Kapittel 1 – Innretning

1. Bakgrunn

Som verdens nordligste universitet er UiT Norges arktiske universitet (UiT) strategisk plassert for å utvikle og formidle kunnskap om Arktis og nordområdene. UiT favner forskning og utdanning om natur, samfunn, teknologi, miljø, kultur, mennesket og samspillet mellom disse. Med faglig bredde og nærhet til natur og samfunn, har UiT forutsetninger til å bidra med kunnskap og kompetanse til omstilling, tilpasning og framtidsrettede løsninger på tvers av fagområder, nærings- og samfunnsliv. UiT har studenter og ansatte fra ulike land og steder, og samarbeider med forsknings- og utdanningsinstitusjoner i inn- og utland, samt med offentlige og private aktører.

UiT er et internasjonalt ledende breddeuniversitet som på grunn av beliggenhet og forskningsprofil kan være spesielt utsatt for trusler og angrep. Aktivister, kriminelle og statlig etterretning forsøker å oppnå økonomisk vinning, politiske mål eller andre fordeler gjennom manipulasjon, sabotasje og spionasje. UiTs forskningsdata kan være spesielt utsatt for fysiske eller digitale sikkerhetsbrudd ved eksempelvis sabotasje og/eller spionasje.

2. Formål og hensikt

Gjennom forebyggende sikkerhet skal UiT redusere sannsynligheten for at en uønsket hendelse inntreffer og redusere konsekvensene ved en slik hendelse. Dette arbeidet må ses i sammenheng med beredskap, som ikke forebygger at en uønsket hendelse finner sted, men omfatter planleggingen i forkant av en hendelse, selve håndteringen når denne enten inntreffer eller er nært forestående, samt den påfølgende gjenopprettingen. Gjennom godt beredskapsarbeid skal UiT på kort varsel kunne øke sikkerhetsnivået.

UiT har en omfattende mengde verdier, informasjon og infrastruktur som må beskyttes og bevares, og dette krever en systematisk og samordnet tilnærming til arbeidet. Dette inkluderer også forsvarlig ivaretagelse av skjermingsverdige verdier, gode rutiner innen eksportkontroll for å forhindre ulovlig kunnskapsoverføring, samt sikre at internasjonalt samarbeid foregår på forsvarlig måte.

Tiltak som er nødvendig for sikkerhetsarbeidet kan være inngripende overfor ansatte, studenter og andre tilknyttet UiT. I vurderingen av hvilke, og hvordan, sikkerhetstiltak skal gjennomføres er det essensielt å samtidig vurdere hvordan personvernet påvirkes og best ivaretas. Videre behandler UiT en stor mengde personopplysninger i alle deler av virksomheten, og god overholdelse av personvernlovverket er viktig for å opprettholde tilliten blant ansatte, studenter, forskningsdeltakere, samarbeidspartnere og gjester.

Hensiktsmessig og god håndtering av disse områdene krever at de ses i sammenheng fremfor hver for seg, og arbeidet organiseres og etableres som en sammenhengende tjeneste. Dette er en utfordrende øvelse, men samtidig nødvendig for at UIT skal oppnå et forsvarlig sikkerhetsnivå, og god ivaretakelse av personvern for alle som er tilknyttet UiT.

For å lykkes med dette har UiT etablert et felles ledelsessystem for sikkerhet, beredskap og personvern.

3. Ledelsessystemets omfang og innhold

Hovedområdene som skal ivaretas gjennom dette ledelsessystemet er informasjonssikkerhet, samfunnssikkerhet, beredskap, personvern, eksportkontroll og nasjonal sikkerhet. Samtlige av disse områdene griper inn i hverandre, og de omfatter det fysiske, menneskelige, organisatoriske og digitale domene. Alle disse domenene kan utgjøre en sårbarhet som kan utnyttes bevisst eller ubevisst, av eksterne eller interne aktører. For å oppnå et tilstrekkelig sikkerhetsnivå er UiT avhengig av å se disse i sammenheng med hverandre, og ta høyde for samspillet mellom disse ulike områdene og nevnte domener. Eksempelvis kan digitale systemer være godt sikret i seg selv, men hvis den fysiske sikringen er svak og en uærlig aktør kommer seg inn i en datahall, kan det gjøres mye skade.

Samfunnsutviklingen og et endret trussel- og risikobilde gjør skillet mellom samfunnssikkerhet og statssikkerhet mer utydelig. Arbeidet med å identifisere og ivareta verdier som er viktige for nasjonal sikkerhet er komplisert, blant annet fordi aktuelle tiltak for overholdelse av sikkerhetsloven og eksportkontrollregelverket kan gripe inn i kjernevirksomheten og potensielt UiTs mulighet for oppfyllelse av samfunnsoppdraget som forskningsinstitusjon.

I dagens høyere utdanning er det stort fokus på læringsfremmende teknologi og digitale eksamensformer, og det er vanskelig å balansere behovet for å hyppig ta i bruk nye tjenester og samtidig ivareta informasjonssikkerheten og personvernet. Både Kunnskapsdepartementet og UiT har ambisiøse digitaliseringsstrategier, og oppfyllelse av disse samtidig som informasjonssikkerhet og personvern ivaretas er en krevende oppgave.

Videre behandler UiT en stor mengde personopplysninger om ansatte, studenter, forskningsdeltakere og andre. Regelverket for lovlig håndtering av personopplysninger er omfattende og kompleks, og det kreves gode retningslinjer, rutiner, verktøy og kunnskap for å sikre at UiT overholder relevant regelverk i all behandling av personopplysninger.

I tillegg kan store ulykker inntreffe som følge av teknisk eller menneskelig svikt, pandemier, forsyningssvikt eller andre katastrofer utløst av utilsiktede hendelser som f.eks naturkatastrofer, eller tilsiktede handlinger fra de som ønsker ramme oss. Slike hendelser kan være i det fysiske eller det digitale rom, eller en kombinasjon. Hendelsene kan være såpass varierte i omfang og type at det er krevende å bygge god beredskap som lar UiT respondere hurtig og tilstrekkelig.

Etableringen av et felles ledelsessystem skal sørge for at UiT har en planmessig og god håndtering av dette komplekse feltet. Ivaretagelse av sikkerhet, beredskap og personvern er et lederansvar, og dette arbeidet skal være en integrert del av den helhetlige virksomhetsstyringen.

Ledelsessystemet for sikkerhet, beredskap og personvern ved UiT omfatter

- alle[1] som får tilgang UiTs informasjonsverdier
- alle UiTs studiesteder/campuser
- alle organisatoriske enheter
- all teknologi[2]
- alle informasjonsverdier[3]
- alle skjermingsverdige verdier (informasjon, objekter og infrastruktur)

Dette ledelsessystemet er avgrenset mot UiTs arbeid innenfor Helse, miljø og sikkerhet (HMS), som er regulert gjennom eget internkontrollsystem. Det påhviler universitetsledelsen å sørge for et godt samspill mellom ledelsessystemet og HMS-systemet.

3.1. Informasjonssikkerhet

Et systematisk og planmessig arbeid for å sikre universitetets informasjonsverdier er 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 sikrer at informasjon i alle former

- ikke blir kjent for uvedkommende (konfidensialitet)
- ikke blir endret utilsiktet eller av uvedkommende (integritet)
- er tilgjengelig ved legitimt behov (tilgjengelighet)

UiT er underlagt en rekke lover og forskrifter som pålegger oss å ha tilfredsstillende informasjonssikkerhet. Dette gjelder blant annet forvaltningsloven, eforvaltningsforskriften, personopplysningsloven (2018), personvernforordningen (GDPR), helseforskningsloven, sikkerhetsloven, virksomhetsikkerhetsforskriften mv. I tillegg inneholder andre lovverk, blant annet offentlighetsloven og arkivloven, bestemmelser som har betydning for

[1] Studenter, ansatte, gjester, samarbeidspartnere etc.
[2] IKT-systemer, datanettverk, databaser/-registre etc.
[3] *Informasjonsverdi* er et samlebegrep som inkluderer både selve informasjonen samt tilhørende støtteverdier som IKT-system, digitale tjenester, datautstyr av ulike varianter mv.

arbeidet med sikring av informasjonen ved UiT. *Ledelsessystemet for sikkerhet, beredskap og personvern* skal ivareta de kravene som lovverket og Kunnskapsdepartementet (KD) stiller til arbeidet med informasjonssikkerhet i universitets- og høyskolesektoren.

3.2. Samfunnssikkerhet og beredskap

Alle aktører i KDs sektor skal jobbe systematisk og helhetlig med samfunnssikkerhet. UiT følger grunnleggende nasjonale prinsipper for arbeidet med samfunnssikkerhet.

Samfunnssikkerhet defineres som samfunnets evne til å verne seg mot og håndtere hendelser som truer grunnleggende verdier og funksjoner og setter liv og helse i fare. Slike hendelser kan være utløst av naturen, være utslag av tekniske eller menneskelige feil eller bevisste handlinger. Beredskap defineres som planlagte og forberedte tiltak som gjør oss i stand til å håndtere uønskede hendelser, slik at konsekvensene blir minst mulig.

Verdiområdene UiT skal beskytte omfatter liv og helse, informasjonssikkerhet, fysiske gjenstander, operativ evne, omdømme, ytre miljø og åpenhet. Arbeidet med samfunnssikkerhet følger KD styringsdokument for arbeid med sikkerhet og beredskap i Kunnskapsdepartementets sektor.

3.3. Personvern

UiT behandler en omfattende mengde personopplysninger, og i tillegg til informasjonssikkerhet påhviler det en rekke øvrige forpliktelser for å sikre godt personvern. Slik som lovlig grunnlag for å samle inn og behandle opplysninger, god og korrekt informasjon om behandlingene, ivaretagelse av rettigheter mv.

Et systematisk og planmessig arbeid for å sikre at UiT overholder disse forpliktelsene i alle ledd er derfor sentralt for å ivareta rettighetene og personvernet til de personene vi behandler opplysninger om, og ivareta den tillit som UiT er avhengig av for å kunne opprettholde og utvikle virksomheten innen forskning, utdanning og formidling.

3.4. Eksportkontroll

Eksportkontroll skal sørge for at sikkerhetspolitikken gjennomføres i praksis, ved at det reguleres og begrenses hvem som får motta hva av forsvarsmateriell, flerbruksvarer, teknologi, kunnskap og tjenester. Dette gjelder både forsvarsmateriell slik som våpen, ammunisjon mv., men også «flerbruksvarer» som i utgangspunktet er sivile varer, men som også har militære anvendelsesområder.

Eksportkontroll retter seg mot to formål:

1. å sikre at eksporten av forsvarsmateriell fra Norge skjer i tråd med norsk sikkerhets- og forsvarspolitikk og
2. at eksporten av flerbruksvarer ikke bidrar til spredning av masseødeleggelsesvåpen (kjernefysiske, kjemiske og biologiske våpen) samt leveringsmidler for slike våpen.

Eksportkontroll reguleres av *lov om eksportkontroll av strategiske varer, tjenester og teknologi m.v*. (eksportkontrolloven) og tilhørende forskrift, eksempelvis målrettede forskrifter om sanksjoner mot enkeltland eller den mer generelle *forskrift om eksport av forsvarsmateriell, flerbruksvarer, teknologi og tjenester*. Dersom eksempelvis teknologi eller kunnskap som omfattes av lovverket skal føres ut av Norge kreves lisens fra Utenriksdepartementet.

3.5. Nasjonal sikkerhet

Sikkerhetsloven skal bidra til å ivareta nasjonale sikkerhetsinteresser, og UiT er omfattet av sikkerhetsloven. Ledelsessystemet er sentralt for at UiT skal klare oppfylle de krav som stilles etter denne lov med forskrift.

Med nasjonale sikkerhetsinteressene menes landets suverenitet, territorielle integritet og demokratiske styreform og overordnede sikkerhetspolitiske interesser knyttet til

a. de øverste statsorganers virksomhet, sikkerhet og handlefrihet
b. forsvar, sikkerhet og beredskap
c. forholdet til andre stater og internasjonale organisasjoner
d. økonomisk stabilitet og handlefrihet
e. samfunnets grunnleggende funksjonalitet og befolkningens grunnleggende sikkerhet

I valg av nødvendige tiltak for tilstrekkelig ivaretagelse av nasjonal sikkerhet skal det tas særlig hensyn til at UiT fremdeles skal kunne oppfylle sitt samfunnsoppdrag, og sikre at akademisk frihet ivaretas.

4. Visjon og overordnet målbilde og prinsipper

UiT skal etablere og opprettholde en forsvarlig sikkerhetskultur, forvaltning, styring og sikring av sine verdier for å ivareta samfunnets tillit til universitetets utdanning, forskning og formidling.

UiT skal:

- arbeide målrettet, systematisk og risikobasert med samfunnssikkerhet, informasjonssikkerhet, beredskap og personvern
- ivareta arbeidet på en helhetlig og felles tilnærming internt på UiT
- redusere sårbarhetene til UiTs informasjonsverdier
- inkludere samfunnssikkerhet, beredskap, informasjonssikkerhet og personvern i universitetets beslutningsprosesser
- forenkle og forbedre universitetets retningslinjer og prosesser for sikkerhet, beredskap og personvern
- forbedre evnen til å oppdage og håndtere hendelser, avvik og brudd raskt slik at eventuelle konsekvenser for virksomheten blir minimale
- sørge for opplæring og bevisstgjøring som gjør ledere, ansatte og studenter i stand til å hindre, oppdage og rapportere hendelser
- Inkludere samfunnssikkerhet, beredskap, informasjonssikkerhet og personvern som faste tema i ledermøter og -opplæring

4.1. Overordnet målbilde for UiT

A. Helhetlig, integrert og effektiv styring og kontroll

Bygge opp og opprettholde nødvendig organisasjon, styring av sikkerhet, beredskap og personvern, prosesser og støtteverktøy. Sikkerhet- og personvernaktiviteter skal være integrert i UiTs prosesser.

B. Overvåkning og hendelsesstyring

Sikkerhetsarbeidet bør i størst mulig grad søke å forebygge uønskede hendelser. Dette kan vi oppnå ved å sørge for tiltak som gjør det mulig ikke bare å oppdage hendelser og brudd, men også håndtere og redusere konsekvensene av disse. Dette har derfor sterk tilknytning til beredskapsområdet.

C. Ansvarsbevisst kultur

Etablere og vedlikeholde en kultur hvor ansatte og studenter er bevisst på sitt ansvar og oppgaver innenfor sikkerhet, beredskap og personvern, og har vilje og evne til å ivareta UiTs informasjonsverdier.

Arbeidet med å oppnå det overordnede målbildet må bygges lagvis, over tid. Det har ingen sluttdato da det ikke bare må etableres, men også opprettholdes i en stor og kompleks organisasjon med et dynamisk risiko- og trusselbilde.

For å oppnå det overordnede målbildet er det fastsatt et sett med delmål i hver kategori, og årlig skal det vedtas tiltak for å oppnå disse delmålene gjennom et veikart. Også her vil det ofte være ulike tiltak over tid som innebærer at delmålet oppnås, og deretter må tiltak gjennomføres for å opprettholde og vedlikeholde dette.

4.2. Prinsipper for håndtering av hendelser og kriser

Utformingen av beredskapsplanverk og retningslinjer for håndtering av hendelser og ansvar skal følge fire prinsipper:

- *Ansvarsprinsippet* innebærer at personene som har ansvar for en enhet eller funksjon i en normalsituasjon også har ansvaret ved avvik eller kritisk hendelse. Dette følger lederansvaret på UiT.
- *Likhetsprinsippet* innebærer at den organisasjonen man opererer med i en beredskapssituasjon, skal være mest mulig lik den organiseringen man har til daglig.
- *Nærhetsprinsippet* innebærer at kriser og hendelser skal håndteres på lavest mulig nivå, hvor nødvendig kompetanse og ressurser er til stede.
- *Samvirkeprinsippet* innebærer at beredskapsenhetene har et selvstendig ansvar for å sikre best mulig samvirke med relevante aktører og virksomheter i arbeidet med forebygging, beredskap og krisehåndtering.

5. Risikostyring

Risikobildet til UiT er dynamisk og vil variere over tid. Derfor er det nødvendig å arbeide systematisk med risikostyring og akseptabel risiko. En effektiv risikostyring skal gi studenter og ansatte best mulig grunnlag til å forstå hvor stor risiko UiT er villig til å akseptere i prosessen med å skape verdier. UiT har en risikobasert tilnærming til ivaretagelsen av sikkerhet og beredskap.

Håndtering av risiko er sentralt for god ivaretagelse av informasjonssikkerhet, personvern, samfunnssikkerhet, fysisk- og personellsikkerhet, brann og beredskap, og nasjonal sikkerhet. Ofte kan risiko reduseres til et akseptabelt nivå gjennom tiltak, men i noen tilfeller er risikoen for høy til at man kan gjennomføre de aktuelle prosjektene, anskaffe de ønskede systemene mv. Dette kan være fordi det ikke finnes tiltak eller tiltakene blir for kostbare å gjennomføre.

Vurdering av risiko skal skje innenfor de rammene som er fastsatt i ledelsessystemet, og det er noen forskjeller i hvordan risiko vurderes innenfor de ulike områdene, se kap. 4. Gjennomføring av risikovurderinger vil være avhengig av at man vet hvilke verdier som behandles, herunder hvordan disse klassifiseres. Se kap. 3 for regulering og informasjon om verdivurdering og klassifisering.

Det er ikke mulig å eliminere enhver risiko, men UiT skal arbeide systematisk og målrettet for å ha et risikonivå som er akseptabelt, sett opp mot UiTs mål og risikobilde. UiT har fastsatt grenser for akseptabel risiko innenfor informasjonssikkerhet og samfunnssikkerhet.

5.1. Verdiområder og akseptkriterier samfunnssikkerhet

UiTs verdiområder og akseptkriterier omfatter følgende:

Verdiområde	**UiTs sikringsmål for verdiområdet (akseptkriterier)**
Liv og helse	**Nullvisjon** UiT aksepterer *ikke* tap av liv og alvorlig tap av helse hos ansatte, studenter og gjester. Dette gjelder også der liv og helse blir berørt i de øvrige satte verdiområdene.
Informasjonssikkerhet	Se egen tabell med akseptkriterier for informasjonssikkerhet
Fysiske gjenstander	UiT aksepterer *ikke* katastrofale eller kritiske konsekvenser som rammer kjernevirksomheten forskning, utdanning og formidling
Operativ evne	UiT aksepterer *ikke* katastrofale eller kritiske konsekvenser som rammer kjernevirksomheten forskning, utdanning og formidling.
Omdømme	UiT aksepterer *ikke* katastrofale eller kritiske konsekvenser for omdømmet relatert til liv og helse, kjernevirksomheten forskning, utdanning og formidling
Ytre miljø	UiT aksepterer *ikke* katastrofale eller kritiske konsekvenser som rammer det ytre miljø og berører kjernevirksomheten forskning, utdanning og formidling
Åpenhet	UiT aksepterer *ikke* katastrofale eller kritiske konsekvenser som rammer UiTs verdigrunnlag, deriblant den akademiske frihet og stor åpenhet i kommunikasjonen ved UiT

Verdiområdene skal beskyttes uavhengig av analysemetode.

5.2. Akseptabel risiko innenfor informasjonssikkerhet

UiT skal ha en risikobasert tilnærming til informasjonssikkerhet, og «akseptabel risiko» er det nivå av risiko UiT er villig til å godta for å skape verdier samt oppnå de mål og gevinster som søkes.

Uønskede hendelser kan gi brudd på informasjonssikkerheten, og da menes brudd på informasjonens

- **Konfidensialitet:** informasjonen skal ikke bli kjent for uvedkommende
- **Integritet:** informasjonen skal ikke bli endret utilsiktet eller av uvedkommende
- **Tilgjengelighet:** informasjonen er tilgjengelig ved legitimt behov

Yttergrensen for akseptabel risiko (skal ikke overstiges)

	Undervisning og utdanning	**Forsknings- og utviklingsarbeid (FoU)**	**Formidling**	**Administrasjon**
Konfidensialitet	UiT er ikke villig til å ta risiko som kan medføre at taushetsbelagte opplysninger kommer på avveie.	UiT er ikke villig til å akseptere brudd på konfidensialiteten til forskningsdata som ikke er godkjent for publisering/offentliggjøring.	UiT er ikke villig til å akseptere at fortrolig informasjon formidles. Dette ville sette legitimiteten til forskningen i tvil og medføre brudd på lover og regler.	Fortrolig informasjon skal sikres forsvarlig og det aksepteres ikke brudd som kan medføre fare for liv og helse.
Integritet	Det skal ikke risikeres utilsiktet tap av integritet til eksamensresultater og oppnådde kvalifikasjoner.	Integritet av forskningsdata er helt kritisk, og UiT er ikke villig til å akseptere risiko som sår tvil om integriteten.	Det aksepteres ikke formidling av informasjon hvor nøyaktigheten, fullstendigheten eller opprinnelsen er i tvil.	UiT er ikke villig til å akseptere brudd på integritet til informasjon som ligger til grunn for beslutninger
Tilgjengelighet	Tilgjengeligheten til digital eksamen må ivaretas	UiT er ikke villig til å akseptere risiko knyttet til permanent tap av forskningsdata.	UiT er ikke villig til å akseptere risiko knyttet til permanent tap av forskningsdata.	Det aksepteres ikke nedetid som er vedvarende eller har alvorlig konsekvens for data og informasjonssystemene (f.eks. brukeradministrative- eller økonomisystemet).

6. Oppbygning av ledelsessystemet

Ledelsessystemet består av tre hovedelementer:

- **Styrende del** – innretning, visjon og mål, risikostyring samt roller, oppgaver og ansvar
- **Gjennomførende del** – konkrete retningslinjer og rutiner, herunder om klassifisering av informasjon, risiko- og personvernkonsekvensvurdering, grunnleggende sikring av det digitale og fysiske domenet, organisatoriske og menneskelige tiltak.
- **Kontrollerende del** – internrevisjon og -kontroll, rapportering og håndtering av hendelser og avvik samt ledelsens gjennomgang/årsrapport.

Kapitteloversikt

	Kapittelnummer	***Kapittel***
Styrende del	1	Innretning
	2	Roller, ansvar og oppgaver
Gjennomførende del	3	Klassifisering og verdivurdering
	4	Risiko- og personvernkonsekvensvurdering
	5	Fysisk sikkerhet
	6	Digital sikkerhet
	7	Personellsikkerhet
	8	Beredskap
	9	Anskaffelser/vedlikehold/utvikling
	10	Personvern
	11	IKT-ressurser og brukere
	12	Internasjonalt samarbeid og eksportkontroll
Kontrollerende del	13	Internkontroll og -revisjon
	14	Håndtering av hendelser og avvik
	15	Ledelsens gjennomgang/årsrapport