Kapittel 2 - Visjon, mål og akseptabel risiko

2.1 Visjon og overordnede mål for informasjonssikkerhet og personvern ved UiT

UiT er et breddeuniversitet som på grunn av beliggenhet og forskningsprofil kan være spesielt utsatt for trusler og angrep knyttet til informasjonssikkerhet. 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 informasjonssikkerhetsbrudd ved eksempelvis sabotasje og/eller spionasje.

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 komplisert, og det kreves gode retningslinjer, rutiner, verktøy og kunnskap for å sikre at UiT overholder relevant regelverk i all behandling av personopplysninger.

Internt ved UiT har vi en sikkerhetskultur som ikke sammenfaller med risikonivået. Uten å gjennomføre tilstrekkelige tiltak for å sikre UiTs informasjonsverdier vil sannsynligheten for et større sikkerhetsbrudd være uakseptabelt høy. Slike brudd kan medføre at legitimiteten og omdømmet til UiT rammes. Det inkluderer å forbedre evnen til å oppdage og håndtere hendelser, avvik og brudd raskt slik at eventuelle konsekvenser for kjernevirksomheten blir minimale, og redusere sannsynligheten for at forskningens troverdighet eller legitimitet rammes.

For å sikre at arbeidet med informasjonssikkerhet og personvern ivaretas på en systematisk og hensiktsmessig måte har UiT identifisert et sett med overordnede, langsiktige mål og en visjon for informasjonssikkerhet og personvern. Tiltak for å oppfylle disse vil fastsettes gjennom *Veikart for informasjonssikkerhet og personvern*, som har en varighet på 12 måneder og fastsettes av Universitetsstyret. Veikartet behandles som hovedregel sammen med *Årsrapport for informasjonssikkerhet og personvern.*

2.1.1 Visjon

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

UiT skal:

- arbeide målrettet og risikobasert med informasjonssikkerhet og personvern
- ivareta informasjonssikkerhet og personvern på en helhetlig og systematisk måte, og sørge for en felles tilnærming internt på UiT
- redusere sårbarhetene til UiTs informasjonsverdier
- inkludere informasjonssikkerhet og personvern i universitetets beslutningsprosesser
- forenkle og forbedre universitetets retningslinjer og prosesser for informasjonssikkerhet 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 ansatte og studenter i stand til å hindre, oppdage og rapportere hendelser

2.1.2 Overordnet målbilde for UiT

A. Helhetlig, integrert og effektiv styring og kontroll

Bygge opp og opprettholde nødvendig organisasjon, styring av informasjonssikkerhet 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.

C. Ansvarsbevisst kultur

Etablere og vedlikeholde en kultur hvor ansatte og studenter er bevisst på sitt ansvar og oppgaver innenfor informasjonssikkerhet 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. Delmålene og tilhørende tiltak fremgår av veikartet.

2.2 Akseptabel risiko

Introduksjon

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 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.

Risikovilje kan kategoriseres på ulike måter:

- **Uvillig:** Skal unngå risiko.
- **Minimalistisk:** Ekstremt konservativt.
- **Forsiktig:** Bør unngå unødvendig risiko.
- **Fleksibel:** Vil ta sterkt begrunnede risikoer.
- **Åpen:** Vil ta berettiget risiko.

For høy risikovilje fra UiTs side vil utsette ansatte, studenter og forskningsdeltakere for en uholdbar risiko for skade og negative konsekvenser, samt kunne skade UiTs omdømme og/eller få økonomiske konsekvenser. For lav risikovilje vil innebære at prosjekter, prosesser, aktiviteter mv. i liten grad er gjennomførbare enten fordi det ikke er mulig å få risikoen ned på et svært lavt nivå, eller det vil være uforholdsmessig tidkrevende og dyrt. Det vil kunne ha store negative virkninger for UiTs virksomhet.

Jo sterkere og bedre sikkerhetskultur, grunnsikring og systematikk rundt arbeidet med informasjonssikkerhet i hele virksomheten, desto større vil mulighetsrommet være for å kunne gjennomføre ambisiøse prosjekter og prosesser som i en organisasjon med svakere sikkerhetskultur og -arbeid vil innebære en uakseptabel risiko. Både UiTs risikobilde og totale grunnlag for å håndtere risiko på en ansvarlig og tillitvekkende måte vil være dynamisk, og må kontinuerlig vurderes, herunder måle sikkerhetskulturen blant ansatte og studenter.

Som hovedregel vil derfor «akseptabel risiko» befinne seg i tre midterste kategoriene («minimalistisk», «forsiktig» og «fleksibel»). Dette kan variere basert på eksempelvis type data som behandles, hvilke gevinster som søkes oppnådd og hvilken risiko det vil innebære å ikke igangsette en prosess, gjennomføre et forskningsprosjekt, ta i bruk et IT-system mv. Det er imidlertid ikke fritt opp til den enkeltes skjønn hvordan risiko skal vurderes, eller hvilke *risikonivå* som kan aksepteres. Nedenfor vil det derfor redegjøres for hvordan UiT vurderer risiko, samt grensene for *akseptabel risiko.*

Risikonivå

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

Brudd på informasjonssikkerheten kan få følger for alle deler av UiTs virksomhet, eksempelvis:

	Et sikkerhetsbrudd kan medføre at:
UTDANNING	UiT rekrutterer færre studenter, som igjen kan føre til økonomiske konsekvenser for universitetet. I tillegg kan et brudd føre til personlige og/eller psykologiske konsekvenser for studenter.
FoU	UiTs samfunnsbidrag reduseres, tap av økonomisk støtte, legitimitet og omdømme, og/eller brudd på lover og regler. I ytterste konsekvens kan det også være fare for liv og helse som følge av manipulering og forfalskning av forskningsdata/-resultater
FORMIDLING	Troverdigheten til og legitimiteten av verdiene som skapes ved UiT trekkes i tvil. Tap av troverdighet og legitimitet kan medføre økonomiske konsekvenser.
ADMIN.	UiT utsettes for økonomisk tap grunnet brudd på lov (f.eks. GDPR), søksmål eller ikke planlagt nedetid. Dårlig sikring av miljø eller systemer kan i ytterste konsekvens være en fare for liv og helse.

Risikonivået er summen av sannsynlighet for at en uønsket hendelse inntreffer, og konsekvensen dersom den inntreffer. Dette kartlegges og vurderes gjennom *risikovurderinger* (se ledelsessystemets kap. 5).

Sannsynligheten for at en uønsket hendelse inntreffer vurderes på en skala fra 1 – 4, etter et sett med kriterier som UiT har fastsatt.

Konsekvensen dersom en uønsket hendelse skulle inntreffe vurderes på en skala fra 1 – 4, etter et sett med kriterier som UiT har fastsatt.

Risikonivået for de uønskede hendelsene kategoriseres på fire nivåer:

- **7 – 8** Svært høy risiko
- **6** Høy risiko
- **4 – 5** Moderat risiko
- **2 – 3** Lav risiko

For å sikre at det på tvers av organisasjonen er en mest mulig lik og korrekt vurdering av hvilken risiko UiT er villig til å akseptere, er det nødvendig å sette noen overordnede krav til håndtering av identifiserte risikoer, se nedenfor under «krav til håndtering av identifiserte risikoer (uønskede hendelser»).

Videre er det nødvendig å sette noen mer absolutte yttergrenser som ikke skal passeres, uansett hvilken gevinst som kan oppnås. Sistnevnte fastsettes av Universitetsstyret, se nedenfor under «yttergrensen for akseptabel risiko».

Typen data, og tilhørende klassifisering etter UiTs *retningslinjer for klassifisering av informasjon* (kap. 4 i ledelsessystemet), vil være en sentral del av grunnlaget for vurderingen.

Krav til håndtering av identifiserte risikoer (uønskede hendelser)

7-8	Risikoreduserende tiltak **skal** gjennomføres. Hvis risikoen ***ikke*** kan reduseres ned fra rødt nivå **gjennom tiltak** gjelder følgende: • Dersom risikoen er knyttet til den type data, aktiviteter og prosesser hvor Universitetsstyret har satt yttergrenser for akseptabel risiko (se tabell nedenfor), **kan ikke** prosjektet, prosessen, endringen, IT-tjenesten/systemet mv. igangsettes. • Dersom risikoen knytter seg til mulige ***konfidensialitetsbrudd*** for strengt fortrolige/svarte data, **kan ikke** ○ prosjektet, prosessen, endringen mv. igangsettes, ○ IT-tjenester/systemer godkjennes for bruk til denne typen data. • Dersom risikoen knytter seg til mulige ***integritetsbrudd*** for data underlagt UiTs høyeste krav til integritet, **kan ikke** ○ prosjektet, prosessen, endringen mv. igangsettes, ○ IT-tjenester/systemer godkjennes for bruk til denne typen data. • Dersom risikoen knytter seg til mulige ***tilgjengelighetsbrudd*** for data underlagt UiTs høyeste krav til tilgjengelighet, **kan ikke** ○ prosjektet, prosessen, endringen mv. igangsettes, ○ IT-tjenester/systemer godkjennes for bruk til denne typen data. • For øvrige risikoer og/eller data må beslutningen om risikoen er akseptabel tas av enhetsleder*, sett ut fra type data, situasjon, lovkrav, mulige gevinster og eventuelle negative konsekvenser ved å unnlate gjennomføringen/innføringen.
6	Dersom risikoen ***ikke*** kan reduseres ned fra oransje nivå **gjennom tiltak**: - Beslutningen om risikoen er akseptabel må tas av enhetsleder*, sett ut fra type data, situasjon, lovkrav, mulige gevinster og eventuelle negative konsekvenser ved å unnlate gjennomføringen/innføringen.
4-5	• *Risikonivå 5:* Risikoreduserende tiltak skal gjennomføres. • *Risikonivå 4:* Risikoreduserende tiltak skal vurderes, og som hovedregel gjennomføres.
2-3	Risikoreduserende tiltak kan vurderes.

** Med enhetsleder menes dekan, direktør UMAK, direktør UB, avdelingsdirektør. Rektor og administrasjonsdirektør kan også fatte disse beslutningene.*

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).