Ledelsessystem for informasjonssikkerhet og personvern

Kapittel 1: Innledning

1.1 Formål og hensikt

~~Universitetet i Tromsø~~UiT – 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.~~

Informasjonssikkerhet

Et systematisk og planmessig arbeid for å sikre våre 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 med forskrift (e-forvaltningsforskriften), personopplysningsloven (2018) med forskrift, personvernforordningen (GDPR) 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 og personvern ved* UiT skal ivareta~~r~~ de kravene som lovverket og Kunnskapsdepartementet (KD) stiller til arbeidet med informasjonssikkerhet i universitets- og høyskolesektoren.

Personvern

Ivaretagelse av informasjonssikkerheten ved behandling av personopplysninger er en sentral del av forpliktelsene etter personopplysningsloven, GDPR og øvrig, relevant lovverk. Imidlertid påhviler det en rekke øvrige forpliktelser utover informasjonssikkerhet for å sikre godt personvern og overholde de forpliktelsene UiT er underlagt etter regelverket, 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.

1.2 Ledelsessystemet for informasjonssikkerhet og personvern ved UiT

Ledelsessystemet for informasjonssikkerhet og personvern 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 og personvern, samt beskrivelse av roller og ansvar, oversikt over informasjonsverdier og retningslinjer.

Ledelsessystemet består av tre hovedelementer:

1. Styrende del – overordnet policy, herunder ~~sikkerhetsmål~~ målsetninger og ~~-~~strategi, akseptabel risiko roller og ansvar.
2. Gjennomførende del – ~~risikovurderinger samt konkrete rutiner og retningslinjer i vedleggene.~~konkrete retningslinjer og rutiner, herunder om klassifisering av informasjon, risikovurderinger, opplæring mv.
3. Kontrollerende del – internrevisjon, rapportering av avvik og ledelsens gjennomgang/årsrapport.

~~1.3 Avgrensning av ledelsessystemet~~

Informasjonssikkerhet og personvern er et topplederansvar. Det operative ansvaret og det praktiske arbeidet med å ivareta informasjonssikkerheten og personvernet kan delegeres til de enkelte enhetene ved UiT, jf. beskrivelsen av sikkerhetsorganisasjonen med roller og ansvar i ~~punkt 3~~kapittel 4.

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

~~Med informasjonsverdier~~*Informasjonsverdi* er et samlebegrep som inkluderer både selve informasjonen samt tilhørende støtteverdier som IKT-system, digitale tjenester, datautstyr av ulike varianter mv.~~ menes utstyr, prosesser eller data som er tilknyttet informasjon og som virksomheten anser som nødvendig å beskytte.~~ Hvordan man skal behandle og beskytte

[1] Studenter, ansatte, gjester, samarbeidspartnere etc.
[2] IT-systemer, datanettverk, databaser/-registre etc.

informasjonsverdiene avhenger av resultatene fra risikovurderinger. Informasjonssikkerhet ~~knyttet~~ skal ivaretas for alle informasjonsverdier, uavhengig av medietype, format, lagringsteknologi, om det er digitalt eller ikke-digitalt, behandles lokalt eller i skytjenester mv. ~~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. Videre er det ikke kun personopplysninger, men også øvrig informasjon som universitetet forvalter. Eksempelvis økonomisk informasjon om virksomheten, bygningsinformasjon, forskningsdata som ikke involverer mennesker mv.

~~*[Fotnoter]*~~

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

~~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]

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 og personvern ved UiT
- har det overordnede ansvaret for personvernet ved all behandling av personopplysninger ved UiT
- ~~kan~~ skal stille krav til det videre arbeidet med informasjonssikkerhet og personvern ved UiT

Universitetsdirektør

- utøver det overordnede ansvaret for ~~er behandlingsansvarlig for~~ all behandling av~~e~~ personopplysninger ved UiT~~, 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 og personvern blir implementert og vedlikeholdt, samt for organiseringen av sikkerhetsarbeidet
- ~~skal iverksette årlig internrevisjon, jf. punkt 6.1.~~
- skal påse at meldingspliktige brudd på personopplysningssikkerheten rettidig oversendes Datatilsynet
- skal årlig gjennomgå status for arbeidet med informasjonssikkerhet og personvern[3]~~8~~
- skal oppnevne medlemmer av informasjonssikkerhetsforumet
- skal oppnevne medlemmer av gruppe for overordnet vurdering av personvernkonsekvensvurderinger (DPIA)
- har myndighet til å avgjøre om behandlinger underlagt personvernkonsekvensvurdering (DPIA) skal anses for å ha redusert risikoen tilstrekkelig, eller om behandlingen må underlegges ytterligere tiltak alternativt avbrytes

IT-direktør

- ~~er informasjonssikkerhetsansvarlig og~~
- har forvaltningsansvaret for informasjonssikkerheten og personvern ved UiT
- har instruksjonsmyndighet overfor alle ~~andre~~ enheter ved UiT i saker som angår informasjonssikkerhet og personvern
- har det praktiske ansvaret for at det føres en protokoll over alle behandlingsaktiviteter som UiT har, både i rollen som behandlingsansvarlig og som databehandler.
- skal påse at holdningsskapende programmer gjennomføres

~~Informasjonssikkerhetsrådgiver(e)~~Faggruppe for informasjonssikkerhet og personvern

- v/faggruppeleder er sikkerhetssjef (CISO)
- skal utøve IT-direktørens myndighet i saker om informasjonssikkerhet og personvern
- ~~~~
- skal være rådgiver for linjeorganisasjonen i spørsmål relatert til informasjonssikkerhet og personvern
- skal lede CSIRT[4]~~-~~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 gis innsyn i alle opplysninger som er nødvendig for å følge opp hendelser og avvik innenfor informasjonssikkerhet og personvern

[3] Jf. Kapittel 9 "ledelsens gjennomgang"
[4] CSIRT står for Computer Security Incident Response Team

- skal drive opplysningsvirksomhet, rådgivning og opplæring innen informasjonssikkerhet og personvern
- skal vedlikeholde overordnet ~~policy~~ regelverk og rutiner for informasjonssikkerhet og personvern
- ~~skal iverksette og delta i revisjoner og risikovurderinger ved behov~~
- har myndighet til å igangsette internrevisjoner innenfor informasjonssikkerhet og/eller personvern, på alle enheter og innenfor alle virksomhetsområder
- skal utarbeide og vedlikeholde verktøy og veiledningsmateriell for gjennomføring av risikovurderinger
- skal utarbeide årlig rapport til ledelsens gjennomgang («årsrapport for informasjonssikkerhet og personvern»)
- skal holde oversikt over databehandleravtaler som inngås på UiT

Personvernombudet

- rapporterer direkte til Universitetsdirektør
- skal informere og gi råd til UiTs ansatte og studenter om gjeldende forpliktelser etter personvernlovgivningen
- skal kontrollere UiTs overholdelse av personvernlovgivningen
- skal involveres på rett tidspunkt og nivå i spørsmål som omhandler personvern
- skal gi råd i vurderingen av personvernkonsekvenser (DPIA) og kontrollere gjennomføringen av disse vurderingene
- skal involveres på passende nivå i håndteringen av avvik etter personvernlovgivningen, og som minimum orienteres om innhold og omfang av avvik
- skal utarbeide årlig rapport som kan tas inn som vedlegg til *årsrapport for informasjonssikkerhet og personvern*
- har observatørstatus i *Informasjonssikkerhetsforum*
- kan kontaktes direkte av de registrerte med spørsmål om UiTs behandling av deres personopplysninger, og om utøvelsen av sine rettigheter etter personvernforordningen (GDPR)
- kan ikke instrueres om utførelsen av de oppgavene som ligger til personvernombudet etter personvernforordningen (GDPR) artikkel 39

Avdeling for IT

- skal bistå systemeier ved utforming av krav til informasjonssikkerhet ved anskaffelse av nye system
- har ansvar for drift av sentrale IT-systeme~~rne~~, 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
-

Avdeling for forskning, utdanning og formidling

- skal ha kontaktpersonen for Norsk senter for forskningsdata (NSD)
- skal motta og ha internt ansvar for oppfølging av personvernkonsekvensvurderinger (DPIA) som NSD utarbeider på vegne av UiT

Enhetsledere

- er ansvarlige for å tilfredsstille krav til informasjonssikkerhet og personvern i egen enhet
- skal sørge for at ~~gjennomføre~~ risikovurderinger gjennomføres
- skal iverksette tiltak dersom det er nødvendig for å ivareta informasjonssikkerheten og personvernet i egen enhet
- har det overordnede ansvaret for at personvernkonsekvensvurderinger (DPIA) iverksettes der det er påkrevd etter personvernforordningen (GDPR) art. 35
- skal rapportere resultat fra risikovurderinger med handlingsplan og avvik til *Faggruppe for informasjonssikkerhet og personvern* ~~informasjonssikkerhetsrådgiver~~
- skal følge opp avviksmeldinger i egen enhet og sørge for at disse blir lukket, i samarbeid med *Faggruppe for informasjonssikkerhet og personvern*
- skal informere ansatte i egen enhet om de rutiner og retningslinjer som gjelder til enhver tid og sørge for at kravene i ledelses~~styrings~~systemet 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 ha fokus på ivaretagelse av innebygd personvern og personvern som standardinnstilling
- 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~~kapittel 5, og dokumentere at risikovurderinger er utført
- skal iverksette eventuelle tiltak på bakgrunn av risikovurderinger

Leder av forskningsprosjekt

- opptrer på vegne av UiT som behandlingsansvarlig for hva gjelder det konkrete forskningsprosjektet
- har det daglige ansvaret for at informasjonssikkerheten ivaretas i forskningsprosjektet
- har ansvaret for at det gjennomføres personvernkonsekvensvurderinger (DPIA) dersom det er påkrevd etter personvernforordningen (GDPR) art. 35.
- nærmere ansvar og forpliktelser følger av *retningslinjer for personvern i forskings- og studentprosjekt*

Studentveiledere

- opptrer på vegne av UiT som behandlingsansvarlig for hva gjelder det konkrete studentprosjektet (eksempelvis masteroppgave)
- har ansvaret for at det gjennomføres personvernkonsekvensvurderinger (DPIA) dersom det er påkrevd etter personvernforordningen (GDPR) art. 35.
- nærmere ansvar og forpliktelse følger av *retningslinjer for personvern i forskings- og studentprosjekt*

DPIA-gruppe

- skal ledes av Avdeling for forskning, utdanning og formidling
- vurderer utarbeidede personvernkonsekvensvurderinger (DPIA) på vegne av UiT
- leverer en innstilling til Universitetsdirektøren med anbefaling om en behandling bør igangsettes eller ikke
- medlemmer skal minst inkludere personvernombudet, én representant fra *Faggruppe for informasjonssikkerhet og personvern* og én representant fra ett fakultet.

~~Brukere av IT-tjenester (ansatte/studenter)~~Ansatte og 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