UiT
NORGES
ARKTISKE
UNIVERSITET

Universitetsledelsen
Arkivref: 2019/1102/INJ024
Dato: 21.02.2019

SAKSFRAMLEGG

Til:	Møtedato:	Sak:
Universitetsstyret		

Ny informasjonssikkerhetsstrategi for UiT - 2019-2021

Innstilling til vedtak:

1. Universitetsstyret godkjenner det vedlagte forslaget til ny informasjonssikkerhetsstrategi

2. Strategien tas inn i kapittel 2 i styringssystemet for informasjonssikkerhet og erstatter dagens kap. 2.1, 2.2 og 2.4, som oppheves.

3. Dagens kap. «2.3 Klassifisering av informasjon» endres til «2.2 Klassifisering av informasjon».

Begrunnelse:

Styringssystemet for informasjonssikkerhet
I 2015 vedtok Universitetsstyret *Styringssystem for informasjonssikkerhet* (sak S 7/15); et internt rammeverk ved UiT Norges arktiske universitet (UiT) som skal sikre at informasjonssikkerheten ivaretas på en systematisk, planmessig og tilfredsstillende måte. UiT er pålagt å ha et slik styringssystem, både gjennom krav i lovverk og fra Kunnskapsdepartementet.

Styringssystemet er tredelt og består av styrende, gjennomførende og kontrollerende del, se vedlegg fire.

I sak F 99/18 ble Universitetsdirektøren gitt fullmakt til å foreta endringer i den *gjennomførende* og *kontrollerende* del. Dette omfatter blant annet regulering av avvikshåndtering, rapportering, risikovurderinger mv.

Strategi for informasjonssikkerhet er del av *styrende del*, og endringer i denne delen ligger til Universitetsstyret.

Prosessen
Gjennom styringssystemet er IT-direktør gitt forvaltningsansvaret for informasjonssikkerhet, jf kapittel 3. Våren 2018 engasjerte IT-avdelingen konsulentselskapet Gartner til å gjennomføre en modenhetskartlegging av UiTs håndtering av informasjonssikkerheten.

Denne kartleggingen klargjorde at selv om det foregår endel godt arbeid med informasjonssikkerhet på UiT er det fortsatt betydelige mangler, blant annet knyttet til systematikk, dokumentasjon og kompetanse. Det ble også raskt klart at UiT manglet en god strategi for arbeidet med informasjonssikkerhet. Det er fastsatt en sikkerhetsstrategi i kapittel 2 i styringssystemet, men denne er altfor overordnet og bl.a vanskelig å måle oppnåelsen av.

Høsten 2018 startet arbeidet med utarbeidelse av ny strategi, og dette arbeidet er del av et større utviklingsprogram som skal sørge for at UiT fortsetter å ha en sikker, relevant og ressurseffektiv plattform for digitalisering (DigU-programmet). Gartner fikk oppdraget med å legge til rette for denne prosessen, og de har vært tungt inne i gjennomføring av intervjuer, workshop, utarbeidelse av dokumenter m.m.

Universitetsstyrets rolle og ansvar
Som øverste organ ved UiT er det Universitetsstyrets ansvar at UiT ivaretar informasjonssikkerheten på en tilfredsstillende måte.

Forsknings- og høyere utdanningsminister Iselin Nybø sendte i januar 2019 ut brev til UH-sektoren hvor det ble orientert om «Kunnskapsdepartementets styringsmodell for informasjonssikkerhet i høyere utdanning og forskning», og hvilke forventninger og krav Kunnskapsdepartementet stiller til virksomhetene, se vedlegg fem.

Gjennom dette brevet understreker ministeren betydningen av ivaretagelse av informasjonssikkerheten, samt styrets ansvar i dette arbeidet:
«Styret har det øverste ansvaret for risikoen som knytter seg til virksomhetens informasjonsverdier, og er ansvarlig for at sikkerheten er tilpasset denne risikoen. Det er styrets ansvar å sette virksomheten i stand til å håndtere risikoen slik at denne er på et nivå som styret aksepterer. Jeg forventer også at håndteringen av dette viktige området integreres i den generelle virksomhetsstyringen og er tydelig forankret i styret og toppledelsen.»

Gjennom styringssystemet setter Universitetsstyret rammene for hvordan informasjonssikkerheten skal ivaretas, herunder mekanismer for å sikre at styret har mulighet for å følge opp sitt ansvar. Dette inkluderer den årlige rapporteringen om informasjonssikkerhet (ledelsens gjennomgang) hvor styret vil bli orientert om siste års arbeid med informasjonssikkerhet, herunder avvik, oppfølging av vedtatte tiltak og særlige utfordringer UiT står ovenfor på dette feltet. For 2018 fremmes denne årsrapporten Universitetsstyret i mars 2019. Strategien oppstiller en rekke tiltak, og gjennom de neste årsrapportene vil status på arbeidet med disse tiltakene rapporteres til styret.

Betydningen av god informasjonssikkerhet
Det er svært ofte fokus på ivaretagelse av informasjonssikkerhet for personopplysninger (personvern) da dette feltet har sterk lovregulering av informasjonssikkerheten. Imidlertid skal informasjonssikkerhet ivaretas for all informasjon; uavhengig av medium (digitalt eller fysisk/manuelt) og type.

Ved UiT er det også en utfordring at store deler av virksomheten gir uttrykk for at informasjonssikkerhet er en IT-sak, som fullt og helt håndteres av Avdeling for IT. Det er nødvendig å arbeide for å endre denne oppfatningen. Hvis ikke vil det bli svært vanskelig å få den nødvendige forankringen av arbeidet i hele organisasjonen, slik at det skapes forståelse og kunnskap om hvorfor og hvordan informasjonssikkerheten ivaretas i det daglige arbeidet.

Videre er det viktig å understreke at informasjonssikkerhet ikke bare omhandler å sikre at uvedkommende ikke får innsyn i fortrolig informasjon (ivaretagelse av konfidensialitet). Det er like sentralt å sikre informasjonen mot uautoriserte endringer («integritet») samt at den ikke blir utilgjengelig eller går tapt («tilgjengelighet»).

Hvis ivaretagelsen av disse kravene og hensynene ikke får tilstrekkelig fokus og ressurser må prosesser og prosjekter i ytterste konsekvens stoppes. Dette fordi sikkerheten ikke har blitt ivaretatt og hensyntatt til rett tid. Det vil heller ikke alltid være mulig å rette opp manglene. Prosessene kan ha kommet alt for langt før det ble fokusert på ivaretagelsen av sikkerheten, og nødvendige tiltak kan da bli uforholdsmessig ressurskrevende eller rett og slett ugjennomførbare.

Styringssystemet skal fungere som et godt internkontrollsystem slik at UiT som organisasjon klarer å ivareta informasjonssikkerheten i alle ledd av virksomheten. Den nye strategien vil være et sentralt steg for å lykkes med dette. Strategien er ambisiøs, og det vil være krevende å nå de mål som er foreslått. Dette arbeidet vil involvere samtlige enheter ved UiT, og vil kreve fokus og ressurser. Universitetsstyret har derfor en sentral rolle i å gi arbeidet den nødvendige forankring.

Hvis UiT ikke lykkes med å styrke og systematisere arbeidet med informasjonssikkerhet vil dette medføre stor risiko for lovbrudd, økonomisk tap samt tap av legitimitet og omdømme. Videre har UiT en ambisiøs digitaliseringsstrategi, og det er nødvendig å ha en god tilnærming til informasjonssikkerhet for å lykkes med digitaliseringsprosessene. Forsknings- og høyere utdanningsministeren uttaler i ovennevnte brev at «informasjonssikkerhet er en grunnleggende forutsetning for å kunne lykkes med digitalisering».

Enhver digitaliseringsprosess som ikke hensyntar informasjonssikkerhet medfører en risiko for UiT; både for at digitaliseringen ikke lykkes, samt for andre konsekvenser slik som tap eller uønsket eksponering av informasjon, mv.

Ny informasjonssikkerhetsstrategi
Strategien gjelder for perioden 2019 t.o.m 2021, og består av et overordnet hoveddokument samt et grunnlags-/underlagsdokument med langt høyere detaljeringsgrad rundt beskrivelsen av målene, tiltakene, utfordringene og ressursbehovet.

I vedlegg én er hoveddokumentet i strategien, og i vedlegg to er grunnlagsdokumentet. Hoveddokumentet vil legges offentlig tilgjengelig, mens grunnlagsdokumentet vil være mer skjermet[1].

Strategien fastsetter UiTs visjon for informasjonssikkerhet:

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

Administrasjonen er ikke eksplisitt nevnt i visjonen. Universitetsdirektøren ønsker derfor å understreke at håndtering av informasjonssikkerhet i administrative prosesser er viktig, og en del av strategien forøvrig. Fokuset for visjonen er rettet mot kjernevirksomheten da det største

[1] Dette grunnet detaljgraden for hvor UiT har utfordringer med tanke på informasjonssikkerhet. Denne informasjonen kan i verste fall misbrukes og lette angrep av sikkerhetsmessig betydning mot UiT.

behovet for styrking av informasjonssikkerheten ligger her, og i de rent administrative prosesser og systemer har det vært et visst fokus på dette allerede.

Det overordnede målet med strategien er at UiT skal bevege seg fra en *tilfeldig* tilnærming til informasjonssikkerhet til en *formalisert* sikkerhetspraksis.

Strategien fastsetter at 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

Målbildet for informasjonssikkerhet er å få på plass en effektiv sikkerhetsstyring, helhetlig oversikt og kontroll, overvåkning og hendelsesstyring samt en ansvarsbevisst sikkerhetskultur i hele organisasjonen. Videre vil et godt sektorsamarbeid være en nøkkel for å lykkes, og bl.a vil Unit[2] og UNINETT[3] ha en viktig rolle i arbeidet med informasjonssikkerhet i UH-sektoren.

Ved å nå målbildet for strategiperioden vil arbeidet med informasjonssikkerhet ved UiT bli betydelig styrket, og hovedendringene vil blant annet inkludere følgende:

- Informasjonssikkerhet forankres bedre utover i virksomheten
- En ansvarsbevisst kultur og kompetanse, som er nødvendig for at UiT skal kunne oppdage avvik mer systematisk
- Sikkerhetsarkitekturen moderniseres i forhold til de kravene som blir stilt i IT-strategien og Digitaliseringsstrategien
- Dokumentstyring og -revisjon skjer mer systematisk
- En kontinuerlig prosess for oppfølging av tiltak etableres
- Risikovurderinger gjennomføres på virksomhetsnivå
- Godt definerte sikkerhetstjenester som bistår og rådfører virksomheten på sikker håndtering av data, risikovurderinger osv.
- Større bredde i sikkerhetsorganisasjonen med hensyn til både roller og kompetanser
- Synligheten og prioritering av informasjonssikkerhet heves både internt i Avdeling for IT og i virksomheten
- Investering i bruk av sikkerhetsverktøy med fokus på automatisering i noen arbeidsprosesser
- Økt fokus på standardisering og samhandling i sektor, og tilstrekkelig utnyttelse av sektortjenestene

[2] Unit – Direktoratet for IKT og fellestjenester i høyere utdanning og forskning. Direktoratet har ansvar for nasjonal samordning og forvaltning av IKT i UH-sektoren, og leverer en rekke tjenester til forskning og høyere utdanning. Https://www.unit.no.

[3] UNINETT er et statlig eid infrastrukturselskap, og leverer nett og nettjenester til UH-sektoren samt at de er leverandør av en rekke fellesløsninger innenfor IKT til sektoren (bl.a. innloggingsløsningen FEIDE, trådløstilgang via Eduroam mv). Https://www.uninett.no.

Rammer for informasjonssikkerhetsarbeidet
Gjennom styringssystemet er enhetslederne tillagt ansvaret for å sikre at kravene til informasjonssikkerheten er oppfylt i egen enhet, herunder gjennomføring av risikovurdering. Tilsvarende gjelder for systemeiere for sine respektive systemer.

All informasjonsbehandling medfører en risiko. Det er sentralt å foreta gode vurderinger av hvilken risiko behandlingen innebærer samt hvilken risiko UiT er villig til, og har mulighet for, å løpe for å oppnå de mål og resultater som er satt. Da er det mulig å vurdere hvilke tiltak som kan iverksettes for å redusere risikoen, samt om behandlingen i det hele tatt er gjennomførbar eller om risikoen blir for høy.

Gjennom informasjonssikkerhetsstrategien fastsetter Universitetsstyret flere styrende prinsipper, samt at det angis noen ytre grenser for hvilken risiko universitetet er villig til å løpe innenfor hhv. utdanning, FoU, formidling og administrasjon. De avveiingene som fremkommer her er et resultat av de observasjoner og den informasjon som er innhentet i prosessen med utarbeidelse av strategien; herunder intervjuer med en rekke personer ved UiT (inkl toppledelsen) og workshop med representanter fra flere av enhetene[4].

Dette danner rammene og grunnlaget for de vurderinger enhetslederne og systemeierne tar når risikoen i prosjekter, prosesser, systemanskaffelser mv vurderes, og det besluttes hvilke tiltak som må gjennomføres og prioriteres - eller om man rett og slett må avbryte det planlagte arbeidet fordi risikoen blir for høy. Totalt sett bidrar dette til å sørge for at UiT får en mer helhetlig og likeartet tilnærming til hvordan risikoer vurderes og informasjonssikkerheten ivaretas.

Høringsrunde
Strategien ble sendt på høring til alle enhetene ved UiT samt Studentparlamentet, og svarfrist var 18.2.19. Noen enheter ba om utsettelse til 20.2.19 og fikk det.

Følgende enheter har sendt inn høringssvar:
- Det juridiske fakultet
- Fakultet for biovitenskap, fiskeri og økonomi
- Studentparlamentet
- Avdeling for forskning, utdanning og formidling

Disse er tatt inn i vedlegg seks-ni.

Høringssvarene var i stor grad positive til strategien og behovet for denne, men hadde noen innspill og kommentarer.

Tilbakemeldinger som går igjen i høringsinnspillene knytter seg til opplæringsbehovet, avklaringer rundt roller og ansvar samt hvordan vurderingene og avveiingene knyttet til akseptabel risiko skal anvendes.

UiT har en stor utfordring knyttet til opplæring innenfor informasjonssikkerhet; dette er et tema alle må kunne noe om, men hvor mye varierer ut fra bl.a. stilling og ansvarsområder. Universitetsdirektøren har vurdert det slik at den nærmere konkretisering av hvordan opplæringen

[4] Både teknisk-administrativt og vitenskapelige ansatte deltok i workshopen.

skal foregå ikke tas inn i selve strategien, men utarbeides og fastsettes i forbindelse med gjennomføringen av strategien.

Rolle og ansvar er regulert av kapittel 3 i styringssystemet, men det hersker en del usikkerhet rundt dette. På bakgrunn av høringssvarene er det tatt inn litt ekstra informasjon i strategien som klargjør noen av de mest sentrale punktene i ansvarsfordelingen mellom enhetene og informasjonssikkerhetsrollene sentralt (s. 12 i hoveddokumentet).

Hva gjelder *akseptabel risiko* ser Universitetsdirektøren at dette er et vanskelig tilgjengelig tema, og slik strategidokumentet var da det ble sendt ut på høring kunne tabellene og avveiingene misforstås. Dette er derfor forenklet noe, og ytterligere forklaring er lagt til.

I vedlegg tre følger en nærmere gjennomgang av sentrale tilbakemeldinger mottatt via høringssvarene, og hvordan disse er fulgt opp.

Jørgen Fossland
universitetsdirektør

Dokumentet er elektronisk godkjent og krever ikke signatur

Saksbehandler: Ingvild Stock-Jørgensen

Vedlegg
1 Strategi for informasjonssikkerhet 2019-2021 - hoveddokument - v1.1
2 Strategi for informasjonssikkerhet 2019-2021 - underlagsdokument - v1.1
3 Gjennomgang av høringssvarene - ny informasjonssikkerhetsstrategi
4 Styringssystemet for informasjonssikkerhet ved UiT
5 Brev fra forsknings- og høyere utdanningsministeren vedrørende satsning på, og styring av, informasjonssikkerhet i UH-sektoren
6 JurFak - Høring Informasjonssikkerhetsstrategi
7 BFE-fak - Høring Informasjonssikkerhetsstrategi
8 Studentparlamentet - Høring Informasjonssikkerhetsstrategi
9 FUF - Høring Informasjonssikkerhetsstrategi