UiT

NORGES ARKTISKE UNIVERSITET

Årsrapport 2018

Avdeling for IT
19.2.2019

Innhold

Det følger av Styringssystemet for informasjonssikkerhet, pkt 6.3, at det skal utarbeides en årsrapport som gjennomgår arbeidet med informasjonssikkerhet («ledelsens gjennomgang»). Rapporten har vært utarbeidet én gang tidligere, for 2017.

Årsrapportens utforming er basert på mal fra Sekretariatet for informasjonssikkerhet for UH-sektoren (uninett.no/infosikkerhet/styringssystemer), og følger samme oppsett som tidligere rapport.

Informasjonssikkerhetsrådgiverne har vært sterkt involvert i arbeidet med GDPR-prosjektet ved UiT, også på spørsmål utenfor informasjonssikkerhetsfeltet (andre områder innenfor personvern). Sommeren 2018 ble antall rådgivere redusert fra to til én, da den ene rådgiveren sa opp sin stilling. En del planlagt arbeid innenfor informasjonssikkerhet har derfor måtte vente, og dette medfører at momenter som var påpekt i forrige rapport igjen blir fremhevet i denne.

Om personvern og informasjonssikkerhet

Ofte blir personvern og informasjonssikkerhet omtalt som om det går ut på det samme, og vi finner derfor grunn til å foreta en kort, innledende avklaring.

Informasjonssikkerhet (ivaretagelse av informasjonens konfidensialitet, integritet og tilgjengelighet) 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, 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.

Denne rapporten omhandler kun UiTs arbeid med *informasjonssikkerhet.*

1. Status på tiltak fra foregående årsrapport

Følgende ble pekt på i forrige rapport:

- **Behov for ny informasjonssikkerhetsstrategi**

Dette arbeidet har pågått høsten 2018, og ny informasjonssikkerhetsstrategi (2019-2021) skal fremmes Universitetsstyret i løpet av våren 2019.

- **Kriterier for akseptabel risiko anbefales gjennomgått**

Disse er tatt inn i arbeidet med ny informasjonssikkerhetsstrategi (2019-2021).

- **Gjennomgang av sikkerhetsorganiseringen**

Arbeidet med dette er satt på vent til ny strategi er vedtatt.

- **Revisjon av styringssystemet**

Arbeidet er i gang, men revidering av de enkelte deler må tas fortløpende. Slik det er nå anbefales det ikke å kjøre et prosjekt med full revisjon av hele styringssystemet for så å vedta en samlet «pakke».

2. Sikkerhetsmål og strategi

Som påpekt i årsrapporten for 2017 er det behov for en ny informasjonssikkerhetsstrategi. Dette arbeidet ble igangsatt høsten 2018, og konsulentselskapet Gartner har tilrettelagt og bistått i arbeidet. Den nye strategien vil gjelde for perioden 2019-2021.

3. Kriterier for akseptabel risiko

Det fins enkelte kriterier for akseptabel risiko, vedtatt av Universitetsstyret våren 2015 da styringssystemet ble vedtatt. Vi ser at disse bør gjennomgås, og punktet bør revideres. I dag er kriteriene angitt på et svært overordnet nivå. Selv om disse kriteriene ikke kan bli for detaljerte, bør de revideres slik at de blir lettere tilgjengelig når enhetsleder, systemeier, prosjektleder mv skal gjennomføre risikovurderinger og avgjør hva som er akseptabel risiko i det aktuelle tilfellet.

Arbeidet med dette er tatt inn i prosjektet som utarbeider ny informasjonssikkerhetsstrategi.

4. Sikkerhetsorganisering

Gjennom styringssystemet er sikkerhetsorganiseringen fastsatt (kap. 3). Nedenfor gjengis enkelte av de rollene som er del av sikkerhetsorganiseringen.

Universitetsdirektør har ansvar for informasjonssikkerhet på et overordnet nivå, herunder å sette av tilstrekkelig med ressurser til arbeidet med informasjonssikkerhet.

IT-direktør er informasjonssikkerhetsansvarlig. IT-direktøren har forvaltningsansvaret for informasjonssikkerhet, og er gitt instruksjonsmyndighet overfor alle enheter ved UiT i saker som angår informasjonssikkerhet.

Informasjonssikkerhetsrådgiverne utøver IT-direktørens myndighet. Dette var tidligere to stillinger; IT-sikkerhetssjef samt jurist. Per årsskiftet er det kun én stilling (jurist), men det er ansatt en ny informasjonssikkerhetsrådgiver som skal tiltre i februar 2019.

Videre har CSIRT[1] rollen for å håndtere IT-hendelser mens de skjer.

Enhetsledere[2] er ansvarlig for å tilfredsstille krav til informasjonssikkerhet i egen enhet, herunder blant annet å gjennomføre risikovurderinger og iverksette nødvendige tiltak.

Vi ser at det er behov for gjennomgang av deler av sikkerhetsorganiseringen. Situasjonen er tilnærmet uendret fra rapporten for 2017, så flere av de samme betraktningene er tatt inn nedenfor.

- **CSIRT:** Avdelingen har ikke tilstrekkelig fokus på den operative rollen til CSIRT. Pt. har UiT ikke et tilstrekkelig godt fungerende responsteam for IT-sikkerhetshendelser.

- **Forholdet mellom styringssystemet for informasjonssikkerhet ved UiT og kvalitetssystemet ved Avdeling for IT (ITA):** I dag er det en stor grad av overlapp mellom styringssystemet og kvalitetssystemet, spesielt når det gjelder avviksbehandling. Dette er uheldig da det blir uklarhet hva avviksrutinene skal være, vi får ikke utnyttet ressursene optimalt og vi risikerer dobbeltbehandling og uklar kommunikasjon.

  Kvalitetssystemet gjelder kun ITA, mens styringssystemet gjelder hele UiT. Vi kan ikke få en situasjon der visse typer avvik skal meldes på en måte hvis de skjer innad på ITA, og på en annen måte hvis det skjer på en annen enhet.

  Dette medfører at informasjonssikkerhetslinja ikke får full oversikt over informasjonssikkerhetsavvik som oppstår på ITA, eksempelvis knyttet til kryptovirus, tyveri av PC, passord på avveie, misbruk av systemer mv. Dette gjør også at denne rapporten ikke viser det fulle bildet. I 2018 er det tatt noen grep for å bedre kommunikasjonen her, men dette må ha fokus også i 2019.

- **Forholdet mellom operativ rolle og forvaltningsrollen:** Frem til sommeren 2018 hadde IT-sikkerhetssjef både det operative ansvaret og en stor rolle inn i forvaltningsoppgavene rundt informasjonssikkerhet, noe som var et for stort omfang for én person. Det operative og forvaltningsarbeidet må skilles mer enn hva var tilfellet før. Imidlertid er det slik at personen som innehadde stillingen forlot UiT sommeren 2018, og det har ikke kommet inn en ny person i tilsvarende stilling. UiT har store utfordringer i det operative arbeidet, og dette må få fokus og ressurser i 2019.

  Det må være faste møtepunkter mellom forvaltning og de operative leddene, så selv om de skilles mer enn i dag skal det fremdeles være et løpende samarbeid og dialog.

- **Fokus hos ledelsen:** Informasjonssikkerhet har i dag for lite fokus hos ledelsen ved UiT, og bør jevnlig være tema i møter mellom informasjonssikkerhetsansvarlig (IT-direktør) og universitets toppledelse. Også ledelseslinjen forøvrig må involveres i sterkere grad enn i dag. Betydningen av at toppledelsen har fokus på informasjonssikkerhet har blitt understreket av Kunnskapsdepartementet, sist gjennom eget brev til UH-sektoren.
    - Informasjonssikkerhet bør være et fast tema på utvidet ledermøte (ULM) og administrativt ledermøte (ALM), f.eks en gang i halvåret.

[1] Computer Security Incident Response Team (CSIRT)

[2] Definert i styringssystemet som dekaner, avdelingsdirektører, museumsdirektør og biblioteksdirektør

- Universitetsstyret bør informeres om informasjonssikkerhetsarbeidet jevnlig, slik at styret får et eierskap til temaet og problemstillingene. F.eks via en muntlig orientering fra informasjonssikkerhetsansvarlig en gang i halvåret.
- Informasjonssikkerhet bør være en fast sak på ledermøtene i ITA.
- De ulike enhetene bør regelmessig ha informasjonssikkerhet oppe på sine leder-/styremøter. Her kan informasjonssikkerhetsrådgiver med fordel inviteres inn.

- **Informasjonssikkerhetsforum:** Iflg. Styringssystemet skal det opprettes et informasjonssikkerhetsforum, som skal ledes av informasjonssikkerhetsrådgiver. Dette forumet har foreløpig ikke blitt startet opp, men dette vil skje i løpet av første halvår i 2019.

- **Personvernombudet:** Høsten 2018 ansatte UiT personvernombud, og reglement, retningslinjer mv må oppdateres i løpet av 2019 slik at ombudets rolle kommer klart frem.

UH-sektoren

UiT er ansvarlig for at informasjonssikkerheten ivaretas for vår informasjon, men dette er likevel ikke et arbeid vi 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. Dette gjøres på vegne av Kunnskapsdepartementet. Det vil bli etablert en styringsmodell i henhold til en anerkjent standard (ISO 27014). I 2019 vil Unit gjennomføre møter med alle institusjonene i UH-sektoren for å informere nærmere om styringsmodellen som nå innføres innenfor informasjonssikkerhet. I etableringen av styringsmodellen kartlegge hvilket behov som finnes i sektoren for veiledning og praktisk bistand, og hvordan denne best kan gis i fremtiden.

Unit har gitt UNINETT[3] 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.

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

[3] 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.

5. Avviksmeldinger

Løpenummer viser til intern oversikt holdt av informasjonssikkerhetsrådgiverne.

De mest alvorlige avvik i løpet av perioden			
Avvik #	**Hendelsesbeskrivelse**	**Tiltak**	**Ansvarlig:**
2	Feil i dataoverføring fra gammelt brukerhåndteringssystem til nytt. Dette medførte gjenbruk av brukernavn, som konkret innebærer at nye brukere fikk tildelt brukernavn som tidligere hadde vært i bruk (men hvor kontoen var deaktivert da bruker hadde sluttet). Det var ikke slik at aktive brukernavn (nåværende brukere) ble gjenbrukt og tildelt nye brukere. Konsekvensene av dette kunne blitt svært store da mange av UiTs systemer benytter brukernavn for å identifisere hvem brukeren er (i motsetning til å knytte dette opp mot f.eks fødselsnummer). I korte trekk medfører det at den nye brukeren i praksis kunne fått tilgang til den forrige brukers informasjon i de aktuelle tjenestene (e-post, filer mv). Dette skjedde ikke da feilen ble oppdaget tidlig før de nye brukerne hadde fått aktivert sine kontoer. Det var registrert to påloggінger før saken ble oppdaget, det ene var av den tidligere kontoeier (dvs den som filene mv tilhørte) og for den andres del var alle filer, eposter mv allerede slettet ihh til eksisterende rutiner. Det var ingen brukere som fikk sine eposter, filer mv på avveie denne gang, men det er ingen tvil om at dette kunne skjedd. Dette var derfor et svært alvorlig avvik.	Avviksrapporten som ble levert har foreslått en rekke tiltak. Disse går både på å forhindre at slikt kan skje, samt tiltak for å begrense konsekvensen dersom dette eller lignende hendelser oppstår i fremtiden. Disse inkluderer forbedringer i testregimet, samt mekanismer og kontrollrutiner som sikrer at det faktisk foretas sletting av innhold tilknyttet deaktiverte brukerkontoer.	ITA
4	Gjennom plagiatkontrollen URKUND kunne studenter får tilgang til medstudenters besvarelser, men	Det ble lagt på FEIDE-pålogging i Urkund. Senere ble også	ITA

	ikke treffprosent på tekstlikhet o.l. Medstudentene kunne identifiseres hvis de hadde skrevet f.eks navnet i filnavnet eller i besvarelsen. Studentene kom inn i Urkund gjennom Canvas.	tilgangslinken fra Canvas til Urkund (for studentene) fjernet. Meldt Datatilsynet.	
5	Student hadde fortrolig samtale med foreleser etter at forelesningen var over. Automatisk opptak av forelesningen var fremdeles aktivt, og opptaket ble gjort tilgjengelig for medstudenter. Avviksbehandlingen avdekket også svakheter med Studentappen, og måten den henter video ut av Mediasite (plattform for video) på.	Opptaket ble satt til privat med en gang UiT fikk beskjed om saken fra studenten. Feil i studentappen gjorde at tilgang til videoen via appen fremdeles var aktiv, og denne tilgangen ble stengt dagen etter. Nye lamper, informasjonsplakater, retningslinjer og informasjonsskriv lages. ROS-vurdering av studentappen gjennomføres. Meldt Datatilsynet.	HELSEFAK og ITA
6	Avviksmelding fra daglig leder EUTRO. Bekymring rundt behandling av avidentifiserte data.	Under behandling. Prosjekt igangsatt for å se på mulighet for å håndtere forskningsdata i sikre skytjenester.	HELSEFAK/ITA
8	Enkelte Powerpoint-presentasjoner fra forelesninger var konvertert til PDF og lagt ut til studentene (via Fronter). Disse presentasjonene inneholdt bilder av netthinner fra pasienter på UNN, og var i utgangspunktet anonyme. Imidlertid var ikke metadata fjernet, så ved å holde musepilen over bildene ble navn og fødselsnummer synlig for enkelte av pasientene.	Filer slettet. Logger over hvor mange som faktisk har åpnet filene kunne ikke hentes da PP-filen var slettet (og dermed også logger i Fronter) før avviksmeldingen var sendt inn og vi kunne sikre informasjonen. Meldt Datatilsynet og UNN.	HELSEFAK

11	Faglærer satte opp egen løsning for innlevering av arbeidskrav (multiple choice) og offentliggjøring av resultater. Dette gjaldt noen emner. Resultatsiden tilgjengelig for alle med linken, og viste alle studenters score på obligatoriske arbeidskrav.	Beskjed sendt til fakultetet om at løsningen måtte tas ned. Dette skjedde umiddelbart. Bedre sikring av opplysningene gjennomføres før løsningen settes opp igjen. Meldt Datatilsynet.	NT-FAK
Flere	Tilfeller hvor utstyr/enheter med konfidensielt innhold blir frastjålet brukeren, slik som minnepinner og datamaskiner. I de tilfellene vi har fått rapportert i 2018 har enhetene vært kryptert, slik at informasjonen har ikke kommet på avveie. Imidlertid var det tilfeller hvor informasjon kun var lagret på disse enhetene, og denne informasjonen gikk derfor tapt.	Ingen særskilte i de aktuelle tilfelle.	Flere

5.1. Oppsummering avvik

Vi fikk meldt inn 15 avvik i 2018, herunder de 6+ som er nevnt ovenfor. Vi holder det som 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. Vi ser at de fleste avvikene vi får meldt 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). Vi er da avhengig av at de som mottar disse henvendelsene klarer å fange opp at dette også omhandler informasjonssikkerhet og deretter meldes det videre. Imidlertid fører dette til en forsinkelse i avviksbehandlingen, noe som kan være problematisk. Både fordi hendelsen kan være tidskritisk for å avverge videre konsekvenser, og fordi vi har en tidsfrist dersom det er en hendelse som må meldes til Datatilsynet (uten ugrunnet opphold og innen 72 timer).

Totalt fire avvik ble meldt til Datatilsynet i 2018, og de var av følgende karakter:

- Ett var noe alvorlig (navn og fødselsnummer på noen pasienter fra UNN fremkom), men omhandlet informasjon som aldri skulle kommet inn i UiTs systemer og hvor vi vanskelig kunne avdekket det på forhånd. I tillegg til Datatilsynet ble UNN varslet.
- To av avvikene var av mindre alvorlighetsgrad, men tilstrekkelige til at de måtte meldes tilsynet
- Ett var alvorlig.

Alle avvikene er ferdigbehandlet hos Datatilsynet, og UiT er ikke ilagt sanksjoner.

Basert på erfaringene med de avvikene som ble meldt har vi følgende oppsummering av risikoområder og årsaker til at avvik kan oppstå. Dette er tilsvarende som var påpekt i rapporten for 2017.

Bruk av video

Video brukes i økende grad, være seg opptak av forelesninger, konferanser, veiledning, eksterne sesjoner, utdanning, forskning etc.

Avhengig av tematikken er det svært lett å trå galt i bruk av video, f.eks med tanke på hva som kommer med på videoen. Hvis man ikke har tenkt nøye gjennom hvordan video brukes som metode, hvilke verktøy som benyttes og hvordan videoen oppbevares og eventuelt tilgjengeliggjøres, så kan skadepotensialet være stort. Hvis temaet er av sensitiv art for den som er med på videoen, kan mediet oppleves som langt mer inngripende og krenkende enn f.eks en tekstlig gjengivelse av samme sak.

Det arbeides med å få bedre retningslinjer og rutiner på plass i forbindelse med bestilling av videoopptak. Dette inkluderer blant annet å sikre at god nok informasjon blir gitt til de som blir tatt opp på video; spesielt i forbindelse med konferanseinnlegg, opptak av foredrag etc. I tillegg må det klargjøres ytterligere at eierskapet til videoopptakene ligger hos enhetene, og plikten til å sikre at opptaket oppfyller pliktene våre etter personopplysningsloven ligger der (især de pliktene som ikke er del av informasjonssikkerhetsarbeidet, slik som lovlig grunnlag, informasjon, ivaretagelse av rettigheter mm). Avdeling for IT arbeider med å få på plass en del rammer og veiledning, men kan ikke ta de konkrete vurderingene på vegne av enhetene.

Her må det derfor skapes mer oppmerksomhet rundt hva som kreves, og enhetene må ha personer som kan ta disse vurderingene fortløpende og nokså effektivt. Ellers blir bruk av video uforholdsmessig risikabelt og krevende for UiT.

Av tiltak som er gjennomført i 2018 kan det nevnes her at vi har montert skilt inne i samt utenfor rom med automatisk opptaksutstyr. Disse har teksten «recording» og lyser rødt når opptak pågår. Tidligere var det en lampe som lyste rødt inne i rommet under opptak. Det er videre montert skjermer fremme på podiene, som viser kamerautsnittet. Dette både for å la foreleser vite hva kameraet filmer (og at bildeutsnittet er korrekt), men vil også fungere som en påminnelse om at kameraet er aktivt.

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. Det finnes rutiner for dette, og fokus må settes på at disse skal følges. Arbeidet Avdeling for IT har igangsatt i 2018 (DigU) vil kunne bidra både til forbedring av disse rutinene, samt fokus på at de skal følges. De systemer og tjenester som anskaffes direkte ute på de øvrige enhetene (f.eks gjennom et forskningsprosjekt) har vi dårlig oversikt over. Høsten 2018 ble enhetene spurt om dette, og 50 % svarte at de hadde noen få egne, tekniske løsninger. 50 % svarte at de ikke hadde noen. Alle som svarte at de hadde egne, tekniske løsninger oppga at de har gjennomført risikovurdering før løsningen ble tatt i bruk. Vi kan imidlertid ikke se at resultatene fra disse risikovurderingene er meldt til informasjonssikkerhetsrådgiver, ihh til Styringssystemet for informasjonssikkerhet kap. 3 (enhetsleders ansvar).

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

6. Status på risikovurderinger

Risikovurderinger gjennomføres ikke i den grad de skal etter gjeldende lovverk. Gjennom 2018 har informasjonssikkerhetsrådgiverne satt mer fokus på risikovurderinger ved UiT, og har aktivt etterlyst disse, spesielt ved systeminnføringer, samt har bidratt til å få disse igangsatt og gjennomført.

Vi ser at det er mer fokus på gjennomføring av risikovurdering, og det er en bedring i antallet som faktisk gjennomføres. Det er imidlertid en lang vei å gå, og vi har også sett eksempler på at risikovurderinger er gjennomført, tiltak vedtatt, men de følges ikke opp. Det mangler gode planer for prioritering og gjennomføring av tiltakene, samt faktisk oppfølging av de planene som fins.

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

I 2018 har det vært mindre fokus på aktiv deltakelse i risikovurderinger fra informasjonssikkerhetsrådgivernes side, av kapasitets- og hensiktsmessighetshensyn. Fokus er dreid over på rådgivning og utarbeidelse av materiell, veiledninger, maler etc., og dette vil fortsette i 2019. Det er avgjørende at enhetene får bedre kompetanse på dette, slik at f.eks forskningsprosjekter får den nødvendige bistand til å gjennomføre risikovurderinger og det ikke oppstår forsinkelser og/eller lovbrudd.

7. Status på risikohåndtering

Det er behov for å utarbeide rutiner og anskaffe systemstøtte for å ha muligheten til å se risikovurderinger i sammenheng, og få et overblikk over risikonivået til UiT som helhet. Dette er en svært krevende oppgave, og vil kreve mye ressurser å få til. Det er helt nødvendig å få gjennomført dette, ellers vil tiltak og vurderinger bli for «lokale» og UiT som institusjon vil ikke klare å sette inn ressurser på korrekt sted. Forutsetninger for å få dette til er en forholdsvis detaljert oversikt over UiTs informasjonsverdier[4], med tilhørende klassifisering av kritikalitet og verdi. Videre brukes i dag Excel som verktøy for å gjennomføre risikovurderinger, og det vil kreves et bedre verktøy for å få en helhetlig oversikt for UiT.

8. Ressurs- og kompetansebehov

Vi mener det er for få ressurser tilknyttet informasjonssikkerhetsarbeidet, både på forvaltningssiden og den operative siden.

De erfaringer vi har gjort oss de siste to årene viser at kapasiteten til å besvare henvendelser, drive veiledning og opplæring, utføre operativt arbeid samt utvikle regelverk, materiell og rammeverk, er for lav.

Dette er også noe som støttes klart opp av de vurderinger og anbefalinger Gartner har gjennomført, både gjennom modenhetskartlegging innenfor informasjonssikkerhet (sommeren 2018) og videre arbeid med informasjonssikkerhetsstrategien.

Høsten 2018 ble det igangsatt et arbeid med å utarbeide en ny informasjonssikkerhetsstrategi, for perioden 2019-2021. Denne leveres Universitetsstyret til behandling våren 2019. Her pekes det også på at det foreligger for få ressurser til dette arbeidet, og informasjonssikkerhetskompetansen på UiT jevnt over er altfor lav.

Fakultetene/enhetene

Etter Styringssystemet for informasjonssikkerhet 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 til gjelder, m.m., jf kapittel tre i Styringssystemet. 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. Risikovurderinger må gjennomføres i et langt større antall enn i dag, og dette må skje der aktiviteten foregår. Informasjonssikkerhetsfunksjonen ved Avdeling for IT kan utvikle og bekjentgjøre metoder, veiledninger og råd, men dette 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 Universitetet har satt).

I HMS-undersøkelsen høsten 2018 (HMS årsrapport) fikk informasjonssikkerhet mulighet til å ta med noen spørsmål. Her svarte 70 % av fakultetene/enhetene at de i stor grad er kjent med styringssystemet for informasjonssikkerhet, og 80 % svarte at de i stor grad er kjent med det ansvaret som er tillagt enhetslederne.

[4] Informasjonsverdi er et samlebegrep som inkluderer både informasjon og tilhørende støtteverdier som IKT-system, digitale tjenester, datautstyr av ulike varianter mv.

På spørsmål om fakultetet/enhetene opplever å ha de verktøy og informasjon som behøves for å oppfylle dette ansvaret, svarte 70 % «delvis» og 30 % «ja». Samtidig svarte 50 % av fakultetene/enhetene at de er usikre på hva som vil innebære et brudd på informasjonssikkerheten.

Ut fra det vi får tilbakemelding om fra enhetene, og opplever av henvendelser, vil vi si at det er et stort behov for informasjon og kompetanseløft rundt informasjonssikkerhet i hele UiT. Blant annet får vi nokså ofte tilbakemelding om at informasjonssikkerhet er en «IT-sak», og at brukeren anser dette som noe Avdeling for IT håndterer og som de ikke har så mye med/er så relevant for dem. Dette gjelder også personer i ulike ledelsesstillinger. Det er en nødvendighet å avkrefte denne myten, ellers vil ikke arbeidet med informasjonssikkerhet lykkes. Vi er her helt avhengige av at ledelseslinjen på UiT involveres, og får en god forståelse av hva dette innebærer og kan bringe det videre til sin enhet.

9. Revisjon av styringssystemet

Gjennom arbeidet med å implementere styringssystemet ser vi at dette må revideres og bygges ut. Det er for overordnet, og vanskelig å anvende i praksis for de ansatte på UiT. Disse endringene tas delvis gjennom GDPR-prosjektet, men må også håndteres utenom og i et litt mer langvarig løp.