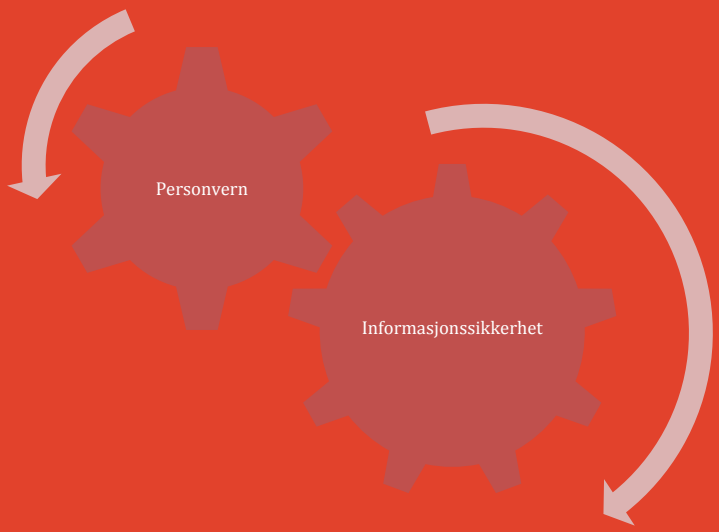
UiT Norges arktiske universitet

Årsrapport informasjonssikkerhet og personvern 2020

Universitetsdirektøren, Avdeling for IT (ITA), 4.3.2020

Ephorte 2018/4050-16



Innhold

Det følger av Ledelsessystemet for informasjonssikkerhet og personvern[1] («ledelsessystemet»), kapittel ni, at det skal utarbeides en årsrapport som gjennomgår arbeidet med informasjonssikkerhet («ledelsens gjennomgang»). Denne rapporten fremlegges for Universitetsstyret i løpet av første kvartal hvert år. Nytt av året er at det også rapporteres på arbeidet med personvern.

Informasjonssikkerheten skal ivareta informasjonens

- **Konfidensialitet** *(informasjonen skal ikke bli kjent for uvedkommende)*
- **Integritet** *(informasjonen skal ikke bli endret utilsiktet eller av uvedkommende)*
- **Tilgjengelighet** *(informasjonen skal være tilgjengelig ved legitimt behov)*

[1] Se https://uit.no/sikkerhet

Om personvern og informasjonssikkerhet

Personvern og informasjonssikkerhet blir ofte omtalt som om det går ut på det samme, og det er derfor nødvendig å foreta en kort, innledende avklaring.

Informasjonssikkerhet er en viktig del av ivaretagelse av personvernet, og følgelig sentrale forpliktelser etter personopplysningsloven og personvernforordningen (GDPR). Imidlertid skal sikkerheten også ivaretas for informasjon som *ikke* inneholder personopplysninger (f.eks byggdata, økonomiske data, forskningsdata som ikke omhandler personer etc).

Tilsvarende gjelder også motsatt. Det er langt mer til ivaretagelsen av personvernet enn informasjonssikkerhet. Eksempelvis må man etter GDPR ha et lovlig grunnlag for å behandle opplysningene (f.eks samtykke, rettslig forpliktelse, oppfyllelse av avtale mv), det er særskilte vurderinger knyttet til gjenbruk, rettighetene til personene skal ivaretas (f.eks informasjonsplikt, rett til innsyn, sletting, retting etc). Dette er ikke del av *informasjonssikkerheten,* men blant de øvrige, sentrale forpliktelser UiT er underlagt etter lovverket (GDPR mv) for ivaretagelse av personvernet.

Det er imidlertid stor overlapp, og i de fleste saker vil ha elementer av begge tema i seg. Det er ikke hensiktsmessig å skille disse fagområdene organisatorisk, og det overordnede forvaltningsansvaret for begge fagområdene ble derfor samlet hos IT-direktør i 2019.

Fokus for årsrapporten 2020

På slutten av 2020 ble UiT utsatt for det klart mest alvorlige datainnbruddet/sikkerhetshendelse i universitetets historie. Når årsrapporten legges frem for Universitetsstyret er ikke opprydningen og håndteringen av denne hendelsen ferdig.

Imidlertid er den mest akutte fasen tilbakelagt, og vi vet en god del. Utfall og etterspill av denne alvorlige hendelsen samt tilhørende tematikk vil bli omtalt i årsrapporten. Dette da alvorlighetsgraden til hendelsen krever store og til dels drastiske omlegginger i UiTs sikkerhetsmodell.

Disse nærmere detaljene om sikkerhetshendelsen og tilhørende oppfølging er tatt inn i vedlegg 2-5, inkludert kopi av orienteringssaken som ble lagt frem for Universitetsstyret 28. januar 2021.

Andre fokusområder for årsrapporten vil være den årlige status-/egenrapporteringen fra fakultetene, Norges arktiske universitetsmuseum og akademi for kunstfag (UMAK) samt Universitetsbiblioteket (UB) (kap. 6), utfordringene korona og tilhørende omlegginger har medført (kap. 7) samt internasjonalisering og de særskilte problemstillingene som må håndteres i den sammenheng (kap. 8).

1 Informasjonssikkerhetsstrategien

Den nåværende informasjonssikkerhetsstrategien gjelder til og med 2021. Strategien er ambisiøs, og har en rekke omfattende tiltak. Ved inngangen til 2020 var UiT på etterskudd med gjennomføringen av den. Det var på tidspunktet for forrige årsrapportering (5.3.2020) vurdert som realistisk at mye kunne hentes inn i løpet av 2020. Dette har organisasjonen ikke lyktes med. Noe skyldes helt nødvendige omprioriteringer i forbindelse med korona, mens en annen medvirkende årsak var at det tok tid etter omorganiseringen av ITA (1.1.2020) før den nye faggruppen for informasjonssikkerhet og personvern fikk satt seg skikkelig.

Særlig tiltak knyttet til sikkerhetsarkitektur, overvåkning av sikkerhetstiltak, vurdering av arbeidsprosesser/sourcing/personellbehov/verktøy samt opplæring er dermed ikke fullført som planlagt i løpet av 2020. Det er tvilsomt om de tiltakene som var planlagt (men forsinket) for 2020 kunne forhindret sikkerhetshendelsen høsten 2020 fullt ut.

Gjennom den omfattende innsatsen i kjølvannet av hendelsen h anses det om sannsynlig at en del av disse tiltakene samt de for 2021 vil bli gjennomført samlet. Dette fordi disse vil være en integrert del av oppfølgingen av hendelsen, som naturligvis vil trekke store deler av ressursene knyttet til informasjonssikkerhet i lengre perioder av 2021.

Grunnet behovet for omfattende oppfølging og håndtering av sikkerhetshendelsen, og fokuset på årsakene til at den kunne inntreffe, vurderes det ikke som sannsynlig at samtlige tiltak (av både teknisk og ikke-teknisk art) i strategien vil være fullført ved slutten av 2021.

Den strategien som skal etterfølge den gjeldende (fra og med 2022) vil måtte inkludere personvern i tillegg til informasjonssikkerhet, for å kunne ha et helhetlig bilde på disse to områdene. Erfaringer fra datainnbruddet vil bli vektlagt også her.

2 Sikkerhetsmål og strategi

I mars 2019 vedtok Universitetet ny informasjonssikkerhetsstrategi, for perioden 2019-2021[2]. Gjennom utvidelsen av ledelsessystemet og den nærmere samlingen av arbeidet med informasjonssikkerhet og personvern, er det påkrevd med en gjennomgang av strategien slik at denne også omfatter arbeidet med personvern. I og med at strategien utløper i 2021 blir dette arbeidet i stor grad lagt til utarbeidelsen av strategi for ny periode.

Fremfor en mer statisk treårsperiode ønsker universitetsdirektøren å foreslå en mer dynamisk tilnærming. Utviklingen på disse feltene skjer i høyt tempo, og det som var sant for tre år siden er ikke nødvendigvis sant i dag.

Gjennom samtaler med Gartner[3] har ITA blitt orientert om at det innenfor informasjonssikkerhet nå er vanligere å ha f.eks en treårsstrategi som utvides (og om nødvendig justeres dersom premissene har endret seg kraftig) hvert år[4]. Siden det vil være en ny og omfattende øvelse å inkludere rene personverntiltak i en slik strategi er det ønskelig å søke ekstern bistand i utarbeidelsen av den nye strategien.

---

[2] Sak S 9/19.

[3] Gartner er et internasjonalt konsulentbyrå, som UiT har avtale med. De fasiliterte blant annet arbeidet med den nåværende informasjonssikkerhetsstrategien.

[4] Eksempelvis slik at i 2021 vedtas strategi for perioden 2022-2024, og i 2022 rapporteres det på denne, og samtidig vedtas utvidelse slik at strategien deretter gjelder for 2023-2025 (med nye tiltak for 2025) og dette gjentar seg årlig.

3 Kriterier for akseptabel risiko

UiT har et vedtatt sett med kriterier for akseptabel risiko. Disse er knyttet opp mot informasjonssikkerhet, og danner noen ytre rammer for hva universitetet er villig til å akseptere for å oppnå sine mål. Disse ble vedtatt av Universitetsstyret i forbindelse med informasjonssikkerhetsstrategien i 2019, og foreløpig foreligger det ikke planer om å revidere disse. Det må imidlertid fokuseres på å informere om disse, og gjøre organisasjonen kjent med hva disse kriteriene innebærer og hvordan benytte dem aktivt.

4 Organisering

Organiseringen er fastsatt gjennom *ledelsessystemet for informasjonssikkerhet og personvern* (kap. 4), og nedenfor gjengis enkelte av de mer sentrale rollene. Ett av tiltakene i informasjonssikkerhetsstrategien er videreutvikling av sikkerhetsorganisasjonen. Her er det tatt konkrete grep, blant annet gjennom opprettelsen av egen *Faggruppe for informasjonssikkerhet og personvern* f.o.m 1.1.2020, men det gjenstår fremdeles arbeidet før vi kan sies å ha en fungerende, helhetlig sikkerhetsorganisering for hele UiT (alle enheter).

- **Universitetsdirektør** har ansvar for informasjonssikkerhet på et overordnet nivå, herunder å sette av tilstrekkelig med ressurser til arbeidet med informasjonssikkerhet. Universitetsdirektøren utøver det overordnede ansvaret for all behandling av personopplysninger ved UiT.
-
- **IT-direktør** har forvaltningsansvaret for informasjonssikkerhet og personvern, og er gitt instruksjonsmyndighet overfor alle enheter ved UiT i saker som angår informasjonssikkerhet og personvern.

- **Enhetsledere** er ansvarlig for å tilfredsstille krav til informasjonssikkerhet og personvern i egen enhet, herunder blant annet å gjennomføre risikovurderinger og iverksette nødvendige tiltak. Høsten 2020 leverte fakultetene og Universitetsbiblioteket en statusrapport om informasjonssikkerhet, hvor det blant annet skulle redegjøres for hvordan enheten organiserer sitt sikkerhetsarbeid. Her har de fleste gjort et svært godt arbeid, og årsrapporten vil komme innpå resultatene fra disse rapportene nedenfor i pkt 6.

- **Faggruppe for informasjonssikkerhet og personvern** utøver IT-direktørens myndighet i saker om informasjonssikkerhet og personvern. Faggruppeleder er UiTs sikkerhetssjef («CISO»). Faggruppen skal blant annet følge opp avvik på et overordnet nivå, drive opplysningsvirksomhet, opplæring og rådgivning. Videre har faggruppen myndighet til å igangsette internrevisjoner innenfor informasjonssikkerhet og/eller personvern på alle enheter på UiT.Denne faggruppen er organisatorisk plassert direkte under IT-direktør, og ikke i en av seksjonene, og består av totalt fem personer inkludert faggruppeleder/sikkerhetssjef.

- **CSIRT**[5] har ansvaret for å håndtere IT-sikkerhetshendelser mens de skjer.

- **Informasjonssikkerhetsforum** skal blant annet gi råd og koordinere planleggingen og gjennomføringen av tiltak og initiativ innenfor informasjonssikkerhet. Forumet har representanter fra samtlige fakulteter, UMAK, UB samt de fleste avdelingene på nivå 1. Dette forumet er nærmere beskrevet i ledelsessystemets kapittel fire[6].

---

[5] Computer Security Incident Response Team (CSIRT)

[6] https://uit.no/om/informasjonssikkerhet#innhold_639741

- **Personvernombudet** skal informere og gi råd til UiTs ansatte og studenter om gjeldende forpliktelser etter personvernlovgivningen, og skal kontrollere UiTs overholdelse av denne lovgivningen. Personvernombudet kan ikke instrueres om utførelsen av de oppgavene som tilligger ombudet etter personvernforordningen (GDPR).

Utfordringer og behov for videreutvikling av organisasjonen

***Fokus hos ledelsen*:** I tidligere årsrapporter har det blitt påpekt at informasjonssikkerhet har hatt for lite fokus hos ledelsen ved UiT. Betydningen av at toppledelsen har fokus på informasjonssikkerhet har også blitt understreket av Kunnskapsdepartementet, blant annet gjennom eget brev til UH-sektoren i begynnelsen av 2019. I tildelingsbrevet for 2020 ble det også referert til dette brevet.

Her har det skjedd en viss bedring, spesielt gjennom de siste to årene. Universitetsstyrets vedtak om at årsrapporten for informasjonssikkerhet skulle behandles i samtlige fakultetsstyrer, styret for Norges arktiske universitetsmuseum og akademi for kunstfag samt bibliotekstyret har vært svært nyttig. I 2020 ble dette gjennomført for annen gang, og *Faggruppe for informasjonssikkerhet og personvern* var i møte med samtlige av de aktuelle enhetene i forkant av behandlingen i styrene. I tillegg til årsrapporten for UiT ble enhetene bedt om å ha fokus på særskilte områder som var viktige eller utfordrende for den konkrete enheten, slik at styrene ble mer involvert. Dette har vært en nyttig tilnærming, og bør opprettholdes som en fast ordning.

Det er imidlertid fremdeles behov for å styrke oppmerksomheten og kompetansen i ledelseslinjen på UiT. Informasjonssikkerhet er egen sak på ledermøtene på Avdeling for IT en-to ganger i semesteret, og det er ønskelig med en tilsvarende kontakt med ledergruppene på de øvrige enhetene. *Faggruppe for personvern og informasjonssikkerhet* kan stille med deltakere på møte i ledergruppen på hver enhet, og tematikken og situasjonen for den konkrete enheten kan diskuteres på riktig nivå. Det fremstår som fornuftig å ha dette på agendaen i enhetenes ledermøter én gang i halvåret. Faggruppen deltok som nevnt på møte med alle enhetene der styret skulle behandle årsrapporten, og et slikt formøte vil være naturlig å ha hvert år.

Faggruppa har hittil ikke deltatt på noen ledermøter i Avdeling for bygg og eiendom, Avdeling for økonomi og organisasjon eller Avdeling for forskning, utdanning og formidling.

Informasjonssikkerhet bør være et fast tema på ULM-ALM, f.eks en gang i halvåret.

Samordning med sikkerhets- og beredskapsarbeidet forøvrig ved UiT

Det fremstår som fornuftig og nødvendig at beredskap innen informasjonssikkerhet knyttes enda nærmere til det øvrige beredskapsarbeidet ved UiT, slik at beredskapsarbeidet behandles helhetlig.

Det er tatt grep for å gjennomføre risikovurderinger på enhetsnivå sammen med beredskap våren 2021, og dette vil være et første steg for å klare å samordne arbeidet bedre.

I tildelingsbrevet for 2021 (18.12.20) [7] peker Kunnskapsdepartementet på at UiT må arbeide systematisk med sikkerhet og beredskap, og informasjonssikkerhet skal være en integrert del av dette arbeidet.

UH-sektoren

UiT er selvstendig ansvarlig for at informasjonssikkerhet og personvern ivaretas for vår virksomhet, men dette er likevel ikke et arbeid UiT gjør helt alene.

I 2018 ble *Unit - Direktoratet for IKT og fellestjenester i høyere utdanning og forskning* opprettet.

Unit har fått i oppgave å lede styringen av informasjonssikkerhet og personvern på sektornivå på vegne av Kunnskapsdepartementet, gjennom en styringsmodell i henhold til anerkjent standard. Unit gjennomfører årlige kartleggingsmøter med alle institusjonene, hvor disse skal besvare en rekke spørsmål om arbeidet med informasjonssikkerhet og personvern. Deretter

---

[7] https://www.regjeringen.no/contentassets/72751a723c654b029d7c04f67e171275/tildelingsbrev-2021-for-universitetet-i-tromso-norges-arktiske-universitet-.pdf, Pkt 4.2.2.

utarbeider Unit både en konkret tilbakemelding til den enkelte institusjon, samt en overordnet risiko-/tilstandsrapport for UH-sektoren.

Videre har Unit gitt UNINETT[8] ansvaret for cybersikkerhet for forskning og høyere utdanning. Dette innebærer blant annet har de har et responsmiljø for IKT-sikkerhetshendelser i UH-sektoren, og hvis de oppdager en hendelse som påvirker UiT vil vår CSIRT få beskjed. Gjennom datainnbruddet UiT ble utsatt for høsten 2020 har vi imidlertid erfart at vi også vil ha behov for ekstern støtte fra profesjonelle, private aktører. Selv om vi fikk god støtte fra UNINETT CERT under håndteringen av hendelsen fremstår det som aktuelt å innlede en dialog med Kunnskapsdepartementet om den sikkerhetssatsingen som skjer via Unit og UNINETT vil treffe så godt som ønskelig.

I tillegg er ett av fagutvalgene under Digitaliseringsstyret[9] i sektoren rettet mot informasjonssikkerhet og personvern[10]. Her har UiT en representant.

Videre er det en egen informasjonssikkerhetsgruppe innad i BOTT-samarbeidet, hvor fellesspørsmål og -utfordringer tas opp.

---

[8] UNINETT er et statlig infrastrukturselskap, og drifter blant annet forskningsnettet (nettforbindelsen UH-sektoren benytter), og er leverandør av en rekke fellesløsninger (bl.a. innloggingsløsningen FEIDE, trådløstilgang via Eduroam mv). Https://www.uninett.no.

[9] https://www.unit.no/mandat-digitaliseringsstyret-fra-2021

[10] https://www.unit.no/fagutvalg-informasjonssikkerhet-og-personvern

5 Avviksmeldinger

Løpenummer viser til intern oversikt holdt av Faggruppe for informasjonssikkerhet og personvern.

De mest alvorlige avvik i løpet av perioden			
Avvik #	**Hendelsesbeskrivelse**	**Tiltak**	**Ansvarlig:**
1	Undervisning ble tatt opp av eksterne uten forutgående klarering (det var klarert at de skulle delta, men ikke at de skulle ta opp). Studentene meldte fra om dette til instituttet.	Opptakene ble slettet.	Institutt for psykologi
Flere	Manglende skjerming i Ephorte medførte at opplysninger ble synlige, i enkelte saker på internett (via møteportalen eller offentlig journal)	Opplæring. Flere av sakene ble meldt til Datatilsynet.	Flere
Flere	Feil mottaker på utgående, elektronisk brev (eksempelvis arbeidskontrakt, svar på søknader). Typisk årsak er at mottaker er søkt opp på navn fremfor fødselsnummer, og det skjer en forveksling.	Gjennomgang av tiltak, herunder opplæring, for å sikre at saksbehandlerne søker opp mottaker ved hjelp av korrekt metode. Enkelte saker ble meldt til Datatilsynet	Flere
11	To forskjellige personer fikk samme brukernavn, og feil	Hendelsen avdekket en svakhet som gjorde det mulig for at dette kunne	ITA

	person kan dermed få tilgang til annens konto	skje igjen, og dette ble grundig fulgt opp av problemhåndteringsteamet på ITA.	
14	Alvorlig datainnbrudd på UiT	Se vedlegg.	ITA

5.1 Oppsummering avvik og risikoområder

Faggruppe for informasjonssikkerhet og personvern fikk melding om ca 14 avvik i 2020. Det er fremdeles svært sannsynlig at det eksisterer en betydelig underrapportering av avvik, og at dette skyldes manglende kompetanse og oppmerksomhet på hva som skal meldes som avvik. Faggruppa observerer at flere av de innmeldte avvikene ikke kommer som en «direkte» melding om informasjonssikkerhetsavvik, men via andre kanaler (f.eks via henvendelser til brukerstøtte om å stenge ned tilganger, melding om stjålet PC fordi bruker behøver ny etc). UiT er da avhengig av at de som mottar disse henvendelsene klarer å fange opp at dette også omhandler informasjonssikkerhet og at det deretter meldes videre. Dette gir forsinkelse i avviksbehandlingen, noe som kan være problematisk - både fordi håndtering av hendelsen kan være tidskritisk for å avverge videre konsekvenser, og fordi UiT har knappe frister dersom det er en hendelse som må meldes til Datatilsynet (uten ugrunnet opphold og innen 72 klokketimer).

I den årlige statusrapporten[11] fra enhetene trekker ett av fakultetene frem at de er bekymret for underrapportering av avvik, og viser til at det meldes for få avvik om brudd på informasjonssikkerheten. Manglende melding om avvik gir uttrykk for mangler ved meldingskulturen i organisasjonen til UiT ved at det f.eks. ikke eksisterer tilstrekkelig kunnskap eller oppmerksomhet hos de ansatte om hva som rent faktisk er et avvik. Denne tilbakemeldingen understøtter faggruppens oppfatning av temaet.

UiT har også en utfordring som må løses knyttet til manglende harmonisering av håndtering av avvik, både internt på Avdeling for IT og på øvrige enheter. Eksempelvis håndteres en

[11] Se kap. 6 nedenfor for nærmere informasjon om statusrapportene fra enhetene.

rekke sikkerhetsavvik via en annen linje internt på Avdeling for IT, da det omhandler forhold som faller inn under *«Kvalitetssystem for IT»*. Utenfor Avdeling for IT har eksempelvis Det helsevitenskapelige fakultet egne rutiner for helseforskning, som bl.a inneholder avvikshåndtering. Disse vil typisk også kunne ha problemstillinger knyttet opp mot personvern og/eller informasjonssikkerhet, og fakultetet har tatt initiativ til dialog for hvordan dette arbeidet kan harmoniseres slik at de rette instansene involveres samt at brukerne har kun en kanal å forholde seg til (for innmelding av avvik).

For å fullt ut lykkes med faktisk å få rapportert inn avvik i et mer reelt omfang fremstår det som nødvendig å samle og harmonisere meldeprosedyrene, på tvers av de felt og fagområder som avvikene knytter seg til (slik som HMS, forskning, informasjonssikkerhet og personvern mv). Dette fordi ett avvik kan omfatte flere felt, og det er etter hvert mange avvikssystem og prosedyrer å holde oversikt over for ansatte og studenter. Å få dette til uten å samtidig introduserer nye risikoer knyttet til avviksbehandlingen (f.eks at fortrolig informasjon blir kjent for en for stor gruppe personer) er imidlertid utfordrende, og det vil kreve at UiT tar en beslutning om at en slik samordning skal skje og setter av tilstrekkelig med ressurser til å få det til på en ordentlig måte[12].

Datatilsynet

Totalt fire avvik ble meldt til Datatilsynet i 2019, mot ett i 2019 og fire i 2018. Tre av sakene er ferdig behandlet av Datatilsynet, og UiT ble ikke ilagt noen sanksjoner i disse. Det har vært flere avvik som har involvert personopplysninger, men disse har ikke vært av en art som utløste meldeplikten. Alle avvik som involverer personopplysninger diskuteres med UiTs personvernombud, herunder om de er meldepliktige til Datatilsynet. Det har vært andre avvik som har involvert personopplysninger, men hvor vi har vurdert det slik at meldeplikten ikke inntrådte.

Oppsummering

Sikkerhetshendelsen (datainnbruddet) som ble oppdaget i desember 2020 utgjør naturligvis det største avviket og den største skaden fra 2020. Det er imidlertid andre, gjentagende problemstillinger som avdekkes gjennom avviksbehandlingen og som UiT må holde fokus på.

---

[12] Her vil det være naturlig å bygge videre på arbeidet bak https://uit.no/siifra, men etter vårt syn må målet være en felles innmeldingstjeneste for alle avvik – uavhengig av hendelsestype eller fagområde.

Ett av disse er knyttet til opplæring. Vi mener at for å lykkes må opplæring innen informasjonssikkerhet og personvern i stor grad integreres i annen opplæring, eksempelvis oppæring i bruken av en IT-tjeneste, den øvrige opplæringen en nyansatt får når vedkommende starter, undervisningen studentene mottar mv. Dette er betraktelig mer krevende å få til enn mer spesialisert opplæring som går direkte på informasjonssikkerhet og personvern isolert sett.

ITA registrerer også at det er prosesser og prosedyrer som enten har mangler, eller hvor prosedyrene er på plass, men ikke følges. Tilsvarende er påpekt i tidligere årsrapporter, og risikoen er fremdeles forholdsvis høy. Det er derfor nødvendig å gjenta ett av disse risikoområdene også i denne rapporten, grunnet utbredelsen og det store potensialet for skadelige hendelser hvis UiT ikke oppnår kontroll (se nærmere beskrivelse av «systeminnføring nedenfor»).

Dersom det er en underrapportering på informasjonssikkerhetsavvik så er det sannsynligvis i enda større grad en underrapportering på brudd på personvernregelverket. I tillegg til informasjonssikkerhetsavvik som involverer personopplysninger, kan avvik innen personvern eksempelvis være behandling av personopplysninger uten lovlig grunnlag, manglende databehandleravtaler, ulovlig gjenbruk av data UiT har innhentet til andre formål etc.

Systeminnføring

Innføringen av nye systemer og tjenester medfører nye risikoer, og det er viktig at vedtatte prosedyrer for systeminnføring følges lojalt. For rask innføring av systemer og/eller tjenester, uten at tilstrekkelig med ressurser er lagt til innføringsprosessen, medfører at UiT vil mangle tilstrekkelig oversikt og kontroll med mulighetene – og dermed risikoene – med det aktuelle systemet/tjenesten. Gjennom kvalitetssystemet for IT finnes det rutiner for dette, og fokus må settes på at disse skal følges. Videre bør kvalitetssystemet utvides slik at det ikke gjelder kun for IT-avdelingen, men for hele UiT. Det er uheldig at virksomheten ikke er samordnet på dette, og at enhetenes innføring og drift av sine egne IT-systemer ikke følger det samme kvalitetssystemet. Eksempelvis har Universitetsbiblioteket en rekke systemer og Det Helsevitenskapelige fakultet drifter og utvikler selv EUTRO (for befolkningsundersøkelsene slik som Tromsøundersøkelsen). Totalt sett gjør dette det vanskelig for UiT å ha en helhetlig kvalitetssikring av samtlige IT-systemer.

I sum kan det sies at det gjøres veldig mye bra arbeid, men at det fortsatt gjenstår et til dels betydelig arbeid for få på plass den nødvendige systematikk som gjør at UiT har tilstrekkelig oversikt og kontroll på virksomhetsnivå.

6 Årlig statusrapport fra enhetene

6.1 Innledning

I 2019 ble det innført en årlig statusrapport for informasjonssikkerhet som fakultetene og enhetene[13] skulle levere. I korte trekk innebærer dette at enhetene skal identifisere sine informasjonsverdier, vurdere trusler og tiltak, vurdere organiseringen av informasjonssikkerhetsarbeidet ved sin enhet samt orientere om status på risikovurderinger.

Bakgrunnen og målsetningen med rapporten kan på overordnet nivå forklares med at det er helt nødvendig å gjennomføre jevnlige kartlegginger og tilhørende vurderinger for å ha en tilstrekkelig oversikt og forståelse av UiTs informasjonsverdier. Uten dette er det i praksis ikke mulig å ta informerte avgjørelser rundt risikonivå, hvordan informasjonssikkerheten må ivaretas på enhetene mv.

Kunnskapsdepartementet nevner spesifikt i tildelingsbrevet for 2021 at «*UiT skal ha en oversikt over sine informasjonsverdier- og systemer*»[14]. Det er viktig at informasjonen i rapportene fra enhetene struktureres og analyseres på nivå 1 slik at UiT får størst mulig utbytte ut av disse kartleggingene, og kan svare ut det ansvaret departementet peker på at vi har.

Det mest omfattende arbeidet ble gjort ved første levering av rapporten i 2019, da tilsvarende ikke var gjennomført tidligere i denne skalaen. Ved leveringen av rapporten for 2020 har enhetene i all hovedsak oppdatert deres tidligere rapport, og tatt inn noen nye momenter basert på erfaringene de har fått siden.

En av utfordringene som ble påvist ved statusrapporten i 2019 var at det var manglende forståelse på de ulike enhetene om hva informasjonssikkerhet innebærer. En forholdsvis utbredt misforståelse var at flere var av den oppfatning at ansvaret lå hos Avdeling for IT (ITA). Dette er en holdning faggruppen mener er i ferd med å endres. Enhetene har i større

---

[13] Samtlige fakulteter, Norges arktiske universitetsmuseum og akademifag samt Universitetsbiblioteket er omfattet av denne rapporteringsordningen. Den vil bli utvidet til at alle enheter på nivå 1 skal levere tilsvarende rapport.

[14] https://www.regjeringen.no/contentassets/72751a723c654b029d7c04f67e171275/tildelingsbrev-2021-for-universitetet-i-tromso-norges-arktiske-universitet-.pdf, Pkt 4.2.2.

grad iverksatt arbeid med å selv få oversikt over egne informasjonsverdier og har en større oppmerksomhet rundt arbeidet med informasjonssikkerhet. Vi ser at enkelte fakultet, hvor 2019-rapporten var forholdsvis lite omfattende, har tatt grep og levert gode rapporter for 2020.

Ved utsendelsen av årets statusrapport ble det vurdert å gjøre endringer i strukturen til rapporten, men ettersom det er ønskelig å se trender over en periode er det hensiktsmessig å beholde nåværende struktur.

Nye problemstillinger i årets rapport er blant annet endringer i informasjonssikkerheten på grunn av endringene i arbeidshverdagen som skyldes koronapandemien.

6.2 Informasjonsverdier

Kartleggingen og resultatene utført i 2019 utgjør som nevnt i stor grad hovedinnholdet i rapporteringen for 2020. Det ble gjennom tilbakemeldingene for 2019 rapporteringen signalisert ønsket presisjonsnivå, samt forslag til metoder for bruk i kartlegging. For de enhetene som var for overordnet er detaljnivået justert til det bedre. For de fleste utgjør endringene for årets rapportering enkelte justeringer og tilføyinger. En særskilt utfordring er at enkelte informasjonsverdier endrer klassifisering over tid, og flere av fakultetene har inkludert informasjon om disse i årets rapportering[15]. Bevissthet rundt trusselaktører og deres metoder er økt, samt at tilføyde kommentarer på enkelte informasjonsverdier vitner om bredere forståelse for krav til sikkerhetsnivå.

6.3 Sammensatte organisatoriske problemstillinger

Flere av enhetene melder om problemstillinger som påvirker hele organisasjonen. Noen rapporterer at UiT som organisasjon har en utfordring når det gjelder mottak av fortrolig informasjon, enten det er informasjon vi aktivt har bedt om å motta eller er informasjon som ikke nødvendigvis skulle vært sendt til UiT. Et eksempel på dette er enkelte situasjoner hvor

[15] Eksempelvis eksamensoppgaver. Disse vil være fortrolige/røde før eksamen er gitt, men endrer seg til å være åpne/grønne etter at eksamen er gjennomført.

UiT avkrever innsender fortrolig informasjon, men deretter ikke alltid har tjenester og/eller rutiner for å tilstrekkelig ivareta informasjonssikkerheten i etterkant. Årsaken til dette kan blant annet være manglende kunnskap om digitale løsninger, eller utilstrekkelig kunnskap om prosedyrer for videre behandling av opplysningen (eksempelvis at enkelte typer opplysninger må arkiveres, mens andre skal slettes fortløpende). Et annet eksempel er tilfeller hvor det sendes mer informasjon enn enhetene har nytte av eller behov for, men hvor mottak av opplysningene er vanskelig å unngå. I slike tilfeller må informasjonen like fullt ivaretas slik at den ikke kommer på avveie, samt at den slettes med mindre det foreligger formelle hindre for dette.

Enhetene tar opp bekymringer knyttet til hvilke verktøy og systemer som er tilgjengelig for studenter og ansatte. Noen systemer som ivaretar konfidensialiteten til informasjonen, kan øke faren for at informasjonen går tapt ettersom den ikke ivaretar tilgjengeligheten like godt. Det kan føre til en risiko for studentenes progresjon, som igjen øker faren for at informasjonen lagres på privat utstyr. Et eksempel på dette er tilfeller hvor studentene må bruke kryptert minnepenn til å lagre informasjon når de f.eks. arbeider med røde/fortrolige data.

Et fakultet påpeker at en manglende oversikt over helhetsbildet er en risiko. Informasjonssikkerheten kan utfordres når verktøyene som benyttes ikke er dimensjonert for å brukes av alle som kan ha behov for dem, f.eks. ved at det ikke er kontoer i Tjeneste for sensitiv data (TSD) til alle studentene. Videre kan systemer som isolert sett fungerer bra i enkeltsituasjoner, være uegnet når det er store mengder studenter eller ansatte som skal benytte seg av dem. Dette er en problemstilling som blir adressert direkte til Avdeling for IT gjennom rapporteringen.

Informasjonssikkerheten blir ytterligere utfordret ved at enhetene har ansatte fra flere nasjoner, herunder land som kan anses å være såkalte «risikoland». Det er utfordringer ved ivaretagelsen av informasjonssikkerheten rundt forskningsprosesser, forskningsdata og ivaretagelsen av samarbeidspartnere – som gjennom sitt samarbeid med UiT kan bli mål for ulike trusselaktører. Se også omtale av dette temaet nedenfor i kap. 8

6.4 Ressurser

Ressursbruken på informasjonssikkerhet har økt for flere av fakultetene i 2020. Det rapporteres om omorganisering i teamstruktur, omdisponering av interne ressurser og formalisering av arbeidsoppgaver knyttet til informasjonssikkerhet. Rådgivere innen forskning og læringsfremende teknologi har fått ansvar for prosesser som styrker informasjonssikkerheten. Det har videre skjedd en styrking av arbeidet med risikovurderinger ved at oppgaven er tillagt personer som jobber direkte i miljø der risikovurderinger skal utføres. Flere fakulteter vil innlede samarbeid med *Faggruppe for informasjonssikkerhet og personvern,* og har dedikert bindeledd for oppgaven.

For 2021 skal det ved tilsettes personell som skal jobbe direkte med oppfølging/bistand i arbeidet med informasjonssikkerhet ved tre av fakultetene. Et fakultet etablerer en arbeidsgruppe underlagt fakultetsdirektøren som vil få ansvar for rapportering og rådgivning for informasjonssikkerhet.

Enkelte rapporter beskriver fortsatt en hverdag der ansvaret for arbeid med informasjonssikkerhet ikke er tydelig formalisert. Enkeltpersoner, grupper med ansatte eller ledelse holder i arbeidsoppgaver knyttet til informasjonssikkerhet der dette er basert på plassering i organisasjonen eller kompetansefelt. For et fakultet ble status fra 2019 videreført selv om de i 2019-rapporten opplyste at ressursdisponeringen og organiseringen innen informasjonssikkerhet var for svak.

I tilbakemeldingene til enhetene på 2019-rapporten var det påpekt at nærhet til informasjonsverdiene er viktig for presis rapportering. Det fremkommer av årets rapportering at avdelinger og institutt nå deltar i større grad i arbeidet med kartlegging og rapportering av informasjonsverdiene. På denne måten oppnås et bedre detaljnivå og tydeligere vurderinger av trusselnivå. Det er fortsatt slik at de enheter som ikke har tilstrekkelig bredde i arbeidet med rapporteringen blir for overordnet, noe som igjen gir et dårligere grunnlag for en reell vurdering av hvilke informasjonsverdier som skal beskyttes.

6.5 Kurs/opplæring

Flere av enhetene rapporterte i 2019 om behov for opplæring knyttet til informasjonssikkerhet. Det er i 2020 satt søkelys på kompetanseheving og gjennomført tilpasset opplæring innen både personvern og informasjonssikkerhet. Særlig har opplæring rettet mot forskning og studenter fått fokus, men også satsninger mot nytilsatte er gjennomført. Ett fakultet har utarbeidet eget opplæringsmateriell rettet mot forskning og studentforskning, og har her inkludert viktige element knyttet til informasjonssikkerhet. Et annet fakultet har innført digital informasjonsmappe som nytilsatte får før tiltredelse som et hjelpemiddel innen informasjonssikkerhet. Dette gjør at ansatte kan tilegne seg kompetanse før behandling av informasjon starter. UiT bør vurdere om dette er noe som kan løftes og gjøres mer allmenngyldig for alle nyansatte, på tvers av enhetene (med ev. lokale tilpasninger der nødvendig).

En direkte gevinst av statusrapporteringen er at kartlagte informasjonsverdier skal brukes til økt bevisstgjøring av ansatte både med hensyn til tilgang og behandling av informasjonsverdiene. Dette er kun mulig for de enhetene som ikke er for overordnet i sin rapportering.

6.6 Konklusjon

Gjennom andregangsrapportering begynner UiT å få en god oversikt over informasjonsverdiene på et detaljnivå som gjør at sikkerhetstiltakene kan styres mer direkte. Rapporteringen gir også et godt innblikk i hvordan enhetene gjennomfører arbeidet, og om de prioriterer de tiltakene som de har rapportert at de skulle satse på/gjennomføre i 2020. I årets rapport ses endringer som er bedre enn ved forrige rapport, men også enkelte endringer som ikke nødvendigvis er positive.

7 Korona/Covid-19

Gjennom den forholdsvis brå nedstengingen av campusene i mars 2020 grunnet korona måtte det en massiv omlegging til på kort tid. Ansatte skulle i stor grad arbeide hjemmefra, med de sikkerhets- og personvernutfordringer dette medførte. Undervisningen ble flyttet over til rene digitale flater, og det krevde en oppskalering av bruk av de verktøyene UiT allerede hadde samt anskaffelsen av noen nye (f.eks Zoom). Dette var bl.a for å sikre tilstrekkelig kapasitet når så mange skulle bruke tjenestene samtidig (her ble vi også påvirket av at de samme tjenesten brukes både i resten av UH-sektøren i Norge, men enkelte tjenester så brukes de i hele Europa og i flere sektorer, og disse fikk visse utfordringer med å levere stabilt).

Når ansatte flyttes ut av kontoret og sitt vante arbeidsmiljø introduseres det en rekke risikofaktorer som UiT måtte håndtere. Disse er ikke unike for situasjonen, og gjelder slikt sett hver gang noen har arbeidet hjemmefra tidligere. Imidlertid medførte den omfattende skalaen hjemmearbeid foregikk på en høyst reell økning av risiko. Eksempelvis sitter man på eget hjemmenettverk, hvor UiT ikke har noen kontroll på sikkerheten. Vi kan ikke kontrollere omgivelsene (hvordan oppbevares papirdokumenter, låses PCen når den ansatte forlater den, har de møter hvor familien kan overhøre det som sies etc). Videre er det enklere at rutiner enten ikke fungerer eller glipper når man i så stor grad sitter utenfor kontormiljøet og den vante måten å arbeide på. Dette kan skape åpninger og sårbarheter som angripere kan utnytte. Risikoen som følger denne utstrakte bruken av hjemmekontor som hele Norge (og verden forøvrig) hadde ble også påpekt av Nasjonal sikkerhetsmyndighet (NSM)[16].

Det ble derfor laget en del materiell inkludert enkelte «kjøreregler» som ansatte måtte huske på, og disse ble bekjentgjort både via UiTs «koronaside» og «Informasjonssikkerhet og personvern»[17].

En tilsvarende problemstilling er behandling av fortrolig informasjon, som normalt ville blitt utvekslet i fysiske møter, men som i 2020 har blitt flyttet til digitale plattformer.

I 2020 gikk fakultetene tidvis over til fulldigital undervisning, noe som medfører at undervisningen er såpass endret at det påvirket informasjonssikkerheten på flere nivåer.

---

[16] https://nsm.no/aktuelt/hjemmekontor-hva-bor-virksomheten-tenke-pa

[17] https://uit.no/om/informasjonssikkerhet#innhold_675202

Videre har enkelte typer undervisning et fortrolig innhold, og dette representerte en utfordring i og med at UiT ikke kontrollerte omgivelsene studentene befant seg i siden undervisningen foregikk digitalt.

Noen studenter og ansatte kom seg ikke inn i Norge pga. strenge restriksjoner i reise eller grensepasseringer, som igjen medvirket til at flere måtte logge seg på UiT sine systemer fra andre land enn Norge.

Vi ønsker i denne sammenheng å trekke frem som positivt at *Faggruppe for informasjonssikkerhet og personvern* fikk en rekke spørsmål og henvendelser fra ansatte som hadde spørsmål rundt hvordan informasjonssikkerheten skulle ivaretas. Dette mener vi er tegn på en økende bevissthet rundt temaet hos ansatte.

Den brå og omfattende omleggingen medførte også positive endringer i måten UiT arbeider på. Nødvendige endringer i rutiner, slik som overgang fra fysisk til digital håndtering av informasjon har skapt en sikrere måte å arbeide på. Det ble f.eks. i 2020 innført digitale bilag ved UiT, som for flere av enhetene har gitt en gevinst i økt informasjonssikkerhet gjennom hvordan bilag håndteres via den digitale arbeidsflyten.

En negativ følge av den omleggingen var imidlertid at planlagte aktiviteter innenfor informasjonssikkerhet ble noe forsinket (slik som risikovurdering av alle enhetene, oppfølging av enkelte tiltak i strategien), da ressursene tilknyttet informasjonssikkerhet måtte omdisponere tiden sin til å håndtere de umiddelbare følgene korona hadde på virksomheten.

8 Internasjonalisering

I strategi for informasjonssikkerhet står det at *«UiT er et breddeuniversitet som på grunn av beliggenhet og forskningsprofil kan være spesielt utsatt for trusler og angrep knyttet til informasjonssikkerhet. Aktivister, kriminelle og statlig etterretning forsøker å oppnå økonomisk vinning, politiske mål eller andre fordeler gjennom manipulasjon, sabotasje og spionasje.*

Internt ved UiT har vi en sikkerhetskultur som ikke sammenfaller med risikonivået. Uten å gjennomføre tilstrekkelige tiltak for å sikre UiTs informasjonsverdier vil sannsynligheten for et større sikkerhetsbrudd være uakseptabelt høy. Slike brudd kan medføre at legitimiteten og omdømmet til UiT svekkes.».

Sikkerhetshendelsen høsten 2020 aktualiserte dessverre disse vurderingene og konklusjonene, og viste at vi er et attraktivt mål for ressurssterke aktører. Det er en rekke tiltak som er gjennomført og som må gjennomføres for å håndtere sikkerhetshendelsen, og lukke de sårbarheter som muliggjorde den. Disse er omtalt i vedlegg 3 og 4.

Det er imidlertid viktig at UiT samtidig klarer å se det helhetlige trusselbildet, og blir bedre i stand til å kartlegge og håndterer de situasjonene hvor UiT potensielt er særlig utsatt for risiko grunnet vår plassering og virksomhet som breddeuniversitet.

Ett av disse knytter seg til internasjonalisering, som forskningssamarbeid med såkalte «høyrisikoland», og inn- og utreise fra disse landene. PST har pekt på dette i sine åpne trusselvurderinger[18], og i Dagens Næringsliv 31.12.2020[19] kritiserte PST UH-sektoren spesifikt for måten de fleste institusjoner tilnærmer seg samarbeid, utveksling mm med andre land, især såkalte «høyrisikoland».

---

[18] Sist for 2021: https://www.pst.no/alle-artikler/trusselvurderinger/nasjonal-trusselvurdering-2021/

[19] «PST hudfletter universitetene: «Fullstendig blåøyde og veldig, veldig naive»»: https://www.dn.no/magasinet/dokumentar/politiets-sikkerhetstjeneste/ntnu/tekna/pst-hudfletter-universitetene-fullstendig-blaoyde-og-veldig-veldig-naive/2-1-919171

I den åpne trusselvurderingen for 2021[20] peker PST på at *«[i] 2021 vil utenlandske etterretningstjenester bruke store ressurser på å bryte seg inn i norske datanettverk. De vil også forsøke å rekruttere kilder og agenter. Målet deres er å få tilgang til informasjon og å påvirke beslutningsprosesser. Russisk og kinesisk etterretningsaktivitet vil utgjøre den største trusselen».*

I tillegg til risikoen for datainnbrudd, kompromittering av IT-utstyr på reise, spionvirksomhet m.m. er det også en tilstedeværende risiko for at ansatte, studenter eller gjester på UiT blir en innsidetrussel, og enten tar grep for å skade UiT (lekke informasjon om sikkerhetstiltak, lekke eller utnytte upubliserte forskningsdata de kan få tak i m.v.) eller utnytter UiTs ressurser til å få overført teknologi eller kunnskap underlagt eksportkontroll til hjemlandet[21]. Her har det vært flere saker i UH-sektoren, blant annet på NTNU i begynnelsen av 2020[22].

Videre bør det også pekes på risikoen som medfølger at UiT kan tenkes å forvalte opplysninger om personer (f.eks studenter) som av ulike årsaker er interessante for etterretningsmyndighetene i eget land, og hvor brudd på informasjonssikkerheten kan medføre en direkte, personlig risiko for disse personene[23].

Det er behov for at UiT tar en mer systematisk og grunnleggende tilnærming til denne problematikken slik at nødvendig og viktig samarbeid innenfor forskning og utdanning kan opprettholdes på en så sikker måte som mulig. Disse problemstillingenr kan ikke løses ved rene tekniske tiltak alene, men krever i stor grad organisatoriske, fysiske og menneskelige tiltak. Det er totalt fire fakulteter som berører problemstillinger knyttet til internasjonalisering i statusrapporten fra høsten 2020. De er innom ulike momenter, men felles er at alle momentene i større eller mindre grad omfatter enten internasjonale studenter, ansatte eller besøkende.

---

[20] https://www.pst.no/alle-artikler/trusselvurderinger/nasjonal-trusselvurdering-2021/, "Statlig etterretningsvirksomhet», s. 5 i pdf-utgaven.

[21] https://www.pst.no/alle-artikler/trusselvurderinger/nasjonal-trusselvurdering-2021/, «Teknologi- og kunnskapsoverføring», s. 12 i pdf-utgaven.

[22] «To forskere siktet av PST og suspendert fra NTNU» (universitetsavisa.no)

[23] Mer om denne problemstillingen: https://www.pst.no/alle-artikler/trusselvurderinger/nasjonal-trusselvurdering-2021/, «Flyktningspionasje», s. 15 i pdf-utgaven.

Her har eksempelvis Nasjonal sikkerhetsmyndighet (NSM) veiledninger som vil være nyttige å ta utgangspunkt i, og tilpasse til en gjennomføring som passer UiTs virksomhet og særskilte forhold. Bl.a. har de en egen veiledning med «grunnprinsipper for personellsikkerhet» som skal bidra til å redusere risikoen for innsidervirksomhet, og de har også en rekke relevante temarapporter.

En slik gjennomgang vil være omfattende, og vil måtte inkludere flere enheter. Eksempelvis Avdeling for organisasjon og økonomi (ORGØK), Avdeling for forskning utdanning og formidling (FUF), Avdeling for IT (ITA) samt fakulteter med fagmiljøer som kan være ekstra utsatt.

Det er en særskilt utfordring å skape en bevisst sikkerhetskultur og aktsomhet tilknyttet disse spørsmålene uten å samtidig gi grobunn for unødvendig intern mistenksomhet og i verste fall dårlig adferd mot utenlandske ansatte, studenter og gjester. Arbeidet vil naturligvis også måtte få klarhet i rammene for *hva* UiT kan vektlegge, hva vi bør og må være oppmerksomme på og hvem vi eventuelt kan søke bistand fra.

Det er videre viktig at UiT har tilstrekkelig kompetanse og oppmerksomhet til å foreta selvstendige vurderinger og beslutninger også innenfor dette feltet. Det har historisk sett ikke alltid vært slik at sikkerhetsmyndigheter og akademia nødvendigvis har hatt sammenfallende prioriteringer og vurderinger. UiT bør være oppmerksomme på også dette aspektet slik at vi har en selvstendig tilnærming, selvsagt innenfor de formelle rammene[24] vi må forholde oss til.

På bakgrunn av det ovennevnte anses det som det nødvendig at dette arbeidet påbegynnes i 2021 og eksisterende retningslinjer, rutiner, prosedyrer mv samles, gjennomgås, revideres og kompletteres der et er behov. Dette for å sikre en saklig og proporsjonal tilnærming til problemstillingen for UiT.

[24] Slik som f.eks sikkerhetsloven o.l.

9 Status på risikovurderinger

Det gjennomføres risikovurderinger ved UiT, men fortsatt ikke i den grad de skal etter gjeldende lovverk og institusjonens egne retningslinjer.

De senere år har det blitt mer fokus på gjennomføring av risikovurdering, og det er en betydelig bedring i antallet som faktisk gjennomføres. Det er imidlertid fremdeles en lang vei å gå, og ved UiT forekommer det også eksempler på at risikovurderinger er gjennomført og tiltak vedtatt uten at de følges ikke opp. Det mangler tidvis gode planer for prioritering og gjennomføring av tiltakene, samt faktisk oppfølging av de planer som fins.

Ansvaret for gjennomføring er tydelig plassert på systemeiere, enhetsledere og prosjekteiere.

I 2020 ble det tatt grep for å lette arbeidet med risikovurderinger. Malverket ble oppdatert, og det ble laget en ordning for ansatte meldte inn hva de skulle risikovurdere og så fikk de tildelt et arbeidsområde i Teams samt tilgang til malverk og veiledninger. I tillegg blir disse ført inn i en samlet oversikt over risikovurderinger ved UiT.

Av de mer sentrale tiltak som gjenstår knyttet til risikovurderinger er å utarbeide såkalte «lettutgaver» av risikovurderinger, så prosjekter, prosesser mv som er forholdsvis ukompliserte og benytter f.eks IT-systemer som allerede er vurdert, lett kan kartlegge og vurdere eventuelle særskilte risikoer for eget prosjekt mv., fremfor å måtte gjennomføre en mer omfattende, ordinær risikovurdering. Dette vil særlig være til hjelp for mange forskningsprosjekter, nye utvidelser til eksisterende IT-systemer mv. Dette etterspørres av mange fagmiljøer, og *Faggruppe for informasjonssikkerhet og personvern* vil ha fokus på å få dette på plass da det fremstår som en klar forutsetning for å få gjennomført risikovurderinger i det omfang og med den kvalitet som er påkrevd i ulike situasjoner.

I «*Årsrapport UiT Norges arktiske universitet 2020»* inngår det en mer overordnet risikovurdering hvor også informasjonssikkerhet er inntatt under ett av temaene.

10 Status på risikohåndtering

UiT mangler i dag verktøy som gjør det praktisk mulig å se risikovurderinger i sammenheng, og på det viset får et overblikk av risikonivået til UiT som helhet. Det ble i 2020 nedsatt en arbeidsgruppe i regi av Unit for å anskaffe et verktøy for sektoren, som ledd i sikkerhetssatsningen. Hvis flere benytter samme verktøy vil dette også lette prosessen med å dele risikovurderinger på tvers av institusjoner, der hvor det er mulig og aktuelt.

Risikoer håndteres derfor fremdeles i stor grad isolert fra prosjekt til prosjekt, IT-system til IT-system, og dette er en risiko i seg selv[25].

[25] Eksempelvis dersom en rekke prosjekter har avdekket den samme sårbarheten, men anser den for å være akseptabel for sin egen del. Blir antallet som har denne høyt nok kan det utgjøre en samlet, uakseptabel risiko for universitetet.

11 Ressurs- og kompetansebehov

Det har over flere år vært for få ressurser tilknyttet informasjonssikkerhets- og personvernarbeidet, både på forvaltningssiden og den operative siden. Her ble det imidlertid en bedring fra 1.1.2020 når ny faggruppe for personvern og informasjonssikkerhet opprettes. Via intern omstilling på Avdeling for IT ble kapasiteten økt fem heltidsstillinger (tre med teknisk bakgrunn, inkludert sikkerhetssjef, og to jurister). Det er imidlertid påkrevd med økt ressursbruk på alle enhetene, for å kunne håndtere de problemstillingene og utfordringene som er på disse feltene.

Fakultetene/enhetene

Etter *ledelsessystemet for informasjonssikkerhet og personvern* er det enhetslederne som er ansvarlige for å ivareta informasjonssikkerheten i sin enhet. Dette innebærer å gjennomføre risikovurderinger, iverksette nødvendige tiltak, informere ansatte i egen enhet om de rutiner og retningslinjer som til enhver tid gjelder, m.m., jf kapittel fire i ledelsessystemet. Det er vår erfaring at enhetene ikke har satt av tilstrekkelig ressurser til dette arbeidet, og det er ikke god nok oppmerksomhet rundt dette arbeidet. Gjennom statusrapportene fra mange av enhetene ser vi imidlertid at det er noe bedring her, se nærmere omtale ovenfor i kap. 6.4.

Risikovurderinger må gjennomføres i et langt større antall enn i dag, og dette må skje der aktiviteten foregår. *Faggruppe for informasjonssikkerhet og personvern* vil utvikle og bekjentgjøre metoder, veiledninger og råd, men selve risikovurderingen er ikke en aktivitet som kan gjøres på vegne av enhetene. Dette skyldes ikke bare kapasitetshensyn, men også fordi en del avgjørelser knyttet til informasjonseierskap, risiko mv ligger til enhetsleder (innenfor de rammer Universitetetsstyret har satt for akseptabel risiko).

Ut fra det *Faggruppe for informasjonssikkerhet og personvern* får tilbakemelding om fra enhetene, samt opplever av henvendelser, kan det slås fast at det er et stort behov for informasjon og kompetanseløft rundt informasjonssikkerhet i hele organisasjonen. UiT er her helt avhengige av at ledelseslinjen involveres og får en god forståelse av hva dette innebærer slik at de kan bringe det videre til sin enhet.

12 Revisjon av ledelsessystemet

Universitetsstyret vedtok den 16.12.2020 å utvide ledelsessystemet til å omfatte både informasjonssikkerhet og personvern. I samme sak ble det vedtatt nødvendige endringer i ledelsessystemets *styrende del*, bortsett fra mål og strategi. I 2021 må ledelsessystemets *gjennomførende* og *kontrollerende* del revideres slik at personvern integreres. Det må også utarbeides en ny strategi da den nåværende utløper etter 2021, og denne må inkludere personvern utover teamet sikkerhet for personopplysninger.

13 Vedlegg

(Nummereringen av vedleggene er styrt av, og fremkommer også av, saksfremlegget til Universitetsstyret.)

- Orientering om datainnbruddet/sikkerhetshendelsen høsten 2020 (vedlegg 2)
- Status på gjennomførte tiltak – oppfølging av sikkerhetshendelsen 2020 (vedlegg 3)
- Fremtidige tiltak – oppfølging av sikkerhetshendelsen 2020 (vedlegg 4)
- VDI – informasjon til styret (vedlegg 5)
- Personvernombudets årsrapport 2020 (vedlegg 6)