

Organisering av arbeidet med informasjonssikkerhet, samfunnssikkerhet, beredskap og personvern

Ved utvidelsen av *Ledelsessystem for informasjonssikkerhet og personvern* til *Ledelsessystem for sikkerhet, beredskap og personvern* inkorporeres flere forvaltningsområder ved UiT under ett og samme ledelsessystem, samt at noe nytt tilføres (styringssystem etter sikkerhetsloven og kommende retningslinjer og rutiner tilknyttet eksportkontroll). Erfaring gjennom evaluering av sikkerhetshendelser, resultat av internrevisjon mv.. viser at det må foretas revidering av flere av dagens styrende dokumenter. Det er spesielt behov for nærmere avklaring av hva som ligger til de ulike rollene og hvordan ansvarsdelingen mellom nivå 1 og 2 skal detaljeres. Denne gjennomgangen faller godt sammen med en samtidig utvidelse av ledelsessystemet, hvor flere områder må ses i sammenheng.

I sine «Grunnprinsipper for sikkerhetsstyring» fremgår det at NSM erfarer at «*de mest alvorlige avvikene ved tilsyn gjerne forekommer i virksomheter hvor sikkerhet er noe litt «annerledes», noe som behandles i et eget fagområde og av en adskilt gruppe mennesker*» (s. 6). Et samlet ledelsessystem for sikkerhet, beredskap og personvern som kobler sammen de ulike fagfeltene og systematiserer arbeidet på tvers av organisatoriske enheter vil være et godt første steg for å få disse temaene mer integrert i den overordnede virksomhetsstyringen.

Tilnærmingen til felles ledelsessystem og oppdelingen støttes opp av *Styringsdokument for arbeidet med sikkerhet og beredskap i Kunnskapsdepartementets sektor* («*Styringsdokumentet*»). Her fremhever Kunnskapsdepartementet (KD) at «*Dokumentet går med det fra å hovedsakelig vektlegge arbeidet med samfunnssikkerhet, til å omfatte de tre sikkerhetsområdene samfunnssikkerhet, nasjonal sikkerhet og informasjonssikkerhet og personvern. Inndelingen i ulike sikkerhetsområder har til hensikt å strukturere sikkerhetsarbeidet, som møter ulike krav i ulike regelverk. Samtidig legger KD til grunn at sikkerhetsarbeidet i sektoren følger en helhetlig tilnærming.*».

Dette er også i tråd med signalene Universitetsstyret ga i styremøtet 10. november 2022 om at de ønsket se helheten i de sikkerhetsmessige problemstillingene og arbeidet ved UiT, fremfor tematisk adskilte områder (slik som eksempelvis IKT-sikkerhet for seg selv osv.).

For at dette skal fungere i praksis innebærer det at det må etableres en klar ansvarsfordeling for de ulike elementene, samt sørge for at samhandlingen sikres ved en hensiktsmessig organisering.

Som utgangspunkt vil UiT håndtere lite til intet gradert materiale (jf. sikkerhetsloven). Det må foreligge klart ansvar (eksempelvis for autorisasjon) og retningslinjer hvis det skulle bli tilfelle, men det er p.t. ikke nødvendig for UiT å bygge en sentralisert, samlet sikkerhetsorganisasjon som er rigget for å håndtere slikt materiale i stort eller utbredt omfang.

Nedenfor følger en redegjørelse for dagens organisering samt to alternative forslag til hvordan dette kan gjøres ved etablering av et samlet ledelsessystem, for styrets vurdering.

1. Dagens organisering

Informasjonssikkerhet og personvern har et etablert ledelsessystem (se <https://uit.no/sikkerhet>), som er vedtatt av Universitetsstyret og forvaltes i det daglige av *Faggruppe for informasjonssikkerhet og personvern («FPI»)* på Avdeling for IT.

Administrasjonsdirektør er gitt et overordnet ansvar for disse feltene, mens IT-direktør har forvaltningsansvaret for informasjonssikkerhet og personvern ved UiT, og har instruksmyndighet overfor alle enheter ved UiT i saker som angår informasjonssikkerhet og personvern. Faggruppen utøver IT-direktørens myndighet.

Enhetsleder er ansvarlig for å tilfredsstille kravene til informasjonssikkerhet og personvern i egen enhet. Alle enhetene rapporterer årlig til faggruppen med identifisering og vurdering av enhetens informasjonsverdier, sårbarheter og risikoer, internt arbeid med tematikken samt tiltak for påfølgende år. Denne rapporteringen ble igangsatt for nivå 2 høsten 2019, og nivå 1 høsten 2021.

Universitetsstyret behandler årlig årsrapport for informasjonssikkerhet og personvern, og deretter behandles rapporten av samtlige enhetsstyrer (fakultetsstyrene, bibliotekstyret og styret i UMAK) samt ledermøtene på nivå 1 (ITA, FUF, BEA og ORGØK). Enheten forbereder selv saken for enhetsstyret/ledermøtet, og skal her også ha fokus på utfordringer og tilstand i sin enhet. *Faggruppe for informasjonssikkerhet og personvern* skal gis tilgang til sakspapirer og referat i etterkant av behandlingen på enhetene, og er til stede under møtene i den grad enhetene ønsker det. For de fleste enhetene på nivå 2 gjennomføres det et formøte mellom enhetsledelsen og faggruppen i forkant av produksjon av saken for enhetsstyret.

Samfunnssikkerhet og beredskap ivaretas gjennom beredskapslinja som forvaltes av ORGØK der det er etablert en faggruppe for HMS og beredskap.

UiT som beredskapsorganisasjon styres administrativt gjennom sentral beredskapsgruppe som ledes av administrasjonsdirektør sammen med avdelingsdirektører, kommunikasjonssjef og beredskapskoordinator (seniorrådgiver ved faggruppe HMS og beredskap). I tillegg er det ti lokale beredskapsgrupper tilhørende lokale beredskapsområder, med egne lokalt tilpassede beredskapsplaner. Berørt enhet bistår sentral beredskapsgruppe avhengig av hendelse.

Fakulteter/enheter og eksterne virksomheter som har aktiviteter på områder der en lokal beredskapsenhet er hovedbruker, samordner sin beredskap med hovedbrukeren. Ressurser hentes inn internt eller eksternt etter hendelse og krisens art.

Dokumenter som omhandler arbeid med beredskap, er å finne både i HR-portalen og på intranett. Arbeid med aktør, ansvar og oppgaver i beredskapsarbeidet er gjennomgått, men ikke besluttet. I og med at revisjon er planlagt er det en god anledning å ta dette samtidig med en omstrukturering av dokumentmaterialet slik at det kan inkorporeres i et samlet Ledelsessystem for sikkerhet, beredskap og personvern.

Arbeidet med samfunnssikkerhet og beredskaps rapporteres i dag til Universitetsstyret gjennom årsrapporten om HMS, samfunnssikkerhet og beredskap (SoB). Universitetsstyret ber rektor om å følge opp identifiserte utviklingsområder og iverksette nødvendige tiltak slik at universitetets mål for HMS og SoB kan nås. Fakulteter/enheter bes om å behandle rapporten som egen sak i sine beslutningsorganer med særlig henblikk på egne forbedringsområder.

Fysisk objektsikkerhet og planverk for brannvern ivaretas av Avdeling for bygg og eiendom.

Sikkerhetsloven samt eksportkontroll er ikke i dag del av noe styringssystem på UiT, men består dels av ulike rutiner og praksis ved de enheter som hittil primært har befatning med disse temaene. Dels mangler retningslinjer og rutiner på dette feltet, og slike må utarbeides. Det pågår et arbeid ved UiT for utvikling av retningslinjer, rutiner mv. for ivaretagelse av eksportkontroll, og dette arbeidet vil påvirkes av pågående arbeid nasjonalt. Regjeringen har varslet at de vil komme med en ny eksportkontrollforskrift med utgangspunkt i forskriftsendringer som var på høring våren 2022. Hva disse endringene til slutt vil bestå i er ikke klart, men det fremstår som svært sannsynlig at regelverket blir strammet til.

HMS har et etablert system og organisering, som forvaltes av ORGØK. Det er ikke tenkt at HMS skal tas inn i det utvidede *Ledelsessystem for sikkerhet, beredskap og personvern*. Dette følger også tankegangen og strukturen i Styringsdokumentet, hvor er samfunnssikkerhet, beredskap, informasjonssikkerhet og personvern inntatt i samme styrende dokument, og KD skriver her at «Arbeidsmiljørelatert HMS-arbeid er i utgangspunktet ikke en del av samfunns-sikkerhetsarbeidet, men det er viktig å se områdene i sammenheng», pkt 2, s. 5.

Krav til roller i sikkerhetsarbeidet

De ulike regelverkene stiller noen ulike krav til hvilke roller som må ivaretas. De fleste av disse har UiT allerede, og behøver eventuelt kun noen få justeringer i beskrivelsen ved samordningen av arbeidet. På nåværende tidspunkt ser det ut til at det i liten grad behov for etablering av helt nye roller, og mer tale om å utvide noen av de eksisterende rollene. Det bør imidlertid etableres noen nye samarbeidsarenaer, se nedenfor.

Såfremt det besluttet at det skal utarbeides et felles ledelsessystem for sikkerhet, beredskap og personvern vil det bli fremmet en sak senere i vår for revidering av dagens ledelsessystems kapittel om roller og ansvar.

2. Fremtidig organisering

Samordningen til ett helhetlig ledelsessystem for sikkerhet, beredskap og personvern vil gi UiT mulighet til å bedre se de ulike feltene i sammenheng, og oppnå en mer strukturert tilnærming til arbeidet.

I dag er ikke arbeidet på tvers av fagfeltene spesielt godt koordinert, og ved å samordne informasjonssikkerhet, personvern, samfunnssikkerhet og beredskap vil det være behov for å se hvordan dette arbeidet skal organiseres slik at ansvaret og linjene er klare, og samhandling kan sikres. Nedenfor skisseres to alternative måter å gjøre dette på.

2.1 Alternativ A

Dette alternativet innebærer ingen større organisatoriske endringer, men klargjøring av ansvarslinjer, etablering av forum for samhandling og mindre organisatoriske endringer internt i en av avdelingene i fellesadministrasjonen.

Ved hjelp av fullmakter, klare ansvarsforhold og etablering av samhandlingsarenaer kan dagens hovedfordeling av ansvar for de ulike fagområdene forbli der de er (organisatorisk), og man vil kunne oppnå de gevinstene som søkes gjennom samordning av ledelsessystemet.

I vedlagt powerpoint «Ledelsessystem for sikkerhet, beredskap og personvern – skisse til samlet system og tilhørende organisering» presenteres dette forslaget nærmere, på et overordnet nivå.

Forvaltning av ledelsessystemet som sådan og de enkelte elementer i det

Forvaltningen av ledelsessystemet forblir slik den er i dag, dvs at den følger informasjonssikkerhets- og personvernlinjen, men de ulike avdelingene vil ha ansvar for å bidra innenfor sine felt, ved å holde reglement og regelverk oppdatert, gjennomføre relevante tiltak fastsatt i ledelsessystemet, ta del i utarbeidelsen av årsrapporten mv.

Rapportering

Dagens årsrapport for informasjonssikkerhet og personvern, som rektor fremmer for styret i første kvartal hvert år, vil med forslaget ovenfor bli utvidet til en årsrapport for sikkerhet, beredskap og personvern. Dette innebærer at samfunnssikkerhet og beredskap tas ut av årsrapporten for HMS, samfunnssikkerhet og beredskap. Den sistnevnte vil heretter være en ren HMS-rapport.

Ressurser fra ulike deler av fellesadministrasjonen (ITA, ORGØK, BEA og FUF) vil bidra inn til arbeidet med årsrapporten for sikkerhet, beredskap og personvern. Faggruppe for informasjonssikkerhet og personvern vil være saksbehandler for administrasjonsdirektøren som vil ha det overordnede og formelle ansvaret for at utkast til rapport leveres til rektor.

Personneltmessige justeringer

I dag er beredskapsrådgiver i faggruppe for HMS og beredskap, og er den eneste i faggruppa som arbeider med beredskap i hel stilling. Ved UiT har beredskap hatt en tendens til å bli forvekslet med HMS, og har ikke fått den synlighet som det bør og må ha.

Forslaget er derfor at beredskapsrådgiver flyttes til staben for avdelingsdirektør for ORGØK. Det vil øke synligheten, og vil også innebære at beredskapsrådgiver organisatorisk er på samme «nivå» som faggruppe for informasjonssikkerhet og personvern (plassert direkte under IT-direktør) og brannrådgiver (plassert i staben til BEA-direktøren).

Samarbeidsforum

Det er behov for arenaer for samarbeid, og dette kan løses dels ved å utvide eksisterende forum og dels ved å opprette nye.

- Forum for sikkerhet og personvern

Dette vil være en utvidelse av dagens forum for informasjonssikkerhet og personvern, som ble opprettet i 2019. Det er et rådgivende forum, og alle enhetene har én representant i dette forumet, og medlemmene er fra fakultetsledelse, vitenskapelige og administrative stillinger. IT-direktør har fått delegert myndighet fra administrasjonsdirektør til å oppnevne nye medlemmer av forumet.

Forumet ledes av representant fra faggruppe for informasjonssikkerhet og personvern.

- **Beredskapsforum**

Dette vil være et nytt forum, som skal ledes av sentral beredskapsleder (administrasjonsdirektør) og består av deler av sentral beredskapsgruppe samt lederne for de lokale beredskapsgruppene.

Koordineringsansvar vil ligge til ORGØK v/beredskapsrådgiver.

- **Eksportkontroll/internasjonalt samarbeid**

Arbeidet med eksportkontroll (teknologi, varer og kunnskap) er komplekst, og en arbeidsgruppe fra 2021 så behovet for at det ble opprettet et tverrfaglig team som kan opparbeide seg god kompetanse på dette feltet. Teamet bør forvaltes av FUF, og består av administrasjonsdirektør, prorektor forskning samt representanter fra ORGØK, ITA og enkelte fakulteter. Det skal rapportere til rektor. Teamet vil både kunne gi innspill og råd.

Nasjonale forum, samarbeid og ressurser

UiT håndterer ikke disse temaene og spørsmålene alene. Det er nasjonale forum og ressurser både i og utenfor sektoren, eksempelvis Beredskapsrådet og Cybersikkerhetssenteret. Der hvor det finnes nasjonale ressurser skal det ikke bygges opp parallellkompetanse, eksempelvis arbeides det med nasjonale ressurser og retningslinjer i tilknytning til eksportkontroll. UiT må fremdeles ha lokale ressurser og retningslinjer, men disse må gjøre bruk av de kommende nasjonale ressursene der det er relevant. Foreløpig er det ikke klart hvilken form disse får.

Videre er det nødvendig å gjennomgå og håndtere samhandlingen med nasjonale sikkerhetsmyndigheter, slik som NSM og PST. Kontakten med PST er både fast og sentralisert (fast møter mellom PST og rektor, administrasjonsdirektør, IT-direktør og sikkerhetssjef), men det er også andre treffpunkter mellom universitetet og PST. Tidvis tar også PST direktekontakt med enkelte miljøer eller campus og ber om møter, og det vil være nødvendig å få en helhetlig og samlet tilnærming til dette fra universitetets side.

2.2 Alternativ B

Dette alternativet innebærer at det opprettes en organisatorisk enhet med et team for sikkerhet og beredskap som rapporterer direkte til rektor. Teamet ledes av en sikkerhetsleder. Dagens ressurser rundt forvaltning og styring av områdene samles her. Det må gås opp hvilke ressurser som bør inngå, men som utgangspunkt bør faggruppe for informasjonssikkerhet og personvern, beredskapsrådgiver, brannkoordinator og en ressurs tilknyttet eksportkontroll/sikkerhet i internasjonalt samarbeid inngå.

Fordelen med en slik organisering er nærhet til den øverste toppledelsen samt samling av spisskompetanse i et felles arbeidsmiljø. I forbindelse med kontrollvirksomhet overfor enhetene vil den organisatoriske distansen også kunne være en fordel.

Dette alternativet anbefales likevel ikke. For enkelte virksomheter kan modellen være en hensiktsmessig løsning, men med tanke på hvor universitetet nå er i arbeidet med de ulike feltene fremstår denne typen omorganisering som potensielt mer skadelig enn fordelaktig. Eksempelvis har plasseringen av ressursene i de ulike avdelingene i fellesadministrasjonen sine fordeler med tanke på å fange opp aktivitet, og ha nærmere kontakt med kjernevirksomheten. I verste fall vil en separat

organisatorisk enhet med en egen rapporteringslinje føre til at sikkerhet blir et anliggende på siden av den ordinære virksomheten (jfr. erfaringene fra NSM nevnt ovenfor).

Med tanke på kontrollvirksomhet kan nødvendig uavhengighet mellom fagressursene og den enheten de organisatorisk tilhører, sikres gjennom fullmakter og rapporteringslinjer direkte til universitetsledelsen i enkelte typer saker. Ett eksempel er årsrapporten, som foreslås levert direkte fra faggruppe for informasjonssikkerhet og personvern til administrasjonsdirektør. Faggruppa står da som saksbehandler for årsrapporten, men de ulike avdelingene bidrar til innholdet innenfor hvert sitt ansvarsområde. Det er administrasjonsdirektør som er ansvarlig for årsrapporten, og leverer den til rektor som (gitt endelig godkjenning) fremmer den for styret.

Nærhet og korte linjer til toppledelsen kan også sikres på mer hensiktsmessige måter enn forholdsvis radikal omorganisering, eksempelvis ved å innta disse områdene som faste tema på et visst antall ledermøter i året, samt via den samme typen fullmakter og direkte rapporteringslinjer som nevnt i avsnittet ovenfor.

Samarbeidsforumene nevnt under alternativ A foreslås etablert også hvis alternativ B velges.

I og med at rektor ikke ønsker å anbefale alternativ B er modellen ikke utredet i nærmere detalj. Dersom styret anser dette som et aktuelt og ønskelig alternativ må spørsmålet om organisering av arbeidet utsettes, slik at modellen kan utredes og detaljeres før endelig beslutning tas.