Universitetsledelsen
Arkivref: 2023/472/INJ024
Dato: 09.01.2023

SAKSFRAMLEGG

Til:	Møtedato:	Sak:
Universitetsstyret	02.02.2023	

Utvidelse og revidering av ledelsessystemet for informasjonssikkerhet og personvern

Innstilling til vedtak:

1. UiT skal utarbeide et samlet *Ledelsessystem for sikkerhet, beredskap og personvern*, med utgangspunkt i dagens ledelsessystem for informasjonssikkerhet og personvern.

2. Organiseringen av arbeidet med sikkerhet, beredskap og personvern skal følge rammene og linjene som er skissert opp i «alternativ A» i vedlegg 1 og 2.

3. Rektor bes legge frem sak om revidering av dagens ledelsessystems styrende del i løpet av vårsemesteret 2023

4. Revidert kapittel 2 i dagens ledelsessystem for informasjonssikkerhet og personvern, herunder veikart for informasjonssikkerhet og personvern 2023, vedtas som foreslått.

Bakgrunn:
Denne saken er todelt og inneholder:

1. forslag om at UiTs arbeid innenfor informasjonssikkerhet, personvern, samfunnssikkerhet, beredskap og nasjonal sikkerhet skal samles i ett helhetlig ledelsessystem, og hvordan dette arbeidet skal være organisert.

2. forslag til revidering av kapittel to i UiTs eksisterende ledelsessystem for informasjonssikkerhet og personvern

1. Samlet ledelsessystem for sikkerhet, beredskap og personvern

UiT er underlagt sikkerhetsloven. Blant de kravene som stilles er at virksomheten har et styringssystem for sikkerhet slik dette er angitt i loven. Kravet gjelder uavhengig av om institusjonen har gradert informasjon eller ikke, og uavhengig av om omfanget av graderte opplysninger er stort eller lite. Kunnskapsdepartementet viser til dette kravet i tildelingsbrevet for 2023 (pkt. 4.2.1), og det er inkludert i punktene som UiT skal rapportere på i årsrapporten for 2023 (behandles av styret i mars 2024). I tildelingsbrevet heter det at UiT i årsrapporten skal *«[r]edegjøre for arbeidet med å utarbeide et styringssystem for sikkerhet, herunder hvordan dette*

samordnes med ledelsessystem for informasjonssikkerhet og virksomhetsstyringen for øvrig. (jf. styringsdokumentets kap 7)».

UiT har i dag en rekke rutiner og regler for beredskap og sikkerhet, men har ikke et samlet *styringssystem* for sikkerhet etter sikkerhetsloven. Dette må utarbeides, og ses i sammenheng med det allerede etablerte ledelsessystemet for informasjonssikkerhet og personvern. UiTs arbeid innenfor dette bør også ses i sammenheng med øvrig sikkerhet- og beredskapsarbeid.

Kunnskapsdepartementet har utarbeidet et styringsdokument for arbeid med sikkerhet og beredskap i KDs sektor, som skal ligge til grunn for arbeidet med samfunnssikkerhet og beredskap, nasjonal sikkerhet, informasjonssikkerhet og personvern. Dette inkluderer også tema som eksportkontroll. Rapporteringskravene for sikkerhet og beredskap i tildelingsbrevet gjenspeiler kravene som stilles i styringsdokumentet.

Å forvalte og arbeide med disse områdene i sammenheng vil kunne gi gode gevinster. Fra et overordnet, styringsperspektiv vil det være enklere å se sårbarheter og risikoer på tvers, man kan samordne enkelte prosesser og for ledere, ansatte og studenter vil det være enklere å få en oversikt over UiTs sikkerhetsarbeid, og hvilket ansvar og oppgaver de har.

Rektor foreslår derfor at UiT utarbeider et samordnet ledelsessystem for sikkerhet, beredskap og personvern. Dette tar utgangspunkt i dagens ledelsessystem for informasjonssikkerhet og personvern (https://uit.no/sikkerhet), og reviderer dette slik at de ovennevnte feltene reguleres sammen.

Rektor har vurdert to alternative måter å organisere det samlede sikkerhetsarbeidet på. Et alternativ (B) innebærer at kjernekompetansen innfor sikkerhet og beredskap samles i en egen organisatorisk enhet ledet av en sikkerhetsleder som rapporterer direkte til rektor. Et annet alternativ (A) er at man ikke bygger opp en separat ny sikkerhetsenhet med en egen rapporteringslinje, men heller lar sikkerhetsarbeidet følge de organisatoriske ansvarslinjene som finnes på beredskapsområdet i dag, og integrerer dette i den strukturen som allerede er etablert for arbeidet med informasjonssikkerhet og personvern. I vedlegget omtales de to alternativene nærmere. Bl.a. basert på anbefalinger fra NSM og de føringene som er gitt i Kunnskapsdepartementets styringsdokument tilrår rektor at styret velger alternativ A slik dette er skissert i vedlegg 1 og 2.

Om styret slutter seg til forslaget vil rektor komme tilbake med konkret forslag til revidering av dagens ledelsessystems styrende del (der roller og ansvar er beskrevet) i løpet av vårsemesteret 2023.

2. Revidering av kapittel 2 i ledelsessystem for informasjonssikkerhet og personvern

I 2019 vedtok UiT en strategi for informasjonssikkerhet for perioden 2019 – 2021. Denne er senere prolongert ut 2022. Strategien utgjør kapittel to i ledelsessystemet, og inneholder overordnede mål, visjon, tiltak og kriterier for akseptabel risiko.

De overordnede målene og visjonen er fremdeles relevant og kan i stor grad beholdes med en viss revisjon for å inkludere personvern, som ble del av ledelsessystemet i 2020. Tiltak for å oppnå disse må imidlertid fastsettes, og erfaring viser at å vedta forholdsvis detaljerte tiltak for en treårsperiode er for langt tidsaspekt på informasjonssikkerhetsområdet.

Rektor foreslår derfor at strukturen legges om, og at kapittel to revideres til å inneholde overordnede mål og visjon for arbeidet, samt kriterier for akseptabel risiko. Yttergrensene for akseptabel risiko beholdes slik de var vedtatt av styret i 2019, men i forslaget er disse knyttet nærmere opp mot nivåene som benyttes for å vurdere risiko (sannsynlighet + konsekvens), da mange fant det vanskelig å benytte de fastsatte kriteriene fra 2019 i praksis. Se vedlegg 3 for forslag til revidert kapittel to.

Forankret i kapittel to utarbeides det et veikart med tiltak for å oppnå målbildet for informasjonssikkerhet og personvern. Tiltakene fastsettes for en periode på 12 måneder, og vil rapporteres på i forbindelse med årsrapporten. Samtidig vil det bli lagt frem forslag for tiltak for påfølgende 12-månedersperiode. Se vedlegg 4 for forslag til veikart for 2023.

Dag Rune Olsen
rektor

Dokumentet er elektronisk godkjent og krever ikke signatur

Saksansvarlig: Jørgen Fossland
Saksbehandler: Ingvild Stock-Jørgensen

Vedlegg

1. Del 1 - Forslag til organisering av sikkerhetsarbeidet
2. Del 1 - Skisse til samlet ledelsessystem og tilhørende organisering
3. Del 2 - Revidert kapittel 2 - visjon for informasjonssikkerhet og personvern, akseptabel risiko
4. Del 2 - Veikart 2023