# Ledelsessystem for informasjonssikkerhet

## Kapittel 1: Innledning

### 1.1 Formål og hensikt

Universitetet i Tromsø – Norges arktiske universitet (UiT) er et nasjonalt og internasjonalt kraftsenter for kompetanse, vekst og nyskaping i nordområdene. Dette skal blant annet vises gjennom høy kvalitet på UiTs kunnskapsforvaltning og informasjonsverdier: forskningsdata, forskningsresultater og informasjon eller kunnskap som inngår i undervisning, forskning og formidling.

Et systematisk og planmessig arbeid for å sikre våre informasjonsverdier er derfor en sentral del av UiTs kunnskapsforvaltning. Både interne og eksterne aktører – ledere, ansatte, studenter, samarbeidspartnere og offentligheten for øvrig – skal kunne stole på at UiT ivaretar

1. informasjonens konfidensialitet – vi beskytter sensitiv eller viktig informasjon mot uautorisert innsyn, tilgang eller misbruk,
2. informasjonens integritet – vi beskytter sensitiv eller viktig informasjon mot uautorisert endring eller sletting,
3. informasjonens tilgjengelighet – vi sørger for at all informasjon er tilgjengelig for alle som skal ha tilgang til den.

UiT er underlagt en rekke lover og forskrifter som pålegger oss å ha tilfredsstillende informasjonssikkerhet. Dette gjelder blant annet forvaltningsloven med forskrift (e-forvaltningsforskriften), personopplysningsloven med forskrift og helseforskningsloven med forskrift. I tillegg inneholder andre lovverk, blant annet offentlighetsloven og arkivloven, bestemmelser som har betydning for arbeidet med sikring av informasjonen ved UiT. I Kunnskapsdepartementets (KD) tildelingsbrev til UiT for 2014 kreves det innføring av et styringssystem for informasjonssikkerhet som bygger på grunnprinsippene i anerkjente sikkerhetsstandarder. *Ledelsessystemet for informasjonssikkerhet ved* UiT ivaretar de kravene som lovverket og KD stiller til arbeidet med informasjonssikkerhet i universitets- og høyskolesektoren.

### 1.2 Ledelsessystemet for informasjonssikkerhet ved UiT

Ledelsessystemet for informasjonssikkerhet skal sørge for at UiTs informasjonsverdier håndteres på en systematisk, planmessig og tilfredsstillende måte. Ledelsessystemet inneholder blant annet mål, strategi og organisering av arbeidet med informasjonssikkerhet, samt beskrivelse av roller og ansvar, oversikt over informasjonsverdier og retningslinjer.

Ledelsessystemet består av tre hovedelementer:

1. Styrende – overordnet policy, herunder sikkerhetsmål og -strategi, roller og ansvar.
2. Gjennomførende – risikovurderinger samt konkrete rutiner og retningslinjer i vedleggene.
3. Kontrollerende – internrevisjon, rapportering av avvik og ledelsens gjennomgang.

## 1.3 Avgrensning av ledelsessystemet

Informasjonssikkerhet er et topplederansvar. Det operative ansvaret og det praktiske arbeidet med å ivareta informasjonssikkerheten kan delegeres til de enkelte enhetene ved UiT, jf. beskrivelsen av sikkerhetsorganisasjonen med roller og ansvar i punkt 3.

Ledelsessystemet for informasjonssikkerhet ved UiT omfatter
• alle brukere av UiTs IT-ressurser[1]
• alle UiTs studiesteder/campuser
• alle organisatoriske enheter[2]
• all teknologi[3]
• alle informasjonsverdier

Med informasjonsverdier menes utstyr, prosesser eller data som er tilknyttet informasjon og som virksomheten anser som nødvendig å beskytte. Hvordan man skal beskytte informasjonsverdiene avhenger av resultatene fra risikovurderinger. Informasjonssikkerhet knyttet til data er medie- og formatuavhengig, gjelder både informasjon som lagres og brukes i mobile enheter, cd-rom og på papir. Det kan være et IT-system, for eksempel personalsystem, læringsplattform og arkivsystem, eller en type informasjon, for eksempel studentinformasjon, pasientinformasjon eller data som inngår i et forskningsprosjekt.

## 1.4 Behandlingsansvarlig og databehandlere

To sentrale begrep går igjen i ledelsessystemet og personvernlovgivningen; behandlingsansvarlig og databehandler. Den behandlingsansvarlige er den som bestemmer formålet med behandlingen av personopplysninger, og hvilke hjelpemidler som skal benyttes. Databehandleren er den som behandler personopplysninger på oppdrag fra den behandlingsansvarlige. Det skal alltid inngås en databehandleravtale før eksterne aktører kan behandle personopplysninger for UiT, også i småskala.

# Kapittel 2: Sikkerhetsstrategi og akseptabel risiko

[innholdet i dette kapittelet berøres ikke i denne saken]

# Kapittel 3: Klassifisering av informasjon

[innholdet i dette kapittelet berøres ikke i denne saken]

[1] *Studenter, ansatte, gjester, samarbeidspartnere etc.*
[2] *Avdelinger, fakulteter, institutter, sentre, museum, databehandlere*
[3] *IT-systemer, datanettverk, databaser/-registre etc.*

# Kapittel 4: Roller, ansvar og oppgaver

I det følgende gis en nærmere beskrivelse av hvilket ansvar og hvilke oppgaver som er lagt til de ulike rollene:

## Universitetsstyret

- behandler og vedtar ledelsessystemet for informasjonssikkerhet ved UiT
- kan stille krav til det videre arbeidet med informasjonssikkerhet ved UiT

## Universitetsdirektør

- er behandlingsansvarlig for alle personopplysninger, dette omfatter også å bestemme formålet med behandling av personopplysninger, samt å ha dokumentert oversikt over disse
- har ansvar for informasjonssikkerhet på et overordnet nivå, herunder å sette av tilstrekkelige ressurser til arbeidet med informasjonssikkerhet, inkludert opplæring og kompetanseheving
- har ansvaret for at ledelsessystemet for informasjonssikkerhet blir implementert og vedlikeholdt, samt for organiseringen av sikkerhetsarbeidet
- skal iverksette årlig internrevisjon, jf. punkt 6.1.
- skal årlig gjennomgå status for arbeidet med informasjonssikkerhet[4]
- skal oppnevne medlemmer av informasjonssikkerhetsforumet

## IT-direktør

- er informasjonssikkerhetsansvarlig og har forvaltningsansvaret for informasjonssikkerheten ved UiT
- har instruksjonsmyndighet overfor alle andre enheter ved UiT i saker som angår informasjonssikkerhet
- skal påse at holdningsskapende programmer gjennomføres

## Informasjonssikkerhetsrådgiver(e)

- skal utøve IT-direktørens myndighet i saker om informasjonssikkerhet
- skal være rådgiver for linjeorganisasjonen i spørsmål relatert til informasjonssikkerhet
- skal lede CSIRT-teamet og Informasjonssikkerhetsforum
- skal utarbeide og vedlikeholde overordnet beredskapsplan for IKT
- skal følge opp avvik på overordnet nivå og sørge for at disse blir kanalisert til og fulgt opp av berørte enheter
- skal drive opplysningsvirksomhet, rådgivning og opplæring innen informasjonssikkerhet
- skal vedlikeholde overordnet policy og rutiner for informasjonssikkerhet
- skal iverksette og delta i revisjoner og risikovurderinger ved behov
- skal utarbeide årlig rapport til ledelsens gjennomgang

[4] Jf. Ledelsens gjennomgang

- skal holde oversikt over databehandleravtaler som inngås på UiT

## Avdeling for IT

- skal bistå systemeier ved utforming av krav til informasjonssikkerhet ved anskaffelse av nye system
- har ansvar for drift av IT-systemene, og skal ivareta tilfredsstillende informasjonssikkerhet på IT-infrastruktur basert på risikovurderinger
- skal, på bakgrunn av risiko- og sårbarhetsanalyser, utarbeide en kontinuitets- og beredskapsplan (KBP) som dekker kritiske og viktige informasjonssystemer og infrastruktur
- skal dokumentere systemer/infrastruktur med tilhørende sikkerhetstiltak
- skal utarbeide og vedlikeholde sikkerhetspolicy, retningslinjer og prosedyrer for den tekniske infrastrukturen
- skal overvåke vesentlige endringer i trusler mot UiTs informasjonsverdier

## Avdeling for bygg og eiendom

- skal sørge for at sikring av tilgang til bygninger, rom og områder er i tråd med kriterier for akseptabel risiko
- skal bistå enheter ved risikovurderinger av fysisk sikkerhet og ved gjennomføring av nødvendige fysiske sikringstiltak

## Enhetsledere

- er ansvarlige for å tilfredsstille krav til informasjonssikkerhet i egen enhet
- skal gjennomføre risikovurderinger
- skal iverksette tiltak dersom det er nødvendig for å ivareta informasjonssikkerheten i egen enhet
- skal rapportere resultat fra risikovurderinger med handlingsplan og avvik til informasjonssikkerhetsrådgiver
- skal følge opp avviksmeldinger i egen enhet og sørge for at disse blir lukket
- skal informere ansatte i egen enhet om de rutiner og retningslinjer som gjelder til enhver tid og sørge for at kravene i styringssystemet til egen enhet blir fulgt

## Systemeier

- skal etablere og vedlikeholde rutiner for å ivareta sikkerhetsmålene
- skal stille krav til informasjonssikkerhet i anskaffelse, utvikling og vedlikehold av informasjon og informasjonssystemet, i samråd med Avdeling for IT
- skal sørge for at tilganger blir gitt etter tjenstlig behov, avsluttet når behovet opphører, samt at nødvendig opplæring blir gitt
- skal, i samråd med informasjonssikkerhetsrådgiver, sørge for at databehandleravtaler inngås
- skal utføre risikovurdering av systemet i henhold til punkt 4, og dokumentere at risikovurderinger er utført
- skal iverksette eventuelle tiltak på bakgrunn av risikovurderinger

## Brukere av IT-tjenester (ansatte/studenter)

- har plikt til å gjøre seg kjent med og følge de sikkerhetsrutiner og retningslinjer som til enhver tid gjelder for sikker håndtering av informasjonsverdier og personopplysninger
- har plikt til å forhindre og rapportere hendelser som kan innebære avvik, samt rapportere avvik når disse oppstår, gjennom avviksmeldingssystemet

## Computer Security Incident Response Team (CSIRT)

- skal iverksette, eller beordre iverksatt, ethvert tiltak som vurderes som tjenlig for å avverge skade på UiTs IT-systemer og data
- skal rapportere om sikkerhetshendelser, skadepotensial, skadeomfang og iverksatte tiltak til IT-direktøren

## Informasjonssikkerhetsforum

- skal gi råd om tiltak/initiativ som fremmer informasjonssikkerheten
- skal koordinere planleggingen og gjennomføringen av tiltak og initiativ på informasjonssikkerhetsområdet som omfatter hele institusjonen
- skal gjennomgå rapporterte avvik og sikkerhetshendelser, og påse at disse blir lukket
- skal gjennomgå rapport til ledelsens gjennomgang
- skal bidra til implementering av ledelsessystemet i organisasjonen
- skal jevnlig gjennomgå ledelsessystemet for informasjonssikkerhet med tilhørende dokumenter og generelle ansvarsforhold, samt vurdere behov for endringer