SAKSFRAMLEGG

Til:	Møtedato:	Sak:
Fakultetsstyret for Det helsevitenskapelige fakultet		

Helsefaks behandling av årsrapport for informasjonssikkerhet og personvern 2020

Innstilling til vedtak:
Årsrapport for informasjonssikkerhet og personvern 2020 tas til orientering.

Bakgrunn:
Avdeling for IT (heretter ITA) har ansvar for informasjonssikkerhet på UiT. Årlig utarbeider ITA en årsrapport for informasjonssikkerhet og personvern, og rapporten legges frem for Universitetsstyret. Universitetsstyret fattet den 4 mars 2021 vedtak om at årsrapporten skulle tas opp i styret for alle fakulteter, UB og UMAK.

Årsrapporten for 2020 har to særlige fokusområder. Det første fokusområdet er det store datainnbruddet UiT ble utsatt for på slutten av 2020. Datainnbruddet påvirket store deler av UiT, også driften ved Helsefak. Eksempelvis ble Eutro tatt ut av drift i en lengre periode. ITA vil redegjøre nærmere for datainnbruddet i fakultetsstyremøtet. I tillegg har man i årsrapporten hatt søkelys på de ulike enhetenes statusrapporter for 2020. Helsefaks statusrapport for 2020 ble lagt frem for fakultetsstyret 25.02.2021.

Som en del av oppfølgingen av Universitetsstyrets vedtak, tas saken nå opp for Fakultetsstyret med særlig fokus på forbedringsområder for Helsefak. Årsrapporten er lagt ved saken som vedlegg 1.

Hovedpunkter i årsrapporten
Et av hovedfokusene i årsrapporten er det store og alvorlige datainnbruddet som UiT ble utsatt for på slutten av 2020. For Helsefak fikk dette konsekvenser ved at Eutro som blant annet blir brukt til lagring av forskningsdata stengt i perioden 19.10.2020 til 22.2.2021.
Andre fokusområder for årsrapporten er;

- Årlige status-/egenrapportering fra fakultetene og andre enheter
- Utfordringer som følge av korona og tilhørende omlegginger
- Særskilte problemstillinger rundt internasjonalisering

Den nåværende informasjonsstrategien gjelder til og med 2021, og den inneholder en rekke tiltak. ITA informerer at UiT er på etterskudd med gjennomføringen av disse tiltakene. Ved fjorårets årsrapportering forventet ITA å gjennomføre tiltakene som ikke var gjennomført, men ser at man

ikke har lyktes med dette. Det skyldes i stor grad omprioriteringer i forbindelse med korona og omorganisering av ITA. For Helsefak har dette hatt betydning med at ITA ikke har kunne gjennomføre opplæring som planlagt eller vurdert behov for konkrete verktøy i oppfølgningen av arbeidet med informasjonssikkerhet og personvern. ITA forventer at en del av tiltakene i strategien vil gjennomføres i 2021, men at samtlige tiltak heller ikke vil bli fullført i 2021.

Årsrapporten trekker frem særskilte utfordringer og behov for videreutvikling av organisasjonen:

- Fokus hos ledelsen. Her har det vært en forbedring de siste to årene, og behandlingen i fakultetsstyrene trekkes frem som svært nyttig. Det er imidlertid fremdeles et behov for å styrke oppmerksomheten og kompetansen i ledelseslinjen på UiT, og ITA ønsker å ha personvern og informasjonssikkerhet som tematikk på enhetens ledermøter én gang i halvåret.
- Samordning med sikkerhets- og beredskapsarbeidet for øvrig ved UiT
- Behov for profesjonell, ekstern bistand og mer samarbeid på tvers i UH-sektoren utover det Unit tilbyr i dag

Helsefaks statusrapport

Helsefak la frem statusrapporten for fakultetsstyret 25.02.2021. Vi blir derfor ikke å gjennomgå den på nytt, men heller trekke ut de viktigste elementene fra fakultetenes statusrapporter. Fakultetene har trukket frem flere viktige utfordringer knyttet til informasjonssikkerhet.

- Utfordringer knyttet til mottak av fortrolig informasjon
- Verktøyene som UiT gjør tilgjengelig for ansatte og studenter
- Manglende oversikt over helhetsbildet
- Ansatte og studenter fra ulike nasjoner
- Behov for kurs og opplæring knyttet til informasjonssikkerhet

I tillegg har flere av fakultetene opplyst i sine statusrapporter om at ressursbruken knyttet til arbeid med informasjonssikkerhet har økt. Flere av fakultetene har gjort organisatoriske endringer for å imøtegå det økte behovet for å løse oppgaver knyttet til informasjonssikkerhet.

Kurs/opplæring

Flere av enhetene, inkludert Helsefak, rapporterte om behov for opplæring knyttet til informasjonssikkerhet. Helsefak har selv utarbeidet opplæringsmateriell i form av brosjyre rettet mot studenter som skal skrive bachelor- og masteroppgave, hvor elementer knyttet til informasjonssikkerhet er inkludert. Helsefak har også oppdatert flere av rutinene innen helseforskning til å inkludere elementer av informasjonssikkerhet og personvern. Her gjenstår det et betydelig arbeid, men som kompliseres av at disse rutinene eies sammen med UNN, og UNN i liten grad har kunne prioritere dette arbeidet. Dermed er det tidkrevende å få endret disse da endringer også forutsetter godkjenning fra UNN. Helsefak jobber også med å utvikle et digitalt kurs i helseforskning, som også vil ha noe innhold innen informasjonssikkerhet og personvern. Helsefak ønsker å gå i dialog med ITA for å vurdere mulig samarbeid om dette kurset. Helsefak har avholdt saksbehandlerkurs hvor taushetsplikt og konfidensialitet har vært del av innholdet.

Risikovurderinger

Det kommer frem av årsrapporten at det gjennomføres risikovurderinger ved UiT, men fortsatt ikke i den grad de skal etter gjeldende lovverk og institusjonens egne retningslinjer. Det kommer frem at risikovurderinger må gjennomføres i et langt større antall enn i dag. På Helsefak ble det gjort intern omdisponering av eksisterende ressurser på Prosjektkontoret, hvor to personer nå har

risikovurderinger som del av sine arbeidsoppgaver. Disse mottok opplæring fra ITA våren 2021 og er i gang med å gjennomføre risikovurderinger av forskningsprosjekter.

Det skal gjennomføres risikovurderinger ved oppstart av alle forskningsprosjekter. I tillegg skal det gjennomføres risikovurderinger før oppstart av behandling av personopplysninger, når trusselbildet endres, ved etablering av IKT systemer og ved organisatoriske endringer som kan påvirke informasjonssikkerheten. Alle risikovurderinger som gjennomføres skal dokumenteres. Helsefak må derfor på sikt gjøre den enkelte forsker og systemeier i stand til å gjennomføre risikovurderinger på egen hånd, og heller gi bistand i større og kompliserte prosjekter. Et institutt på Helsefak har utarbeidet en lettversjon for risikovurderinger av masterprosjekter som letter arbeidet betydelig for denne typen prosjekter. ITA informerer at de vil jobbe videre med å utarbeide såkalte «lettutgaver» av risikovurderinger, så prosjekter, prosesser mv som er forholdsvis ukompliserte og benytter kjente IT-systemer, lett kan gjennomføre risikovurdering for eget prosjekt. Helsefak er koblet på videre i dette arbeidet.

Antallet risikovurderinger som gjennomføres eller kan dokumenteres ved Helsefak står ikke i forhold til antall prosjekter som utføres. Antallet gjennomførte risikovurderinger er også tidligere lagt frem for fakultetsstyret, hvor fakultetsstyret ba om at det ble utarbeidet et parameter som gjør det mulig å følge utviklingen i gjennomførte risikovurderinger.

UiT har ikke et datasystem hvor risikovurderinger skal gjennomføres, men gjennomfører risikovurderinger i Excel. Det betyr at Helsefak ikke kan ta ut ferdig genererte rapporter, men må følge utviklingen manuelt. For å kunne si noe om utviklingen i gjennomførte risikovurderinger over tid, vil Helsefak derfor føre en manuell oversikt som fremover vil kunne si noe om trenden i utførte risikovurderinger.

Antall risikovurderinger gjennomført på Helsefak:

År	**Antall gjennomførte risikovurderinger**
2019	4
2020	7
2021	24 (per september 2021)

ITA har gitt Helsefak tilbakemelding om at de ser at det har vært en økning i antall risikovurderinger gjennomført på fakultetet, noe som tyder på at fakultetet har gjort et godt arbeid med å informere om når risikovurderinger skal gjennomføres. ITA er ellers enig med Helsefak om at det skal jobbes med å utarbeide rapporter som kan benyttes i evt. ledelsens gjennomgang.

Innmeldte avvik

I 2020 ble det meldt inn 14 avvik til faggruppe for informasjonssikkerhet og personvern. Dette var en nedgang i meldte avvik fra 2019 hvor det ble meldt inn 20 avvik. Av de 14 avvikene ble 4 meldt til Datatilsynet. UiT er ikke ilagt sanksjoner av Datatilsynet.

Tre av avvikene er direkte knyttet opp til Helsefak:

Enhet på Helsefak	**Kort beskrivelse**	**Tiltak**	**Meldt Datatilsynet?**	**Lukket?**
Institutt for psykologi	Opptak av undervisning knyttet til film «Rekonstruksjon	Opptak slettet	Nei	Ja

	Utøya». Etter filmen ble samtale om filmen mellom studentene tatt opp uten at studentene var klar over dette på forhånd.			
Helsefak	Forsøk pålogging i Eutro med databasebruker.	Oracle-konto stengt grunnet antall påloggingsforsøk	Nei	Ja
Helsefak	Trakassering via falskt navn i zoom	Følges opp av fagmiljøet. ITA ser på innstillinger i zoom.	Nei	Ja

ITA har opplistet de fem mest alvorlige avvikene i årsrapporten. Ett av disse avvikene er avviket referert i tabellen over knyttet til Institutt for psykologi. To av avvikene er gjelder flere av fakultetene, men Helsefak har ikke oversikt over om vi også har hatt slike avvik. UiT hadde i 2020 et større datainnbrudd som også har påvirket Helsefak. ITA vil redegjøre nærmere for datainnbruddet under fakultetsstyremøtet.

I årsrapporten fremgår det at det er svært sannsynlig at det er en betydelig underrapportering av avvik ved UiT, og at det kan skyldes manglede kompetanse og oppmerksomhet på hva som skal meldes som avvik. ITA opplever også at flere av avvikene ikke meldes inn gjennom avvikssystemet til UiT, men oppdages i andre kanaler, som for eksempel at det meldes fra om mistet utstyr etc. til orakelet. I årsrapporten for 2020 går det frem at underrapporteringen av avvik også kan skyldes at en rekke sikkerhetsavvik meldes via en annen linje internt på ITA og at Helsefak har egne rutiner for melding av avvik knyttet til helseforskning. Det er ikke meldt om avvik i Helsefaks system for avviksrapportering for helseforskning, og i fakultetets statusrapport ble underrapportering av avvik opplistet som en sårbarhet for Helsefak. Manglende avviksrapportering både knyttet til informasjonssikkerhet og helseforskning gjør det vanskelig for Helsefak å identifisere mulige sikkerhetsutfordringer og iverksette tiltak for å ivareta informasjonssikkerheten. Helsefak har vært i dialog med ITA for å forsøke å gjøre det enklere å melde inn avvik, ved at avvik meldes inn digitalt gjennom samme system. Ved å forenkle systemet for å melde avvik, håper vi at det skal komme inn flere avviksmeldinger. Vi har ennå ikke kommet i mål med felles portal for å melde avvik. I årsrapporten går det frem at det er nødvendig å samle og harmonisere meldeprosedyrene på tvers av alle fagområder for å få inn et reelt antall avvik, dette har betydning for arbeidet vi har påbegynt knyttet til avviksmeldinger innen helseforskning og informasjonssikkerhet.

I tillegg til å forenkle samle og harmonisere avvikssystemet er det nødvendig å tilby opplæring knyttet til hva et avvik er og hvordan avvik meldes. Helsefak har ikke hatt ressurser til å tilby slik opplæring i 2020, eller så langt i 2021. Enkelte institutt har etterspurt opplæring som mer spesifikt er tilpasset deres aktiviteter.

ITA skriver i årsrapporten at for å lykkes må opplæring innen informasjonssikkerhet og personvern i stor grad innlemmes i annen opplæring, eksempelvis opplæring i bruken av en IT-tjeneste, den øvrige opplæringen en nyansatt får når vedkommende starter, undervisningen

studentene mottar mv. Dette er imidlertid mer krevende å få til enn mer spesialisert opplæring innen informasjonssikkerhet og personvern. Til dette bemerker Helsefak at fakultetet lenge har jobbet med å få på plass en digital opplæringspakke innen helseforskning rettet mot forskere, men dette arbeidet har blitt nedprioritert som følge av andre oppgaver især bestillinger innen personvern og informasjonssikkerhet. Det kan imidlertid være en løsning å inkludere personvern og informasjonssikkerhet, og dermed også samlet øke ressurser som jobber med opplæringspakken dersom ITA har mulighet til å bidra til arbeidet.

Organisering av informasjonssikkerhet og personvern på Helsefak
Ledelsessystemet for informasjonssikkerhet og personvern har definert sentrale roller på fakultetet.
Dekan («Enhetsleder»):

- Er ansvarlig 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 dette er påkrevd
- Skal rapportere resultat fra risikovurderinger med handlingsplan og avvik til ITA
- Skal følge opp avviksmeldinger i samarbeid med ITA
- 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

Høsten 2020 leverte fakultetene en statusrapport om informasjonssikkerhet, hvor det blant annet ble redegjort for hvordan fakultetene organiserer sitt sikkerhetsarbeid.

Instituttene eller seksjonene har ikke egne definerte roller i ledelsessystemet. Systemeiere, ledere av forskningsprosjekt, studentveiledere, ansatte og studenter har imidlertid egen definerte roller og ansvar.

Det har vært utfordrende for Helsefak å estimere ressursbruk som følge av nye oppgaver knyttet til informasjonssikkerhet og personvern, og i fakultetet har siden 2019 hatt en betydelig økning av oppgaver knyttet til dette. Det kan dreie seg om faste rapporteringer, føring av behandlingsprotokoll, flytting av data fra server til skyløsninger, rapportering på overføring av data til tredjeland, generell veiledning knyttet til informasjonssikkerhet og personvern mm.

Økningen har ikke medført økte ressurser på fakultetet, og fakultetet har derfor vært nødt til å omdisponere interne ressurser for å løse de nye oppgavene knyttet til informasjonssikkerhet og personvern. Det er i dag fire personer på fakultetet som har informasjonssikkerhet og personvern som del av sine arbeidsoppgaver. Det er imidlertid ingen ansatte som har dette som sitt eneste fagfelt, slik som det er organisert på ITA. Fagfeltet er omfattende og komplekst, og i rask utvikling. Det er derfor problematisk å holde seg faglig oppdatert på det detaljnivå som ITA forventer i sine bestillinger til fakultetet. Mangel på tilstrekkelig kompetanse vil kunne medføre at man risikerer at arbeidet, eksempelvis rapporter, blir mer overordnet og at man ikke i tilstrekkelig grad får involvert instituttene eller fanger opp utfordringer og avvik.

Det fremgår videre i årsrapporten at det er nødvendig med økt ressursbruk på alle enheter, for å kunne håndtere de problemstillingene og utfordringene som er innen informasjonssikkerhet og

personvern. ITA har uttrykt at det etter deres mening ikke er satt av tilstrekkelig med ressurser til enhetene til arbeidet med informasjonssikkerhet og personvern.

Det kan diskuteres om det er avsatt tilstrekkelige ressurser på fakultetet til å sikre at arbeidet med informasjonssikkerhet og personvern er tilstrekkelig strukturert og målrettet. Det er imidlertid vanskelig å si noe om ressursbehovet på nåværende tidspunkt uten at det er helt klart på hvilket nivå ITA forventer at fakultetet har kapasitet og kompetanse.

Konklusjon
Fakultetsdirektør og dekan har ansvaret for å ivareta informasjonssikkerheten i sin enhet. For å kunne lykkes i dette arbeidet må man sørge for at lederlinjen har tilstrekkelig søkelys på informasjonssikkerhet. Lederlinjen må videre sørge for at ansatte har tilstrekkelig kompetanse om de rutiner og retningslinjer som finnes og at disse følges i praksis. Årsrapporten viser at det er utfordrende å jobbe så strukturert og målrettet med informasjonssikkerhet og personvern som det legges opp til i ledelsessystemet. Fakultetet bør derfor jobbe med å avklare med ITA hvordan man skal jobbe med informasjonssikkerhet og personvern på fakultetet videre, og om rollene bør formaliseres ytterligere.

Thrina Loennechen
Dekan
–

Trond Nylund
Fungerende fakultetsdirektør
–

Dokumentet er elektronisk godkjent og krever ikke signatur

Saksbehandlere: juridisk seniorrådgiver Jannicke Persen og juridisk seniorrådgiver Frank Tore Mengkrogen

Vedlegg
1 Årsrapport for informasjonssikkerhet 2020