UiT Norges arktiske universitet

Dato:

Møteinnkalling

Utvalg:	**Universitetsstyret**
Møtested:	Microsoft Teams
Møtedato:	16.12.2020
Tidspunkt:	12:00 – 15:00

Eventuelt forfall må meldes snarest til britt.a.mikkelsen@uit.no. Vararepresentanter møter etter nærmere beskjed.

Saksliste

Saksnr	*Tittel/beskrivelse*	*U.off.*	*Arkivref.*
S 52/20	Styrende del av ledelsessystem for informasjonssikkerhet – revidering og utvidelse til å omfatte personvern		2017/5560
S 53/20	Ansettelse av rektor ved UiT Norges arktiske universitet	X	2020/6291

SAKSFRAMLEGG

Til:	Møtedato:	Sak:
Universitetsstyret	16.12.2020	52/20

Styrende del av ledelsessystem for informasjonssikkerhet – revidering og utvidelse til å omfatte personvern

Innstilling til vedtak:
Universitetsstyret vedtar de foreslåtte endringene til styrende del av ledelsessystemet for informasjonssikkerhet.

Ledelsessystemet endrer navn til «ledelsessystem for informasjonssikkerhet og personvern ved UiT Norges arktiske universitet»

Bakgrunn:

I 2015 godkjente Universitetsstyret «styringssystem for informasjonssikkerhet» i sak S 07/15.

Styringssystemet har senere blitt omdøpt til ledelsessystem for informasjonssikkerhet, samt undergått visse mindre strukturendringer. Deler av ledelsessystemet har også blitt revidert, eksempelvis gjennom vedtakelsen av ny strategi for informasjonssikkerhet (sak S 9/19) og ny retningslinje for klassifisering av informasjon (sak F 13/19).

Ledelsessystemet består av tre deler:

1. **Styrende del** (overordnet policy, herunder sikkerhetsstrategi og -mål, akseptabel risiko, klassifisering, roller og ansvar)
2. **Gjennomførende del** (konkrete retningslinjer og rutiner, risikovurderinger, opplæring mv.)
3. **Kontrollerende del** (internrevisjon, rapportering og håndtering av avvik, ledelsens gjennomgang/årsrapport).

Som hovedregel er det Universitetsstyret som vedtar endringer i den *styrende* del, mens Universitetsdirektøren vedtar endringer tilhørende *gjennomførende* og *kontrollerende* del.

Som nevnt omfatter ledelsessystemet i dag kun informasjonssikkerhet. Som forespeilet i årsrapport 2019 (sak S 10/20) er det ønskelig å utvide ledelsessystemet til å omfatte både informasjonssikkerhet og personvern. Dette fordi disse temaene henger nært sammen, selv om sentrale deler av personvern ikke omhandler informasjonssikkerhet (f.eks ivaretagelse av registrertes rettigheter, lovlig behandlingsgrunnlag mv) og vice versa (sikring av informasjonsverdier som ikke inneholder personopplysninger, eksempelvis byggdata, økonomiske

data, forskningsdata som ikke omhandler personer mv). Erfaring har vist at det ikke er hensiktsmessig å forsøke å skille feltene, og en mer enhetlig tilnærming er derfor ønsket.

Denne saken fremmes derfor Universitetsstyret for å få en beslutning på at ledelsessystemet skal bygges ut, samt foreta de nødvendige endringer i ledelsessystemets *styrende del.* De nødvendige endringer i *gjennomførende* og *kontrollerende del* vil deretter bli utarbeidet og fremmet Universitetsdirektøren for behandling.

I dag består *styrende del* av fire kapittel:

1. Innledning
2. Sikkerhetsstrategi (inkludert sikkerhetsmål) og akseptabel risiko
3. Klassifisering av informasjon
4. Roller, ansvar og oppgaver

I denne saken fremmer Universitetsdirektøren forslag til materielle endringer i kapittel 1 og 4. Kapittel 3 ønskes flyttet til *gjennomførende del* da tematikken som reguleres er mer passende der, fremfor i den overordnede, styrende delen av ledelsessystemet[1].

Det vil være viktig å revidere og utvide informasjonssikkerhetsstrategien (kapittel 2) til å også omfatte en strategi for UiTs arbeid med, og ivaretagelse av, personvern. Dette er imidlertid er omfattende arbeid som ikke vil bli klart før tidligst våren 2021. Universitetsdirektøren anser det derfor som hensiktsmessig å fremme de øvrige forslagene til endringer nå, slik at arbeidet med nødvendig revidering av resten av ledelsessystemet kan ta til. Inntil videre vil derfor kapittel 2 forbli uendret selv om ledelsessystemet skal omfatte både informasjonssikkerhet og personvern.

Kapittel 1 - innledning

I kapittel 1 er det foretatt en viss omstrukturering for å ta inn personvern, og det er lagt til tekst som beskriver UiTs ansvar for ivaretagelse av personvern.

Videre foreslår Universitetsdirektøren at kapittel 1.4 *«Behandlingsansvarlig og databehandlere»* tas ut. Dette underkapittelet forklarer primært hva som ligger i begrepene samt understreker at databehandleravtale alltid skal inngås før eksterne aktører behandler personopplysninger på vegne av UiT. Slik ledelsessystemet og øvrig regelverk ved UiT har utviklet seg etter hvert som det har blitt større modenhet på feltet fremstår det som unødvendig å ha dette med i *styrende del,* og innholdet kan bedre ivaretas direkte i egne retningslinjer.

Den siste foreslåtte endringen i kapittel 1 er at oppdelingen mellom kapittel 1.2 og 1.3 fjernes slik at disse slås sammen til ett underkapittel (1.2).

Kapittel 4 – roller, ansvar og oppgaver

De største endringene kommer i kapittel 4 *roller, ansvar og oppgaver.* Primært går dette på å ta inn eksisterende roller og strukturer på UiT innenfor personvern, slik at disse fremkommer på et overordnet nivå. Eksempelvis gjelder dette personvernombudet samt gruppen som gjennomgår utførte personvernkonsekvensvurderinger («DPIA-gruppen»).

[1] Kapittel tre (klassifisering av informasjon) blir da nytt kapittel fire, mens dagens kapittel fire (roller, ansvar og oppgaver) blir nytt kapittel tre. Kapittelnummer og henvisninger ajourføres dersom vedtatt som foreslått.

Ellers er det ønskelig at arbeidet med personvern legges opp slik at det følger den samme organiseringen og ansvarsfordeling som for informasjonssikkerhet, og de eksisterende rollene i dagens ledelsessystem er revidert slik at dette gjenspeiles.

Av andre endringer som kan trekkes frem her er at i nåværende utgave står det at *«Universitetsdirektøren er behandlingsansvarlig for alle personopplysninger, dette omfatter også å bestemme formålet med behandling av personopplysninger, samt å ha dokumentert oversikt over disse».*

Den *behandlingsansvarlige* er den som bestemmer formålet med behandling av personopplysninger og hvilke midler som skal benyttes, og er en svært sentral og viktig rolle i personvernforordningen (GDPR). Når det er tale om en organisasjon eller virksomhet som behandler personopplysninger vil den behandlingsansvarlige etter personvernforordningen typisk være virksomheten som sådan, og ikke en konkret rolle i virksomheten, selv om avgjørelser i det daglige naturligvis ofte vil være delegert til ulike posisjoner og roller.

Spørsmålet om hvem som formelt regnes som behandlingsansvarlig ("controller"), og hvorfor dette legges på organisasjonsnivå fremfor til konkrete roller eller posisjoner, omtales bl.a i boken *The EU General Data Protection Regulation (GDPR) A Commentary*[2]: "However, where an organised collective entity determines the purposes and means of processing, the point of departure is that the entity as such is the controller, rather than any particular individual natural/physical person who is part of that entity. In the words of WP29, this is due not just to 'the strategic perspective of allocating responsibilities', but also 'in order to provide data subjects with a more stable and reliable reference entity for the exercise of their rights'. Thus, for instance, in the case of a corporation, the controller will usually not be any of the members/employees of the corporation (e.g. Chief Executive Officer, Board Chairperson, Chief Financial Officer, Chief Privacy Officer etc.) who actually decide on the purposes and means of the processing, but the corporation as such.".

Det er slikt sett ikke helt treffende med den nåværende formuleringen. Universitetsdirektøren foreslår derfor at dette synliggjøres ved at det tas inn et nytt punkt under Universitetsstyrets ansvar, og nåværende punkt under Universitetsdirektørens ansvar omformuleres. Beskrivelsen av ansvaret vil da bli mer presist, og i tråd med de premisser som personvernforordningen setter.

I vedlegg én følger revidert forslag til *styrende del*. I vedlegg to følger samme forslag, men med «spor endringer» markert slik at de konkrete endringene lettere vises, mens i vedlegg tre er någjeldende utgave.

Jørgen Fossland
universitetsdirektør

Stig Ørsje
IT-direktør

Dokumentet er elektronisk godkjent og krever ikke signatur

Saksbehandler: Ingvild Stock-Jørgensen

Vedlegg
1 Revidert styrende del av ledelsessystemet (forslag)
2 Revidert styrende del av ledelsessystemet (forslag - med spor endring)
3 Gjeldende versjon av styrende del av ledelsessystemet
4 Grovskisse org.kart DPIA-gruppe og faggruppe for informasjonssikkerhet og personvern

[2] Lee A. Bygrave og Luca Tosoni, "Article 4(7), Controller" i The EU General Data Protection Regulation (GDPR) A Commentary, edited by Kuner, Bygrave, Docksey, 1st ed., 2020, Oxford University Press, s 149

Ledelsessystem for informasjonssikkerhet og personvern

Kapittel 1: Innledning

1.1 Formål og hensikt

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.

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 forøvrig – 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. *Ledelsessystemet for informasjonssikkerhet og personvern ved* UiT skal ivareta 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 målsetninger og strategi, akseptabel risiko roller og ansvar.
2. **Gjennomførende del** – konkrete retningslinjer og rutiner, herunder om klassifisering av informasjon, risikovurderinger, opplæring mv.
3. **Kontrollerende del** – internrevisjon, rapportering av avvik og ledelsens gjennomgang/årsrapport.

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 kapittel 4.

Ledelsessystemet for informasjonssikkerhet og personvern ved UiT omfatter
• alle som får tilgang UiTs informasjonsverdier[1]
• alle UiTs studiesteder/campuser
• alle organisatoriske enheter
• all teknologi[2]
• alle informasjonsverdier

Informasjonsverdi er et samlebegrep som inkluderer både selve informasjonen samt tilhørende støtteverdier som IKT-system, digitale tjenester, datautstyr av ulike varianter mv. Hvordan man skal behandle og beskytte informasjonsverdiene avhenger av resultatene fra risikovurderinger. Informasjonssikkerhet skal ivaretas for alle informasjonsverdier, uavhengig av medietype, format, lagringsteknologi, om det er digitalt eller ikke-digitalt, behandles lokalt eller i skytjenester mv. 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.

Kapittel 2: Sikkerhetsstrategi og akseptabel risiko

[innholdet i dette kapittelet berøres ikke i denne saken]

Kapittel 3: Klassifisering av informasjon

[1] Studenter, ansatte, gjester, samarbeidspartnere etc.

[2] IT-systemer, datanettverk, databaser/-registre etc.

[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
- skal stille krav til det videre arbeidet med informasjonssikkerhet og personvern ved UiT

Universitetsdirektør

- utøver det overordnede ansvaret for all behandling av personopplysninger ved UiT
- 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 påse at meldingspliktige brudd på personopplysningssikkerheten rettidig oversendes Datatilsynet
- skal årlig gjennomgå status for arbeidet med informasjonssikkerhet og personvern[3]
- 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

- har forvaltningsansvaret for informasjonssikkerheten og personvern ved UiT
- har instruksjonsmyndighet overfor alle 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

[3] Jf. Kapittel 9 "ledelsens gjennomgang"

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
- skal drive opplysningsvirksomhet, rådgivning og opplæring innen informasjonssikkerhet og personvern
- skal vedlikeholde overordnet regelverk og rutiner for informasjonssikkerhet og personvern
- 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

[4] CSIRT står for Computer Security Incident Response Team

Avdeling for IT

- skal bistå systemeier ved utforming av krav til informasjonssikkerhet ved anskaffelse av nye system
- har ansvar for drift av sentrale IT-systemer, 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 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*
- 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 ledelsessystemet 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 sørge for at databehandleravtaler inngås
- skal utføre risikovurdering av systemet i henhold til 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.

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 bidra til implementering av ledelsessystemet i organisasjonen
- skal jevnlig gjennomgå ledelsessystemet for informasjonssikkerhet med tilhørende dokumenter og generelle ansvarsforhold, samt vurdere behov for endringer

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]~~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

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

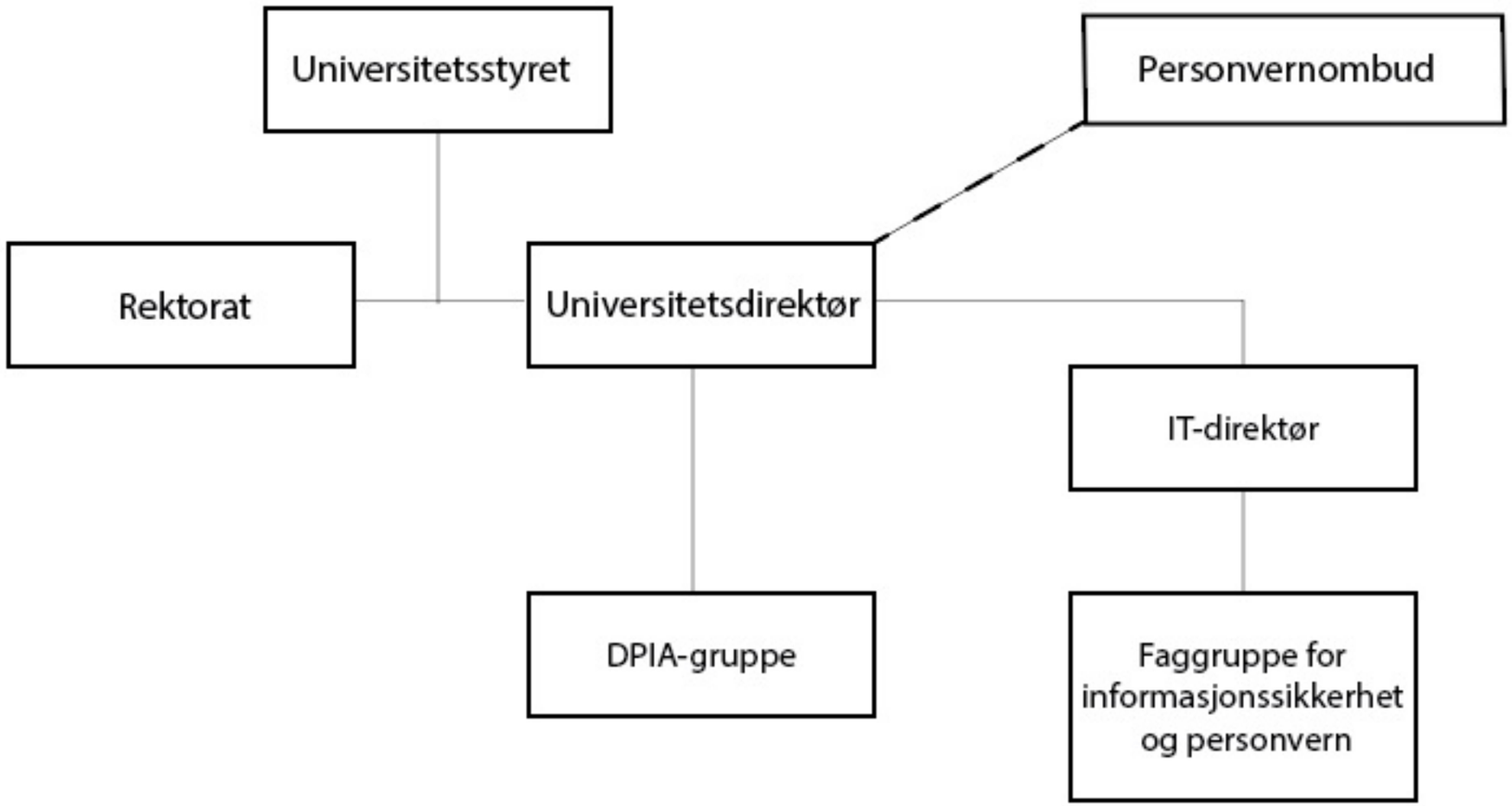
Computer Security Incident Response Team (CSIRT)

- 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

Grovskisse org.kart som viser plassering av DPIA-gruppe og Faggruppe for informasjonssikkerhet og personvern



UiT Norges arktiske universitet
Universitetsdirektøren - Rektor og universitetsdirektør

Ingress

UiT Norges arktiske universitet (UiT) er et breddeuniversitet som bidrar til en kunnskapsbasert utvikling, regionalt, nasjonalt og internasjonalt. Vi utnytter vår sentrale beliggenhet i nordområdene, vår faglige bredde og kvalitet og våre tverrfaglige fortrinn til å møte fremtidens utfordringer. Troverdighet, akademisk frihet, nærhet, kreativitet og engasjement skal prege forholdet mellom ansatte, mellom ansatte og studenter og mellom UiT og våre samarbeidspartnere.

Les mer om UiT og vår strategi Drivkraft i nord på uit.no. UiT har 16 600 studenter, mer enn 4 000 ansatte, og er etablert på 10 studiesteder i Nord-Norge. Våre største campuser er Tromsø, Alta, Narvik og Harstad. Rektor har sitt hovedarbeidssted i Tromsø.

Universitetet i Tromsø - Norges arktiske universitet

Rektor ved Universitetet i Tromsø - Norges arktiske universitet

Om stillingen
UiT Norges arktiske universitet (UiT) søker en utviklingsorientert og engasjert rektor som skal

- lede universitetets samlede virksomhet
- stimulere til fremragende faglige resultater
- lede universitetets samarbeid med myndigheter og samfunns- og næringsliv
- lede arbeidet med å utvikle universitetets organisasjon, universitetsdemokrati og medbestemmelse

Ansvar og oppgaver for rektor er beskrevet i universitets- og høyskoleloven.

UiT er skapt av fremsynte folkevalgte, dedikerte ansatte og kunnskapstørste studenter. Vi bidrar med kunnskap om helse, urfolk, hav, teknologi, klima og miljø, ressurser, geopolitikk og samfunns- og næringsutvikling som verden trenger. Gjennom 50 år har vi utdannet mer enn 65 000 fagfolk til samfunns- og næringsliv. UiT har et særlig mandat til å frembringe og formidle kunnskap om arktiske forhold på vegne av nasjonen Norge og for en verden som ser mot nord.

Kontakt
Flere opplysninger om stillingen kan du få av **rektor Anne Husebekk**

- telefon: +47 481 41 286
- e-post: anne.husebekk@uit.no

eller **universitetsdirektør Jørgen Fossland**

- telefon: +47 951 50 414
- e-post: jorgen.fossland@uit.no

eller **leder av innstillingsutvalget Stig Slørdahl**

- telefon: +47 918 97 510
- e-post: stig.slordahl@helse-midt.no

Kvalifikasjoner
Vi søker en rektor med kunnskap, vilje og kraft til å videreutvikle og forsterke universitetets posisjon og betydning regionalt, nasjonalt og internasjonalt.

Den som ansettes må

- være bedømt som professor- eller dosentkompetent
- ha bred erfaring fra ledelse innenfor større kunnskapsorganisasjoner
- ha gode strategiske evner og god forståelse av universiteters virksomhet
- ha kjennskap til offentlig forvaltning og politiske beslutningsprosesser
- ha gode evner til å representere universitetet utad og delta i den offentlige debatten
- ha god organisasjonsforståelse og erfaring fra organisasjonsutvikling
- ha gode evner til muntlig og skriftlig fremstilling på norsk og engelsk

Ønskede personlige egenskaper:

- Være nytenkende og nyskapende.
- Være resultatorientert, tydelig og beslutningsdyktig.
- Ha gode evner til kommunikasjon.
- Ha gode evner til å skape tillit og nettverk internt, nasjonalt og internasjonalt.
- Ha gode evner til samarbeid og å skape resultater sammen med andre.

Vi tilbyr

- en sentral lederposisjon ved et av Norges største og viktigste universiteter
- dyktige og engasjerte medarbeidere i aktive fagmiljøer
- interessante og utviklende lederoppgaver
- lønn og vilkår etter nærmere avtale

Rektor ansettes for en periode på fire år fra 1.8.2021, og med mulighet for ansettelse i ytterligere en fireårsperiode. Hovedarbeidssted for stillingen vil være Tromsø. Reisevirksomhet innen- og utenlands må påregnes.

Søknaden

Søknaden sendes elektronisk via www.jobbnorge.no, og skal inneholde

- søknadsbrev, CV og referanser
- vitnemål og karakterutskrifter
- dokumentasjon på språkferdigheter

All dokumentasjon som skal vurderes må være på et skandinavisk språk eller engelsk.

Generelt

Ansettelsen skjer i henhold til regler og vilkår som til enhver tid gjelder for statsansatte, og til retningslinjer ved UiT. På våre nettsider finner du mer informasjon til søkere på stillinger ved UiT. Ved UiT legger vi vekt på mangfold, og oppfordrer særlig kvinner og personer med minoritetsbakgrunn til å søke stillingen.

Personopplysninger som oppgis behandles i henhold til lov om behandling av personopplysninger. Søkere kan be om ikke å bli oppført på den offentlige søkerlisten, men universitetet kan likevel beslutte at navnet på søkeren skal offentliggjøres. Søkeren vil da bli varslet i forkant av offentliggjøring.

Jobbnorge-ID: 192339, Søknadsfrist: 02.11.2020, Kundens referanse: 2020/6291