de som er overordnet ansvarlig for all lokal IT-drift ved enheten.

5.4 IT-tjenesten ved NTNUs enheter sikrer dokumentasjon av enhetens systemer og virksomhetsomfattende systemer som driftes på enheten etter *Standard for driftsdokumentasjon for informasjonssystemer ved NTNU*. For virksomhetsomfattende systemer er IT-avdelingen ansvarlig for å påse at det utarbeides og vedlikeholdes slik dokumentasjon.

5.5 Installasjon av IT-utstyr inklusive programvare skal godkjennes av IT-tjenesten ved den enhet der installasjonen utføres. Godkjenning skal foreligge før installasjon. For utstyr og programvare som har innvirkning utenfor enhetens område skal installasjonen godkjennes av IT-avdelingen.

5.6 Arbeidsoppgaver og ansvarsforhold/autorisasjonsmyndighet skal skilles på en slik måte at det reduserer muligheter for uautorisert- eller uforutsett misbruk av NTNUs informasjonssystemer og informasjon.

5.7 IT-utstyr for utvikling og test skal holdes adskilt fra ordinær produksjon for å redusere risikoen for uautorisert tilgang eller uautoriserte endringer og for å redusere risiko for feilsituasjoner.

Eksterne parter

5.8 Det skal være utarbeidet og godkjent avtaler i forbindelse med utveksling av informasjon og programvare med ekstern tredjepart og ekstern serviceleverandør. Alle avtaler skal tilfredsstille krav til informasjonssikkerhet i forhold til personvernlov, andre lover og krav fra eier av data.

5.9 Ved bruk og kjøp av IT-tjenester skal alle avtaler inneholde:

- krav til informasjonssikkerhet (Konfidensialitet, Integritet og Tilgjengelighet)
- beskrivelse av avtalt sikkerhetsnivå
- krav til fortløpende rapportering av avvik fra leverandør
- beskrivelse av hvordan NTNU kan etterprøve at driftsleverandørene oppfyller avtalene.
- rett til revisjon
- Krav til driftsdokumentasjon for å tilfredsstille lover og forskrifter
- Krav til driftsdokumentasjon for de deler av driften der NTNU er medvirkende.
- Bestemmelser for ekstern lagring og bruk av NTNUs og tredjeparts data i forhold til krav i personvernlov, andre lover og krav fra eier av data

5.10 Ledere ved andre organisasjoner, f.eks stiftelser og randsoneselskaper, som er direkte knyttet til NTNUs infrastruktur for informasjonsbehandling er ansvarlig for at NTNUs krav til informasjonssikkerhet følges i enheten. Før slik tilgang gis skal det foreligge en skriftlig avtale mellom organisasjonen og IT-avdelingen der blant annet dette ansvarsforholdet er spesifisert.

Systemplanlegging og aksept/godkjenning

5.11 Dimensjonering av IT-systemer skal avpasses kapasitetskrav. Det skal foretas beregninger av framtidige kapasitetsbehov for å sikre at systemet oppnår påkrevd ytelse.

5.12 Belastning av IT-systemer skal overvåkes slik at oppgradering og tilpasning kan finne sted løpende. Dette gjelder særlig for virksomhetskritiske systemer.

5.13 Kravene til informasjonssikkerhet skal ivaretas når nye IT-systemer designes, testes, implementeres og oppgraderes, og ved andre systemendringer.

Beskyttelse mot skadelig kode

5.14 Datasystemer og informasjon skal sikres mot virus og annen skadelig kode. IT-tjenesten ved NTNUs enheter er ansvarlig for at sikringen gjennomføres.

Sikkerhetskopiering

5.15 Det skal være dokumenterte rutiner for sikkerhetskopiering og gjenoppretting.

5.16 Det skal gjennomføres regelmessig sikkerhetskopiering og testing av denne.

5.17 Tilgangskontrollen for sikkerhetskopier skal minst tilsvare kravene til informasjonssikkerhet for de lagrede data.

5.18 Sikkerhetskopier oppbevares eksternt eller i egen relevant sikret brannsone.

Nettverksadministrasjon

5.19 IT-avdelingen har det overordnede ansvaret for å beskytte NTNUs nettverk.

5.20 IT-avdelingen er ansvarlig for dokumentasjon av NTNUs nettverk.

5.21 Alle enheter skal føre oversikt over eget IT-utstyr eid eller disponert av NTNU, som kobles opp i NTNUs nettverk.

5.22 Alle enheter skal ha driftsrutiner for å tilfredsstille kravet til sikkerhet for enhetens eget IT-utstyr tilkoblet NTNUs nettverk.

5.23 Alle enheter skal ha driftsrutiner for raskt å kunne lokalisere og eliminere sikkerhetsbrudd i NTNUs nettverk med opphav i hendelser fra enhetens del av nettet.[6]

[6] Fra nettilkoblinger i fysiske områder disponert av enheten.

Håndtering av datamedier

5.24 Håndtering av flyttbare datamedia (som f.eks. magnetbånd, USB- minnepinner, mobiltelefoner, CD/DVD-plater og utskrifter) sikres i henhold til klassifikasjon av informasjon og mediet.

5.25 Ved gjenbruk eller avhending av datamedier skal informasjonssikkerheten ivaretas i henhold til klassifisering av innhold. Ref. *Rutine for gjenbruk og kassasjon av IT-utstyr og datamedier*.

Håndtering av systemdokumentasjon

5.26 Systemdokumentasjon skal beskyttes mot uautorisert tilgang.

Utveksling av informasjon

5.27 Ved intern utveksling og forflytting av informasjon utnyttes sikkerhetsmekanismer i nettet – se 6.9 og interne rutiner for slik informasjonsbehandling for å tilfredsstille kravene til sikkerhet stilt av systemeieren og i lover og regler.

5.28 For ekstern utveksling og forflytting av informasjon skal det være etablert dokumenterte rutiner og kontroller. Rutinene skal tilfredsstille krav til informasjonssikkerheten stilt av systemeieren og i lover og forskrifter.

5.29 Ved utveksling av informasjon klassifisert som *Fortrolig* – ref. 3.4 skal informasjonen krypteres. Eventuelle flyttbare medier som brukes i utvekslingen skal beskyttes på tilfredsstillende måte. Krypteringens styrke og utveksling av krypteringsnøkler skal tilfredsstille krav til sikkerhetsnivå for informasjonen.

5.30 Ved utveksling av informasjon klassifisert som *Intern* – ref. 3.4 benyttes kryptering eller andre sikkerhetstiltak som tilfredsstiller kravene til sikkerhetsnivå stilt av systemeieren.

Elektronisk tjenesteyting

5.31 Informasjon som utveksles i forbindelse med tjenesteyting over nettet (eksempler oppmelding eksamen, bestillings-/betalingstjenester), skal beskyttes mot svindel, uautorisert adgang og endringer.

5.32 Informasjon som gjøres offentlig tilgjengelig på NTNUs nettverk skal beskyttes for å forhindre uautorisert endring.

Overvåkning av systemtilgang og bruk

5.33 Tilgang og bruk av systemer logges og overvåkes for å kunne identifisere potensielt misbruk. IT-tjenesten ved aktuell enhet er ansvarlig for logging og oppbevaring av logger. For virksomhetsomfattende systemer er den IT-avdelingen ansvarlig for loggtjenesten.

5.34 Logger skal beskyttes mot manipulering og uautorisert tilgang. Oppbevaring, tilgang og bruk av loggene skal tilfredsstille lovbestemte krav til personvern.

5.35 Hendelser i loggen skal være sporbare til en spesifikk entitet (f.eks. person eller enkeltsystem).

5.36 Loggtjenesten skal registrere vesentlige forstyrrelser og uregelmessigheter i driften av systemene, samt mulig årsak til feil.

5.37 Loggtjenesten skal registrere sikkerhetshendelser i alle vesentlige systemer.

5.38 Sikkerhetshendelser i logger rapporteres slik det er fastlagt i Kap 8 - Hendelseshåndtering.

5.39 IT-tjenesten ved den enkelte enhet i samarbeid med IT-avdelingen sikrer at systemenes klokker jevnlig synkroniseres til korrekt tid.

6 Tilgangskontroll

Rutiner for tilgangskontroll

6.1 Det skal finnes skriftlige rutiner for tilgangskontroll, passord og andre autentiseringsmekanismer. Rutinene skal inneholde passordregler (minimumslengde, type karakterer som kan/skal benyttes mv), endringsfrekvens for passord og regler for lagring og oppbevaring av passord. Rutinene skal være basert på virksomhets– og sikkerhetsmessige krav og behov.

Brukeradministrering – og ansvar

6.2 Systemaksess autentiseres minimum ved hjelp av personlige brukeridenter og personlige passord. Bruk av gruppebrukerident og gruppepassord er bare tillatt dersom det er nødvendig av systemtekniske eller driftstekniske årsaker. Ved slik bruk av gruppebrukerident/passord skal brukerens personident kunne spores på andre måter.

6.3 Ved tildeling av personlige brukeridenter kreves undertegning eller annen autentisert aksept av *Datadisiplinerklæring ved NTNU*.

6.4 Brukere er ansvarlige for enhver bruk av brukeridenter og passord. Brukere holder brukeridenter og passord konfidensielle. Se også *NTNUs IT-reglement*.

Tilgangskontroll/Autorisasjon

6.5 Tilgang, tilgangsrettigheter og aksessrettigheter til informasjonssystemer, skal være autorisert av systemeier for det enkelte system. Rettighetene gis på grunnlag av ”need to know”-prinsippet og reguleres av type rolle og stilling.

6.6 Ved endring i tilknytningsform eller rolle skal tilgangsrettigheter endres tilsvarende uten unødig opphold. Nærmeste leder er ansvarlig for å initiere endring. Se også 4.6

Kontroll med nettverkstilgang

6.7 IT-avdelingen har ansvaret for at brukernes nettverkstilgang skjer i overensstemmelse med rutinene for systemtilgang, punkt 6.2

6.8 Brukere skal kun ha tilgang til de nettverkstjenester de er autorisert for.

Oppdeling av nettverk

6.9 Det skal benyttes en soneoppdeling av NTNUs nettverk med definerte sikkerhetsnivå for hver sone. Valg av sone for det enkelte informasjonssystem, beskyttelsesmekanismer for sonen og tilgangsbegrensninger fastlegges etter en risikovurdering.

Mobilt utstyr og fjerntilgang

6.10 Arbeid på NTNUs datasystemer utenfor NTNUs lokaler, direkte eller via fjerntilgang krever at brukeren har underskrevet og overholder datadisiplinerklæring.

6.11 Fjerntilgang til NTNUs nettverk skal kun skje gjennom sikkerhetsløsninger godkjent av IT-avdelingen.

6.12 Enheter brukt til fjerntilgang sikres med tilstrekkelige sikkerhetsmekanismer. Sikkerhetsmekanismene skal tilpasses aktuell bruk og skal være godkjent av IT-avdelingen – ref *Rutine for fjerntilgang til NTNUs datasysteme.*

6.13 Ved overføring data mellom fjernarbeidsplasser og NTNU skal utvekslingen være sikret etter bestemmelsene for Utveksling av Informasjon – punkt 5.27 - 5.30.

6.14 Informasjon klassifisert som *Fortrolig* etter punkt 3.4 skal lagres kryptert ved all lagring utenfor NTNU. Dette gjelder både på bærbare og stasjonære maskiner, flyttbare medier slik som USB-stick, PDAer, mobiltelefoner, CDer, DVDer, disketter etc. og for faste lagringssystemer. Krypteringen skal ha styrke tilsvarende sikkerhetskravet for lagret informasjon. For informasjon klassifisert som *Intern* etter 3.4 benyttes kryptering eller andre sikkerhetstiltak som tilfredsstiller krav til sikkerhetsnivå stilt av systemeieren.

6.15 Tilgang til privilegerte kontoer og fortrolige områder ved fjerntilgang skal begrenses ut fra en sårbarhets og risikovurdering.

7 Anskaffelse, utvikling og vedlikehold av informasjonssystemer

Sikkerhetskrav til informasjonssystemer

7.1 Utredninger av virksomhetsbaserte krav til nye informasjonssystemer eller til forbedringer av eksisterende systemer skal spesifisere hvilke krav som settes til sikringstiltak. Informasjonssystemer omfatter operativsystemer, infrastruktur, tjenester, standardsystem – eventuelt tilpasset NTNU og egenutviklede systemer.

7.2 Alle krav til informasjonssikkerhet skal identifiseres i forbindelse med kravspesifiseringer i et prosjekt og skal begrunnes, godkjennes og dokumenteres.

7.3 Ved kjøp av produkter skal det verifiseres om de spesifiserte krav til sikring er tilfredsstilt. Dersom ikke sikkerheten i et foreslått produkt tilfredsstiller de angitte kravene gjennomføres og dokumenteres en vurdering av risiko og tilhørende sikkerhetstiltak før produktet eventuelt kjøpes inn. Eventuelle kontrakter med leverandør skal også omfatte spesifisering av sikringskrav. For kjøp av tjenester – se 5.9.

Riktig behandling i applikasjoner

7.4 Hensiktsmessige tiltak for å forhindre feil, tap, uautorisert endring eller misbruk av informasjon skal integreres i applikasjonene, medregnet egenutviklede programmer. Disse sikringstiltakene bør omfatte godkjenning av inndata, utdata og kontroller av intern behandling.

Kryptografiske kontroller

7.5 Det skal være rutiner for administrasjon og bruk av kryptografiske kontroller for beskyttelse av informasjon.

Sikring av systemfiler

7.6 Installasjon av programvare eller andre endringer i produksjonsmiljø skal følge gjeldende driftsrutiner og endringsrutiner.

7.7 Programkildekode for produksjonssystemene skal sikres mot uautorisert tilgang og mot tap av koden.

Sikkerhet i utvikling og vedlikehold

7.8 De systemer som utvikles for, eventuelt av NTNU, skal ha klare krav til sikkerhet, inkludert validering av data, sikring av koden før produksjonssetting, og eventuell bruk av kryptografi.

7.9 Kravene til sikkerhet i systemarkitekturen skal tilfredsstille kravene stilt i de overordnede IT-arkitekturprinsipper for offentlig sektor, se Stortingsmelding nr. 19 (2008-2009) og referanser fra websidene til Direktoratet for forvaltning og IKT.

7.10 Det skal gjennomføres en sårbarhets- og risikovurdering. – Ref: *Rutine for risiko og sårbarhetsvurdering i forbindelse med informasjonssikkerhet ved NTNU* før nye informasjonssystemer klassifisert som *Høy*, etter punkt 3.5, settes i produksjon. Det gjelder også før større endringer av eksisterende systemer gjennomføres.

7.11 Implementering av endringer skal kontrolleres - gjennom bruk av formelle rutiner for endringskontroll - for å minimalisere mulighetene for skade på informasjon eller informasjonssystemer.

7.12 Programvare skal gjennomtestes og aksepteres formelt av eier/brukere og driftsansvarlig før programvaren overføres til produksjonsmiljøet.

8 Hendelseshåndtering

Ansvar for rapportering

8.1 Alle brukere, kontraktører og tredjepartsbrukere er ansvarlig for å rapportere brudd og mulige brudd på sikkerheten og sikkerhetssvakheter. Rapporteringen går linjevei som gitt i NTNUs rutiner for avviksrapportering.

Administrasjon av informasjonssikkerhetsbrudd og forbedringer

8.2 Det skal være utarbeidet rutiner for avvikshåndtering og rapportering av avvik og sikkerhetssvakheter. Rutinene skal inneholde krav til tiltak for å forhindre gjentagelser, forbedre sikkerheten og krav om tiltak for skadereduksjon.

Bevissikring

8.3 IT-tjenesten ved enhetene skal være kjent med enkle rutiner for bevissikring ved mistanke om brudd på informasjonssikkerheten.

8.4 Dersom brudd på informasjonssikkerheten vil kunne medføre strafferettslig påtale, opphør av studie- eller arbeidsforhold og tiltak av tilsvarende type, rapporteres saken direkte til NTNUs sentrale sikkerhetsansvarlige eller den han har utpekt.

8.5 Ansatte og studenter skal være gjort kjent med at bevis fra sikkerhetshendelser tas vare på (lagres) og overleveres ved rettslig krav.

9 Kontinuitetsplanlegging

Kontinuitetsplan

9.1 Det skal være utarbeidet kontinuitetsplaner som dekker kritiske/viktige informasjonssystemer og infrastruktur. Planen skal følge *NTNUs sentrale mal for beredskapsplaner*. Planene avstemmes med NTNUs øvrige beredskap og katastrofeplanverk.

9.2 Den enkelte enhet er ansvarlig for utarbeidelse og vedlikehold av planer for lokale systemer.

9.3 IT-avdelingen er ansvarlig for utarbeidelse og vedlikehold av overordnet plan som omfatter fellessystemer og virksomhetsomfattende systemer.

9.4 Systemene som inngår i planene klassifiseres med tilgjengelighetskrav *Høy*. *Medium* og *Lav* iht. rutiner.

9.5 Kontinuitetsplaner utarbeides på bakgrunn av risiko og sårbarhetsanalyser som tar utgangspunkt i risikoer for NTNUs virksomhet. *Rutine for risiko og sårbarhetsvurdering i forbindelse med informasjonssikkerhet ved NTNU* legges til grunn for arbeidet.

9.6 Kontinuitetsplanene testes og oppdateres periodisk for å sikre at den er dekkende, og sikre at ledelse og ansatte forstår gjennomføringen.

9.7 Infrastruktur for informasjonsbehandling med tilgjengelighetskrav klassifisert som *Høy* (se 9.4) skal plasseres eller beskyttes slik at det reduserer risikoen for miljømessige trusler (brann, oversvømmelse, temperatursvingninger, fukt etc.). Tiltak skal settes med basis i ROS-vurdering.

9.8 Infrastruktur for informasjonsbehandling med tilgjengelighetskrav klassifisert som *Høy* skal sikres mot bortfall av støttetjenester som strøm, kjøling og mot bortfall av kommunikasjonsforbindelser. Tiltak skal settes med basis i ROS-vurdering.

10 Referanser

- NTNUs websider for sikkerhet
  - http://sikkerhet.ntnu.no
- Policy for Informasjonssikkerhet ved NTNU
  - en URL
- Prinsipper for informasjonssikkerhet ved NTNU
  - en URL
- Referanser for informasjonssikkerhet ved NTNU
  - en URL
- Lovdata
  - http://www.lovdata.no/
- Datatilsynets websider
  - http://datatilsynet.no

Vedlegg

Policy for informasjonssikkerhet ved NTNU

Ledelsens formål med informasjonssikkerhet

Informasjon, informasjonsbehandling og informasjonssikkerhet er kritiske faktorer i NTNUs virksomhet innenfor læring, forskning, formidling og forvaltning. Det stilles derfor strenge krav til at informasjonssikkerheten blir tilstrekkelig ivaretatt. Systemer og infrastruktur skal være pålitelige i bruk, samtidig som informasjon skal være korrekt og beskyttet mot uautorisert tilgang.

Informasjon eid eller forvaltet av NTNU skal sikres:

konfidensialitet; sikkerhet for at kun autoriserte personer har tilgang til informasjonen, og at den ikke avsløres til uvedkommende.

integritet; sikkerhet for at informasjonen og informasjonsbehandlingen er fullstendig, nøyaktig og gyldig, og et resultat av autoriserte og kontrollerte aktiviteter.

tilgjengelighet; sikkerhet for at en tjeneste oppfyller bestemte krav til stabilitet, slik at aktuell informasjon er tilgjengelig for autoriserte ved behov.

Behandling og beskyttelse av informasjon og informasjonssystemer skal skje i samsvar med personopplysningsloven og andre lover og bestemmelser som regulerer behandling av informasjon og informasjonssystemer, samt etter metoder fra internasjonale standarder for informasjonssikkerhet (ISO/IEC 27001/2).

Informasjonssikkerheten skal ivaretas av policy for informasjonssikkerhet og et sett av underliggende og komplementerende dokumenter.

Dokumentet *Prinsipper for informasjonssikkerhet ved NTNU* beskriver ansvar og roller i forhold til informasjonssikkerhet og fastlegger de overordnede prinsippene for ivaretakelse og vedlikehold av informasjonssikkerheten ved NTNU. Prosedyrer og rutiner for implementering av prinsippene er gitt i egne dokumenter.

Infrastruktur for informasjonsbehandling omfatter i dette dokumentet alle former for utstyr og alle rutiner som benyttes til elektronisk eller papirbasert bearbeiding og lagring av informasjon, og de metoder som gjør slik informasjon tilgjengelig.

Konkrete mål for sikkerheten

- Ivareta NTNUs, ansattes, studentenes og andre brukeres krav til konfidensialitet, integritet og tilgjengelighet.

- Etablere kontroller for å beskytte NTNUs informasjon og informasjonssystemer mot alle former for uønskede hendelser, skade og tap.
- Sørge for å være i samsvar med gjeldende lover, forskrifter, retningslinjer og være tilnærmet i henhold til internasjonale standarder for informasjonssikkerhet (ISO/IEC 27002 og kontrollområdene i ISO/IEC 27001)..
- Etablere ansvar og eierskap for informasjonssikkerhet ved NTNU.
- Motivere ledelse, ansatte, studenter og andre brukere til å opprettholde kunnskap og kompetanse om informasjonssikkerhet, slik at frekvens og skadenivå av sikkerhetshendelser kan minimaliseres.
- Sikre at NTNU er i stand til å fortsette sine tjenester, også i fall større hendelser i forhold til informasjonssikkerhet skulle inntreffe.
- Sikre at personvernet ivaretas.

Brudd på policyen kan skade NTNUs informasjon og infrastruktur, føre til at informasjon som er eid eller forvaltet av NTNU blir misbrukt eller ødelagt og skade NTNUs omdømme. Overtredelse av denne policy for informasjonssikkerhet og vedtatte sikkerhetskrav vil derfor være et tillitsbrudd mellom brukeren og NTNU, og vil kunne medføre konsekvenser for ansettelses- eller studieforholdet.