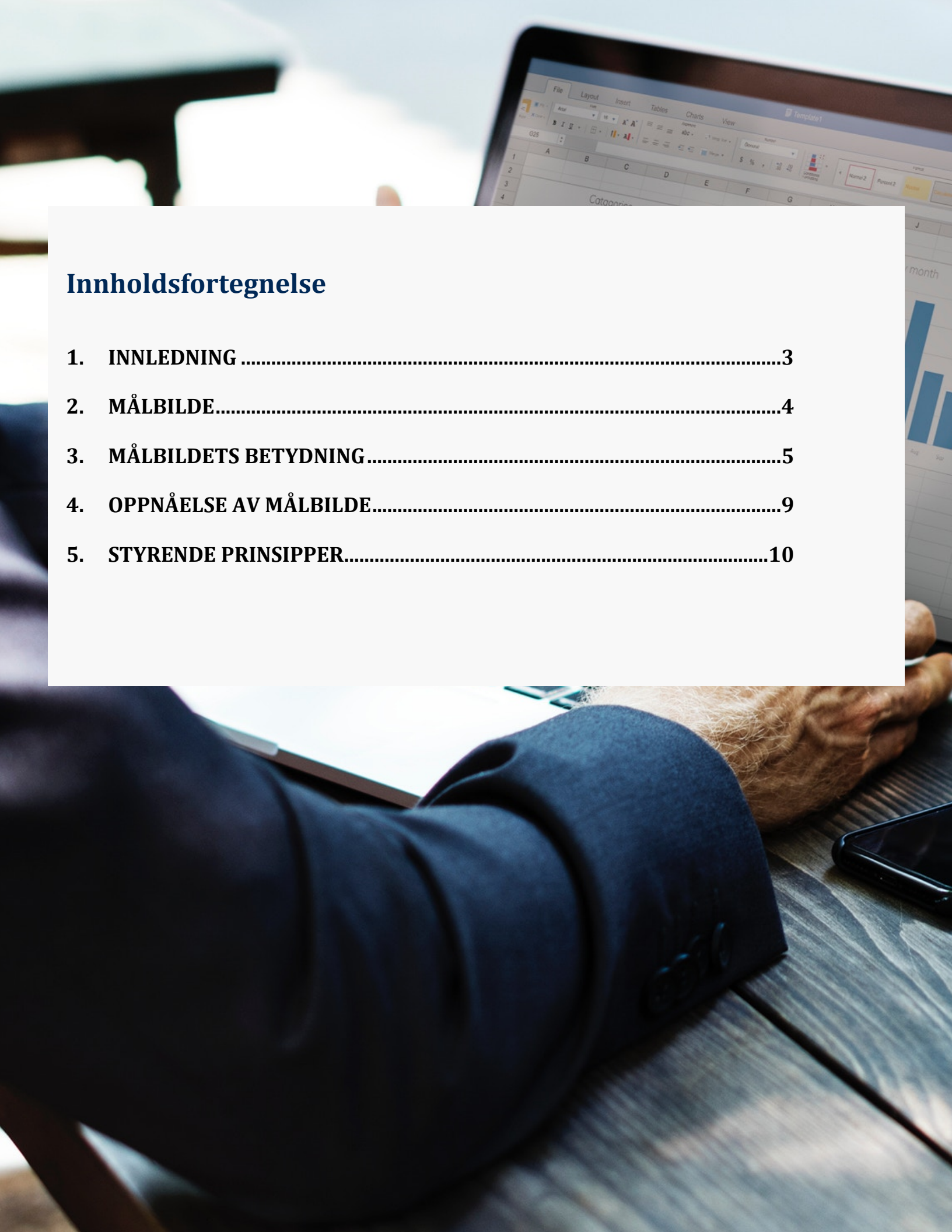
Strategi for informasjonssikkerhet

2019 – 2021

UiT Norges arktiske universitet

Versjon: v 1.1

Postboks 6050 Langnes, N-9037 Tromsø / 77 64 40 00 / postmottak@uit.no / uit.no



Innholdsfortegnelse

Strategi for informasjonssikkerhet

1. INNLEDNING

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.

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 svekkes.

Både Kunnskapsdepartementet og UiT har utarbeidet ambisiøse digitaliseringsstrategier som vil kreve store endringer for hvordan UiT håndterer informasjonssikkerhet. Disse endringene må gjennomføres for å sikre universitetets kritiske informasjonsverdier.

Denne strategien angir mål og prioriteringer for å sikre UiTs informasjonsverdier, slik at tilliten til universitetets utdanning, forskning og formidling ivaretas.

Informasjonssikkerhet *handler om å sikre informasjonens konfidensialitet, integritet og tilgjengelighet.*

Informasjonsverdi *er et samlebegrep som inkluderer både informasjon og tilhørende støtteverdier som IKT-system, digitale tjenester, datautstyr av ulike varianter mv.*

Flere begreper defineres i vedlegg 3

Figur 1 - Visjon for informasjonssikkerhet

Visjon

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

UiT skal:

- arbeide målrettet og risikobasert med informasjonssikkerhet
- ivareta informasjonssikkerhet på en helhetlig og systematisk måte og sørge for en felles tilnærming til informasjonssikkerhet
- redusere sårbarhetene til UiTs informasjonsverdier
- inkludere informasjonssikkerhet i universitetets beslutningsprosesser
- forenkle og forbedre universitetets retningslinjer og prosesser for informasjonssikkerhet

2. MÅLBILDE

Figur 2 - Målbilde for informasjonssikkerhet i 2021

Effektiv sikkerhetsstyring

UiT skal implementere en helhetlig sikkerhetsstyring av universitetets informasjonsverdier.

Målet realiseres bl.a. gjennom:

- god forankring hos ledelsen
- tilfredsstillende sikkerhetsdokumentasjon
- tydelig ansvarsfordeling og organisering i sikkerhetsarbeidet
- å etablere og kontinuerlig følge opp konkrete mål for sikkerhetsarbeidet
- strukturerte styringsmetoder som inkluderer: planlegging, risikovurderinger, tiltak, oppfølging og kontroll, og rapportering

Helhetlig oversikt og kontroll

Modernisere sikkerhetsarkitekturen ved å implementere sikkerhetsaktiviteter og rutiner som integreres i UiTs arbeidsprosesser og IT systemer.

Målet realiseres bl.a. gjennom:

- kontinuerlig kontroll av sikkerhetsrutiner
- samarbeid med systemeiere om langsiktige forbedringstiltak
- å sikre at IT-drift er tilpasset UiTs aksepterte risikonivå
- at kontrollaktiviteter og avvik er beskrevet og klassifisert
- å tilpasse seg anerkjente standarder (ISO/IEC 27001) i henhold til føringer fra KD

Overvåking og hendelsesstyring[1]

Etablere en mer systematisk overvåkingstjeneste for raskere å identifisere, følge opp og lære av uønskede hendelser.

Målet realiseres bl.a. gjennom:

- å innføre mekanismer og prosesser som reduserer tiden fra en sikkerhetshendelse oppstår til den oppdages og stoppes
- automatisk og manuell analyse av data, samt hendelsesinformasjon og rapporter
- oppdatert og testet kontinuitets- og beredskapsplan
- kontinuerlig overvåking av tjenester, systemer og IKT-infrastruktur

Ansvarsbevisst sikkerhetskultur

Gjennomføre opplæring slik at alle ved UiT har nødvendig kunnskap om informasjonssikkerhet, og er bevisst sitt ansvar i sikringen av UiTs informasjonsverdier.

Målet realiseres bl.a. gjennom:

- å bevisstgjøre studenter og ansatte om hvilke risikoer de må være oppmerksomme på når de håndterer informasjonsverdier på vegne av UiT
- å overføre kunnskap og motivere for god sikkerhetsatferd
- å etablere et sikkerhetsutvalg

[1] Overvåking her referer til monitorering av fysiske områder, teknisk komponenter, logger, mv, avhengig av eksponert nivå for risiko. Hva som skal overvåkes og hvordan det skal skje er en del av tiltakets utforming.

3. MÅLBILDETS BETYDNING

Utdanning

I dagens høyere utdanning er det stort fokus på bruk av læringsfremmende teknologi og digitale eksamensformer. Det kan gjøre det vanskeligere å balansere behovet for hyppig å ta i bruk nye tjenester, og samtidig ivareta informasjonssikkerheten.

UiT skal jobbe aktivt for å balansere disse behovene og sikre at teknologiløsningene gir tilstrekkelig beskyttelse av informasjonsverdiene til studenter og ansatte.

Figur 3 - Målbildets betydning for utdanning:

Effektiv sikkerhetsstyring	Sikre at studenters og ansattes informasjonsverdier ivaretas på en forsvarlig måte.
Helhetlig oversikt og kontroll	Sikre at teknisk utstyr og utdanningstjenester ivaretar studenters og ansattes behov for informasjonssikkerhet.
Overvåking og hendelsesstyring	Sikre at studenter og ansatte har en hverdag uten alvorlige avvik og sikkerhetshendelser. Eventuelle avvik og hendelser skal håndteres systematisk og effektivt.
Ansvarsbevisst sikkerhetskultur	Opplæring og bevisstgjøring skal gjøre ansatte og studenter i stand til å hindre, oppdage og rapportere sikkerhetshendelser.

Forskning og utviklingsarbeid (FoU)

UiTs forskningsdata kan være spesielt utsatt for informasjonssikkerhetsbrudd ved eksempelvis sabotasje og/eller spionasje.

UiT skal opptre som en tillitsverdig aktør og sikre integriteten til forskningen ved å prioritere tiltak som aktivt forhindrer brudd på informasjonssikkerheten. UiT skal tilby opplæring til forskere slik at de er bevisst sin rolle i sikring av egne forskningsdata.

UiT skal sikre at forskningsdata blir beskyttet og forvaltet på en forsvarlig måte.

Figur 4 - Målbildets betydning for FoU:

Effektiv sikkerhetsstyring	Tilby tjenester som sikrer evnen til å bevare integritet, konfidensialitet og tilgjengelighet til forskningsdata i åpne og selvstendige forskningsmiljø.
Helhetlig oversikt og kontroll	Forbedre beskyttelsesevnen til IT-infrastruktur, teknologi og løsninger som understøtter forskeres behov for autonomi.
Overvåking og hendelsesstyring	Forbedre evnen til å oppdage og håndtere hendelser, avvik og brudd raskt slik at eventuelle konsekvenser for forskningen blir minimale.
Ansvarsbevisst sikkerhetskultur	Gi faglige enheter og forskere kompetanse til å oppdage mulige sikkerhetsavvik i sitt arbeid.

Formidling

En av UiTs kjerneoppgaver er å formidle forskningsresultater til samfunnet.

UiT skal sikre at informasjonen som formidles ikke har blitt endret utilsiktet eller av uvedkommende. Videre skal det jobbes aktivt med bevisstgjøring og opplæring slik at både forskere og formidlere er i stand til å identifisere mulige avvik før formidlingen skjer.

Figur 5 – Målbildets betydning for formidling:

Effektiv sikkerhetsstyring	Gi faglig rådgivning og støtte for å sikre at konfidensiell informasjon ikke formidles.
Helhetlig oversikt og kontroll	Sikre formidlingsplattformer og samhandlings- og publiseringsteknologi mot inntrengere eller avvik.
Overvåking og hendelsesstyring	Raskt identifisere hendelser, avvik og brudd for å hindre eller redusere sannsynligheten for at forskningens troverdighet eller legitimitet rammes.
Ansvarsbevisst sikkerhetskultur	Øke kompetansen og evnen til å oppdage eventuelle avvik før forskningen formidles.

Administrasjon

Administrasjonen ved UiT skal legge til rette for høy kvalitet i utdanning, forskning og formidling. Dette inkluderer å tilby løsninger som tilrettelegger for deling av data, bruk av fellestjenester, samt standardiserte og effektive administrative arbeidsprosesser.

Det skal jobbes på tvers av enhetene slik at informasjonsverdiene blir tilstrekkelig sikret, særlig med tanke på ivaretakelse av personvernet.

Figur 6 - Målbildets betydning for administrasjon:

Effektiv sikkerhetsstyring	Øke evnen til å systematisere sikkerhetsarbeidet, samt klargjøre roller og ansvar for risikostyring.
Helhetlig oversikt og kontroll	Alle tjenester, data og systemer skal kartlegges og sikres mot uautorisert tilgang eller uaktsomhet, slik at man forhindrer at informasjon kommer på avveie eller blir endret.
Overvåking og hendelsesstyring	Øke evnen til å identifisere mulige brudd på kritiske tjenester for å kunne forhindre avvik.
Ansvarsbevisst sikkerhetskultur	Økt ressursbruk og utvikling av sikkerhetskompetanse forbedrer UiTs evne til å sikre tjenestene i administrasjonen.

4. OPPNÅELSE AV MÅLBILDE

Det finnes mange trusselaktører med vilje og evne til å utføre angrep mot UiTs informasjonsverdier. Nye metoder må derfor tas i bruk for å forebygge, oppdage, håndtere og styre hendelser. Dette for å beskytte informasjonsverdiene og ivareta samfunnsoppdraget og tilliten til UiT.

Risiko og tiltak må kontinuerlig vurderes, forankres, besluttes og gjennomføres. Prioriteringen og omfanget av arbeidet må styres av sikkerhetsrisikoen UiT til enhver tid er eksponert for, og det akseptable risikonivået som gjelder for den enkelte informasjonsverdien.

For å lykkes er det nødvendig med kompetanse, kulturendring, bevisstgjøring og mer systematikk i informasjonssikkerhetsarbeidet ved UiT. Tiltakene må vurderes opp mot evnen til å redusere risiko og ivaretakelse av informasjonsverdienes konfidensialitet, integritet og tilgjengelighet.

Figur 7 - Tiltak for oppnåelse av målbilde

5. STYRENDE PRINSIPPER

Styrende prinsipper for informasjonssikkerhet er definert som en del av strategien og gir retning for løpende prioriteringer, beslutninger og ønsket atferd i strategiperioden. Prinsippene **uttrykker mål, prioriteringer og strategiske føringer** for UiT. Disse kan fravikes, men det skal i så fall dokumenteres og godkjennes.

Tabell 1 – Styrende prinsipper for informasjonssikkerhet ved UiT

1	Alle har et personlig ansvar for informasjonssikkerheten.
2	Alle brukere skal gjennomføre nødvendig opplæring i informasjonssikkerhet
3	Informasjon skal sikres slik at personvernet ikke krenkes.
4	Informasjonsverdier skal ivaretas i henhold til gjeldende lover, forskrifter, interne retningslinjer og føringer fra myndighetene.
5	Klassifisering og håndtering av data skal vurderes i alle tjeneste-, system- og teknologivalg.
6	Informasjonssikkerhet skal ivaretas i virksomhetsstyring og kvalitetsarbeid.
7	Informasjonsobjekter skal kontinuerlig kartlegges og behandlingen risikovurderes.
8	Aktiviteter og prosjekter skal styres innenfor akseptabelt risikonivå.

Vedlegg 1: Akseptabel risiko

Risikobildet til UiT er dynamisk og vil variere over tid, derfor er det nødvendig å jobbe 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.

Akseptabel risiko erstatter ikke behovet for risikovurderinger, men skal sikre god balanse mellom de målene UiT ønsker å oppnå og kravene til formasjonssikkerhet.

Følgende tabell gir et utgangspunkt for bruk av akseptabel risiko i risikovurderingsarbeidet. For mer informasjon om hvordan en selv kan foreta en risikovurdering mtp. akseptabel risiko ta kontakt med en av UiTs informasjonssikkerhetsrådgivere.

Akseptabel risiko: *Risikoen UiT er villig til å godta.*

Konfidensialitet: *Uvedkommende skal ikke få kjennskap til informasjon/data*

Integritet: *Informasjon må være sikret mot utilsiktet eller uautorisert endring eller sletting*

Tilgjengelighet: *Dataene er tilgjengelig ved behov*

Figur 8 - Akseptabel risiko innen utdanning, FoU, formidling og administrasjon

	Et sikkerhetsbrudd kan medføre at:	Akseptabel risiko
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.	UiT aksepterer et høyt risikonivå der det er nødvendig for å kunne tilby tilstrekkelig kvalitet i utdanningene. Dette skal ikke gå på bekostning av integriteten til eksamensresultater og kvalifikasjonene som studentene har oppnådd. UiT har lav toleranse for brudd som medfører personlige konsekvenser for studenter eller økonomisk tap for universitetet.
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.	UiT aksepterer et middels til høyt risikonivå ved FoU-aktiviteter. Aktivitetene må likevel ikke være i strid med UiTs etiske retningslinjer eller forårsake brudd på lover og regler. UiT aksepterer ikke risiko forbundet med tap av integritet i forskningen.
FORMIDLING	Troverdigheten til og legitimiteten av verdiene som skapes ved UiT trekkes i tvil. Tap av troverdighet og legitimitet kan medføre økonomiske konsekvenser.	UiT er ikke villig til å akseptere risiko som medfører at universitetets omdømme, troverdighet og legitimitet settes i fare.
ADM.	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.	For å nå de strategiske målene er UiT villig til å akseptere et middels til høyt risikonivå. UiT aksepterer imidlertid ikke risiko som er i strid med universitetets verdier, medfører lovbrudd eller er forbundet med fare for liv og helse.

Vedlegg 2: Ansvarsfordeling

For å ivareta effektiv styring av informasjonssikkerhet må ansvarsfordelingen i UiT tydeliggjøres.

Følgende ansvar tilhører enhetene:

Ivareta UiTs krav for informasjonssikkerhet og etterleve relevante lovverk

Dette innebærer bl.a. at:

- Ansvaret for ivaretagelse av informasjonssikkerhet ligger hos enhetene
- Enhetene skal følge gjeldende retningslinjer, protokoller og rutiner utarbeidet av UiT

Samarbeide med informasjonssikkerhetsrådgiver for å sikre effektiv avviks- og hendelseshåndtering

Dette innebærer bl.a. å:

- Melde mulige avvik eller hendelser
- Informere underliggende enheter når det forekommer alvorlig avvik eller hendelser som kan medføre en konsekvens for flere
- Følge opp og implementere tiltak hvor nødvendig

Implementere nødvendig risikostyring

Dette innebærer bl.a. å:

- Gjennomføre risikovurderinger av prosjekter, aktiviteter og systemer enheten er ansvarlig for
- Holde oversikt over eventuelle egne løsninger som brukes for å lagre eller behandle fortrolig informasjon
- Sikre at studenter og ansatte tilhørende enheten gjennomfører nødvendig opplæring og etterlever de kravene UiT stiller

Følgende ansvar tilhører informasjonssikkerhet sentralt:

Forvaltning av informasjonssikkerhet

Ansatte med tildelt ansvar for informasjonssikkerhet (bl.a. informasjonssikkerhetsrådgiver) skal være aktive tilretteleggere for enhetene. De skal utforme rutiner, prosedyrer, samt iverksette organisatoriske, operative og tekniske tiltak som sikrer UiT sine informasjonsverdier. Informasjonssikkerhetsrådgivere skal gi støtte til enhetene ved bl.a. kontinuerlig opplæring og veiledning.

Vedlegg 3: Begreper

Begrep	Beskrivelse
UiT	Universitetet i Tromsø - Norges arktiske universitet
Akademisk frihet	Retten til fritt å kunne forske, undervise, uttale seg og publisere i tråd med anerkjente akademiske normer og standarder uten å bli utsatt for sanksjoner.
Akseptabel risiko	Hva UiT er villig til å akseptere av risiko for måloppnåelse.
Avvik	Enhver håndtering av data/informasjon som ikke utføres i henhold til gjeldende regelverk, retningslinjer og/eller prosedyrer, samt andre sikkerhetsbrudd.
Hendelse	Uønskede situasjoner som kan medføre eller kan ha medført et informasjonssikkerhetsbrudd.
Informasjonssikkerhet	Informasjonssikkerhet handler om å sikre informasjonens konfidensialitet, integritet og tilgjengelighet.
Informasjonssikkerhetsbrudd/ sikkerhetsbrudd	Brudd på konfidensialitet, integritet og/eller tilgjengelighet. Bruddet kan ha store, små eller ingen konsekvenser.
Informasjonsverdier	Et samlebegrep som inkluderer både informasjon og tilhørende støtteverdier som IKT-system, digitale tjenester, datautstyr av ulike varianter mv.
Integritet	Informasjon må være sikret mot utilsiktet eller uautorisert endring eller sletting.
Konfidensialitet	Uvedkommende skal ikke få kjennskap til informasjon/data.
Personvern	Personopplysninger skal beskyttes i henhold til relevant lovgivning.
Risiko	Uttrykk for forholdet mellom trusselen mot en gitt verdi og denne verdiens sårbarhet overfor den spesifiserte trusselen.
Risikostyring	Et sett av aktiviteter for å styre og kontrollere risiko.
Risikotoleranse	Ekstra risiko UiT er villig til å ta i enkelte saker fordi gevinsten veier tyngre enn risikoen.
Tilgjengelighet	Dataene er tilgjengelig ved behov.
Trussel	Begrepet benyttes om både aktører for villede handlinger og farekilder.
Uninett	Uninett-konsernet leverer nett og nettjenester til universiteter, høgskoler og forskningsinstitusjoner, samt håndterer andre nasjonale IKT-oppgaver. Uninett eies av Kunnskapsdepartementet
Unit	Unit – Direktoratet for IKT og fellestjenester i høyere utdanning og forskning. Direktoratet har ansvar for nasjonal samordning og forvaltning av IKT i universitets- og høyskolesektoren, og leverer allerede et bredt spekter av tjenester til forskning og høyere utdanning.