



Årsrapport informasjonssikkerhet 2019

Avdeling for IT, 5.3.2020

A large, light pink gear icon with a curved arrow around it, symbolizing information security.

Informasjons-
sikkerhet

- Konfidensialitet
- Integritet
- Tilgjengelighet

Innhold

1. Status på tiltak fra foregående årsrapport	3
2. Status på tiltak i informasjonssikkerhetsstrategien	3
3. Sikkerhetsmål og strategi	6
4. Kriterier for akseptabel risiko	6
5. Sikkerhetsorganisering	6
6. Avviksmeldinger	10
6.1. Oppsummering avvik og risikoområder	12
7. Årlig statusrapport fra enhetene	15
8. Status på risikovurderinger	18
9. Status på risikohåndtering	19
10. Ressurs- og kompetansebehov	19
11. Revisjon av ledelsessystemet	20
12. Vedlegg	21

Det følger av Ledelsessystemet for informasjonssikkerhet¹ («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.

Informasjonssikkerheten skal ivaretas informasjonens

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

¹ Se <https://uit.no/sikkerhet>

Om personvern og informasjonssikkerhet

Ofte blir personvern og informasjonssikkerhet 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 bygghdata, 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.

Siden 2015 har IT-direktør hatt forvaltningsansvaret for informasjonssikkerhet, og ble sommeren 2019 tillagt tilsvarende ansvar for personvern forøvrig. I og med at det overordnede forvaltningsansvaret nå er samlet ser Universitetsdirektøren behovet for å bygge ut ledelsessystemet for informasjonssikkerhet til å også omfatte personvern, slik at det blir en naturlig, indre sammenheng. Dette er imidlertid et større arbeid, som er planlagt påstartet i 2020.

Når dette er gjennomført vil denne årsrapporten omhandle både informasjonssikkerhet og personvern, men for 2019 omhandler den altså fremdeles kun UiTs arbeid med *informasjonssikkerhet*.

1. Status på tiltak fra foregående årsrapport

Følgende ble pekt på i foregående rapporter:

- **Behov for ny informasjonssikkerhetsstrategi**

Ny informasjonssikkerhetsstrategi (2019-2021) ble vedtatt av Universitetsstyret våren 2019. Her inngår det en rekke tiltak som skal gjennomføres i denne treårsperioden.

- **Kriterier for akseptabel risiko anbefales gjennomgått**

Disse kriteriene ble gjennomgått og revidert i forbindelse med ny strategi.

- **Gjennomgang av sikkerhetsorganiseringen**

Ett av tiltakene i strategien er oppbygning av en sterkere sikkerhetsorganisasjon. Dette er igangsatt og blir nærmere omtalt nedenfor i pkt 5.

- **Revisjon av ledelsessystemet**

Dette er et arbeid som vil pågå gjennom hele strategiperioden. I 2019 ble strukturen for ledelsessystemet justert, navnet endret² samt at ny strategi, sikkerhetsmål og kriterier for akseptabel risiko ble vedtatt i tillegg til nye retningslinjer for klassifisering av informasjon.

2. Status på tiltak i informasjonssikkerhetsstrategien

Det følger en rekke konkrete, men omfattende tiltak av informasjonssikkerhetsstrategien. Disse er lagt inn i en periodisert handlingsplan og skal bidra til at UiT når målbildet i strategien, se vedlegg 3.

Nedenfor vil det bli knyttet en kort kommentar på status for de tiltak som etter strategien har oppstart/gjennomføring i 2019, samt de tilfeller hvor enkelte tiltak har blitt gjennomført tidligere enn planlagt. Enkelte av tiltakene er noe forsinket, og dette skyldes mangel på kapasitet og korrekt kompetanse. Etableringen av den nye faggruppen³ vil i betydelig grad bøte på dette, og det anses som sannsynlig at mye av denne forsinkelsen kan hentes inn.

² Fra «styringssystem for informasjonssikkerhet» til «ledelsessystem for informasjonssikkerhet»

³ Gjennom omorganiseringen av Avdeling for IT opprettes *faggruppe for personvern og informasjonssikkerhet* f.o.m 1.1.2020.

Flere av tiltakene, slik som videreutvikling og styrking av sikkerhetsorganisasjonen (1.1), formell rapportering (1.4) mv., er imidlertid avhengig av at enhetene tar det ansvaret de er tillagt gjennom ledelsessystemet. Dersom dette ikke skjer vil ikke disse tiltakene kunne gjennomføres som planlagt.

Tiltak 1.1 – Videreutvikling av sikkerhetsorganisasjonen.

Fra 1.1.2020 etableres *faggruppe for personvern og informasjonssikkerhet (FPI)* ved ITA, og antall årsverk som er dedikert til dette arbeidet styrkes fra to til fem. Dette vil gi den nødvendige kompetansesammensetning og kapasitet til å utvikle verktøy, veiledningsmateriell mv samt få opp et mer fungerende internkontrollsystem.

Statusrapporten fra høsten 2019 (se nedenfor under «tiltak 1.4» samt pkt 7) gir et godt innblikk i hvordan enhetene både stiller seg til det ansvaret de har, og hvordan de er rigget. Dette er et nødvendig grunnlag for å se hvordan organisasjonen må videreutvikles, og hvilken kompetanseheving som må til på enhetene. Sistnevnte omfatter både enhetene innehar den nødvendige forståelsen av sin rolle og ansvar, samt at de har den kompetansen de behøver for å ivareta dette ansvaret.

Tiltak 1.2 – Revisjon og utvikling av styrende dokumenter

Dette arbeidet er påbegynt i 2019, og det vises her til pkt 1 (underpunkt om ledelsessystemet) for nærmere informasjon.

Tiltak 1.3 – Evaluere risikostyringsverktøy og arbeidsmetodikk

Foreløpig brukes Excel som verktøy for risikovurderinger, og UiT bygger på Units malverk og metodikk (som igjen er utviklet på bakgrunn av internasjonale standarder). UiT har tilpasset Excelskjemaet noe, og inkludert flere brukerveiledninger, mer automatikk mv. Imidlertid er det et prekært behov for et bedre verktøy for risikovurdering og -håndtering innen informasjonssikkerhet, og dette gjelder for hele UH-sektoren. Unit har derfor tatt oppgaven med å igangsette et prosjekt for anskaffelse av slik verktøy. UiT og NTNU representerer UH-institusjonene i prosjektgruppen, og denne har oppstart våren 2020.

Tiltak 1.4 – Etablere formell rapportering og bruk av måleparametere

I 2019 ble det innført en årlig statusrapport som enhetene skal levere. Her skal både informasjonsverdiene⁴ kartlegges (i tråd med styrende prinsipp nr 7 for informasjonssikkerhet ved UiT, se vedlegg 2), sårbarheter, trusler og tiltak vurderes samt at enhetene skal orientere om status på risikovurderinger, organiseringen av arbeidet ved sin enhet mv. I første omgang var det fakultetene og universitetsbiblioteket som leverte denne rapporten, men også de administrative avdelingene på nivå 1 må levere denne rapporten. For utdypende informasjon vises det til pkt 7 *Årlig statusrapport fra enhetene* nedenfor.

Tiltak 1.5 – Etablere en styringskomité eller sikkerhetsutvalg

Informasjonssikkerhetsforumet ble etablert våren 2019, for nærmere informasjon vises det til pkt 5 *Sikkerhetsorganisering* nedenfor.

Tiltak 2.1 – Etablere prosess for behov og kravinnhenting (virksomhetsperspektiv)

Avdeling for IT har fått noen tilbakemeldinger gjennom statusrapporten for informasjonssikkerhet, men det må bygges videre på disse og utvikle en prosess som sikrer at informasjonssikkerhet blir den støttespilleren den skal være, fremfor noe organisasjonen oppfatter som en hindring.

Tiltak 2.2 – Definer grunnnivå (baseline) sikkerhetsmekanismer

Dette tiltaket er forsinket grunnet kapasitets- og til dels kompetansemangel. Gjennomføringen må derfor forskyves til 2020, og håndteres gjennom den kommende faggruppen.

Tiltak 2.3 – Gjennomføre GAP-analyser

Den informasjonen Avdeling for IT/faggruppen for personvern og informasjonssikkerhet har fått gjennom statusrapporten er et viktig utgangspunkt for å kunne gjennomføre GAP-analysen. Første del av prosessen er gjennomført ved at nåsituasjonen er kartlagt. Neste steg er å følge opp med analyser opp mot hvor UiT skal være.

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

Tiltak 3.1 – forenkle rapportering av hendelser, avvik og sikkerhetsbrudd

I 2019 ble det laget ny nettside for UiTs arbeid med informasjonssikkerhet, hvor «melde avvik» er lagt synlig og lett tilgjengelig. Informasjon og prosedyre for melding av avvik er også lagt ut på UiTs «Si ifra!»⁵-side. Prosedyrer for melding av avvik vil bli ytterligere forenklet i 2020 gjennom innføringen av TopDesk, som er et nytt saksbehandlingssystem hvor det også følger en selvbetjeningsportal med støtte for innmelding av saker via skjema mv.

3. Sikkerhetsmål og strategi

I mars 2019 vedtok Universitetet ny informasjonssikkerhetsstrategi, for perioden 2019-2021⁶. Strategien er ambisiøs, men representerer et høyst nødvendig fokus på og styrking av informasjonssikkerhetsarbeidet ved UiT.

4. Kriterier for akseptabel risiko

I rapporten for 2018 ble det fremhevet at kriteriene for akseptabel risiko burde gjennomgås og revideres. Dette fordi kriteriene var på et for overordnet nivå, og vanskelig å anvende. I forbindelse med ny informasjonssikkerhetsstrategi ble det utformet reviderte kriterier for akseptabel risiko, og disse ble integrert i strategidokumentene og vedtatt av Universitetsstyret.

5. Sikkerhetsorganisering

Sikkerhetsorganiseringen er fastsatt gjennom ledelsessystemet for informasjonssikkerhet (kap. 4). Nedenfor gjengis enkelte av rollene i sikkerhetsorganiseringen. Som påpekt i årsrapport 2018 er det behov for videreutvikling av sikkerhetsorganiseringen, og dette er tatt inn som ett av tiltakene i informasjonssikkerhetsstrategien.

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

⁵ <https://uit.no/si-ifra>

⁶ Sak S 9/19.

- **IT-direktør** er informasjonssikkerhetsansvarlig. IT-direktøren har forvaltningsansvaret for informasjonssikkerhet, og er gitt instruksjonsmyndighet overfor alle enheter ved UiT i saker som angår informasjonssikkerhet.
- **Enhetsledere**⁷ er ansvarlig for å tilfredsstille krav til informasjonssikkerhet i egen enhet, herunder blant annet å gjennomføre risikovurderinger og iverksette nødvendige tiltak. Høsten 2019 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 7.
- **Informasjonssikkerhetsrådgiverne** utøver IT-direktørens myndighet. Dette var tidligere to stillinger; teknisk sikkerhetsrådgiver samt jurist. IT avdelingen gjennomførte en større omorganisering høsten 2019⁸, og foretok da en økt satsning på feltet ved å omdisponere interne ressurser. Fra 1.1.2020 opprettes det en egen *Faggruppe for personvern og informasjonssikkerhet*, som består av totalt fem personer inkludert faggruppelider. Denne faggruppen er organisatorisk plassert direkte under IT-direktør, og ikke i en av seksjonene.
- **CSIRT**⁹ har ansvaret for å håndtere IT-hendelser mens de skjer.
- **Informasjonssikkerhetsforum** ble opprettet våren 2019, og har representanter fra samtlige fakulteter, UB samt de fleste avdelingene på nivå 1. Dette forumet er nærmere beskrevet i ledelsessystemets kapittel fire.

Videre har også personvernombudet en rolle for hva gjelder ivaretagelsen av informasjonssikkerheten for personopplysninger. Gjennom revideringen av ledelsessystemet og utvidelsen til å også omfatte personvern forøvrig vil personvernombudets rolle bli inkludert der. Personvernombudet har utarbeidet egen årsrapport for 2019, som delvis omfatter informasjonssikkerhetsspørsmål, se vedlegg 15.

⁷ Definert i ledelsessystemet som dekaner, avdelingsdirektører, museumsdirektør og biblioteksdirektør

⁸ Ny organisering ble fastsatt av Universitetsstyret i sak S 21/19.

⁹ Computer Security Incident Response Team (CSIRT)

Utfordringer og behov for videreutvikling av organisasjonen

Fokus hos ledelsen: I årsrapport 2018 ble det påpekt at informasjonssikkerhet har for lite fokus hos ledelsen ved UiT. Betydningen av at toppledelsen har fokus på informasjonssikkerhet har blitt understreket av Kunnskapsdepartementet, blant annet gjennom eget brev til UH-sektoren i begynnelsen av 2019.

Her har det skjedd en viss bedring gjennom 2019, blant annet gjennom Universitetsstyrets vedtak om at årsrapport 2018 skulle behandles i samtlige fakultetsstyrever. Dette ble gjennomført hos alle fakultetsstyrene samt bibliotekstyret. Informasjonssikkerhetsrådgiverne deltok på disse møtene og la frem både årsrapporten og informasjonssikkerhetsstrategien. Avdeling for IT opplevde en god dialog med styrene, og foreslår at dette blir 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 da 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.

Informasjonssikkerhet bør være et fast tema på utvidet ledermøte (ULM) og administrativt ledermøte (ALM), f.eks en gang i halvåret.

Samordning med beredskapsarbeidet forøvrig ved UiT

Universitetsdirektøren ser et behov for å få beredskap innen informasjonssikkerhet enda nærmere knyttet til det øvrige beredskapsarbeidet ved UiT, slik at beredskapsarbeidet behandles helhetlig.

UH-sektoren

UiT er selvstendig ansvarlig for at informasjonssikkerheten 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 (ISO 27014). I 2019 gjennomførte Unit møter med alle institusjonene i UH-sektoren hvor de informerte nærmere om denne styringsmodellen. Videre måtte alle institusjonene besvare en rekke spørsmål om arbeidet med informasjonssikkerhet og personvern, og sommeren 2019 leverte Unit en tilstandsrapport for informasjonssikkerhet i sektoren. Slike kartleggingsmøter med Unit blir gjennomført årlig, og for UiTs del er neste møte i februar 2020.

Videre har Unit gitt UNINETT¹⁰ 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.

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

¹⁰ UNINETT er et statlig infrastrukturselskap, og drifter blant annet forskningsnett (nettforbindelsen UH-sektoren benytter), og er leverandør av en rekke fellesløsninger (bl.a. innloggingsløsningen FEIDE, trådløstilgang via Eduroam mv). <https://www.uninett.no>.

6. Avviksmeldinger

Løpenummer viser til intern oversikt holdt av informasjonssikkerhetsrådgiverne.

De mest alvorlige avvik i løpet av perioden			
Avvik #	Hendelsesbeskrivelse	Tiltak	Ansvarlig:
12	<p>Helseopplysninger om barn ble tilgjengeliggjort for andre deltakere i et forskningsprosjekt.</p> <p>Forsker oppfattet opplysningene som anonymiserte, men de var i realiteten kun avidentifisert og kunne potensielt reidentifiseres med relativt enkle midler.</p>	<p>Deltakerne ble kontaktet og oppfordret til å slette de mottatte opplysningene.</p> <p>Forsker ble fulgt opp for å unngå at dette skjer igjen.</p> <p>Saken ble meldt til Datatilsynet.</p>	Helsefak
13	<p>UiT ble utsatt for et vellykket bedrageri i størrelsesordenen 1,2 millioner Euro, ved at aktøren lyktes med å utgi seg for å være den ekte leverandøren og fikk derfor endret bankinformasjonen.</p>	<p>Saken ble anmeldt.</p> <p>UiT foretok umiddelbart tekniske undersøkelser, men det er ingen indikasjoner på at uvedkommende har vært inne i våre systemer.</p> <p>Risikovurderinger innenfor økonomiforvaltningen gjennomføres første halvår 2020.</p>	Helsefak / ORGØK

14	Forsker opplever at data blir borte fra fellesdisk.	Saken er fremdeles under behandling, men CSIRT har utelukket at uvedkommende har vært inne.	Helsefak
Flere	<p>UiT har flere hendelser som omhandler feilsending av epost og SMSer, tyveri av PCen, utskrifter som ligger igjen på skriver mv.</p> <p>Disse har imidlertid vært at mindre alvorlig art, og har ikke krevd f.eks melding til Datatilsynet.</p>	Videre arbeid med utvikling av sikkerhetskultur, samt få redusert bruk av e-post til visse typer informasjon.	Flere
Flere	<p>Privat utstyr benyttes i forbindelse med studentprosjekter. Dette skyldes delvis dårlig kjennskap om at privat utstyr ikke skal benyttes, og i visse tilfeller at UiT mangler gode tjenester.</p> <p>Sistnevnte er særlig gjeldende for videoopptak med fortrolig innhold, da dette er en komplisert materie å håndtere korrekt. Den løsningen UiT har er tungvidt og forholdsvis kostbar hvis det er mange studenter som behøver den (krypterte minnepinner).</p>	<p>Det arbeides både med å utvikle bedre tekniske løsninger, samt opplæring og kompetanseheving slik at det blir kjent at privat utstyr ikke skal benyttes.</p> <p>Her ligger det imidlertid en potensielt stor kostnad for UiT for få dette håndtert på god nok måte.</p>	Flere

6.1. Oppsummering avvik og risikoområder

Informasjonssikkerhetsrådgiverne ved Avdeling for IT mottok melding om 20 avvik i 2019, herunder de 3+ som er nevnt ovenfor. 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. Informasjonssikkerhetsrådgiverne 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 deretter meldes det videre. Imidlertid fører dette til en 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 klokke timer). Høsten 2019 arrangerte Avdeling for IT målrettet opplæring mot systemeierne for å gjøre dem bevisste på hva de måtte melde videre, samt sikre at dette skjer raskt.

Totalt ett avvik ble meldt til Datatilsynet i 2019, mot fire i 2018. Saken er ferdig behandlet av Datatilsynet, og UiT ble ikke ilagt noen sanksjoner. 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.

Basert på erfaringene med de avvikene som ble meldt har er sentrale risikoområder og avviksårsaker oppsummert nedenfor. Tilsvarende er påpekt i tidligere årsrapporter, og risikoen er fremdeles forholdsvis høy. Disse risikoområdene er forholdsvis spesifikke (bruk av video og systeminnføring), og er tatt med grunnet utbredelsen og det store potensialet for skadelige hendelser hvis UiT ikke oppnår kontroll. I årsrapporten for UiT inngår det en mer overordnet risikovurdering hvor også informasjonssikkerhet er inntatt. Universitetsdirektøren viser til den årsrapporten for nærmere detaljer om, og vurdering av, disse.

Bruk av video

Video er i utstrakt bruk på UiT, 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 fortrolig 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. 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.

For automatisert opptaksutstyr er det gjennomført en rekke tiltak, og her må UiT sies å ha forholdsvis god kontroll. Tiltakene inkluderer skilt inni og utenfor rom med automatisk opptaksutstyr. Disse har teksten «recording» og lyser rødt når opptak pågår. Det er også oppslag utenfor rommene med mer informasjon. Fremme på podiene er det montert skjermer 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.

Universitetsdirektøren ser imidlertid særlige utfordringer når video skal benyttes som verktøy av studentene (f.eks i forbindelse med datainnsamling for masteroppgaver, arbeidskrav mv) og i særdeleshet når det er tale om fortrolig materiale. Det skjer forholdsvis ofte at studentenes private utstyr benyttes selv om dette ikke er tillatt i henhold til *retningslinjer for personvern i forskings- og studentprosjekt* pkt 11¹¹, og da har UiT per definisjon ikke den nødvendige kontrollen med informasjonssikkerheten. UiT har noen løsninger for å håndtere dette, slik som bruk av krypterte minnepinner. Sistnevnte løsninger er imidlertid ikke spesielt skalerbar, og selv om konfidensialiteten til informasjonen er godt ivaretatt så foreligger det en klar risiko for tap av tilgjengelighet (informasjonen går tapt, f.eks ved at minnepinnen ødelegges eller mistes). Dette kan få tildels store konsekvenser for studentene, eksempelvis dersom materialet skulle benyttes som del av eksamen. Utvikling/innkjøp av egnet teknisk

¹¹ https://uit.no/forskning/art?p_document_id=604029&dim=179056

løsning fremstår derfor som påkrevd ut fra et sikkerhetsmessig perspektiv, men dette vil medføre kostnader.

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

7. Årlig statusrapport fra enhetene

Som nevnt under pkt 2 ovenfor ble det i 2019 innført en årlig statusrapport som enhetene skal levere. Denne ble sendt ut i slutten av september 2019 med svarfrist 31.12.2019. Her skulle enhetenes kartlegge sine informasjonsverdier¹², identifisere sårbarheter, vurdere trusler og tiltak samt at enhetene skal orientere om status på risikovurderinger, organiseringen av arbeidet ved sin enhet mv. I første omgang var det fakultetene og universitetsbiblioteket som leverte denne rapporten, men også de administrative avdelingene på nivå 1 må levere det samme i 2020. Det mest omfattende arbeidet er ved førstegangslevering mens det for påfølgende år blir mindre omfattende da det er primært vil være tale om vedlikehold og oppdateringer av tidligere rapporter.

Vedlagt årsrapporten er oversendelsesbrevet til enhetene¹³ vedrørende statusrapporten samt spørsmålene, se vedlegg 4 og 5.

I oversendelsesbrevet fremkommer bakgrunnen og målsetningen med rapporten i mer detalj, men i korte trekk kan det her fremheves 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 enheten mv.

Disse kartleggingene og vurderingene må foretas av enhetene selv. Dette fordi enhetene er nærmest til å skaffe seg oversikt, samt vurdere hvilken informasjon som har størst betydning og særlig kan være utsatt angrep fra trusselaktører. Videre er det gjennom *ledelsessystem for informasjonssikkerhet* fastslått at det er enhetslederne som har ansvaret for ivaretagelsen av informasjonssikkerheten på egen enhet. En nødvendig forutsetning for å oppfylle dette ansvaret er å vite hva man faktisk har.

¹² Bl.a i tråd med styrende prinsipp nr 7 for informasjonssikkerhet ved UiT, se vedlegg 2

¹³ Til spørsmålene var det også vedlagt en del veiledningsmateriale.

Til hjelp i arbeidet ble det utarbeidet og oversendt veiledninger rundt hva en informasjonsverdi er, hvilke trusselaktører som er identifisert som relevante for UiT¹⁴, eksempler på hvordan vurdere trusler mot informasjonsverdiene samt tabeller for vurdering hvor alvorlig eventuelle konsekvenser kan være. Videre ble det understreket i brevet at dersom enhetene hadde spørsmål eller behov for bistand kunne informasjonssikkerhetsrådgiverne ved Avdeling for IT kontaktes. Flere av enhetene valgte å benytte seg av dette, men ikke alle.

Fakultetsstyrene og bibliotekstyret ble orientert om at denne rapporten ville komme da årsrapporten og informasjonssikkerhetsstrategien ble behandlet i styremøtene våren 2019. Før utsendelse ble det gjennomført en mindre pilot på ett av fakultetene for å undersøke hvor lett materialet var å benytte, og hvordan det var fornuftig å legge opp arbeidet. Som følge av denne piloten ble det gjennomført noen mindre endringer i materialet, og deretter ble det sendt ut.

Erfaringene med utarbeidelsen av 2019-rapporten vil bli brukt til å evaluere spørsmålene, fokus og om det skal foretas justeringer til neste års utsendelse. Det er også sannsynlig at den kommende faggruppen for personvern og informasjonssikkerhet vil klare å foreta nødvendig spissing av rapportene etter hvert som UiT generelt og fakultetene spesielt får erfaringer med denne typen kartlegging og vurdering. Målet er å ivareta balansegangen mellom å ha tilstrekkelig innsikt i alle informasjonsverdier ved UiT (slik at sikkerheten kan ivaretas tilstrekkelig), og det at universitetet er en virksomhet med høyt tempo og ulikeartet aktivitet. En oversikt med svært høy detaljgrad og som skal være fullt ut oppdatert til enhver tid vil neppe være forsvarbar ressursmessig. I vurderingen av hvilket detaljnivå man skal oppnå bør det fokuseres på at målet er at fakultetet (og i forlengelsen UiT) skal vite om, ha kontroll på og kunne reelt sett vurdere sine informasjonsverdier. Blir man for overordnet er oversikten tilnærmet verdiløs, mens hvis det blir for detaljert klarer man ikke benytte informasjonen på en fornuftig måte eller holde den oppdatert og relevant.

¹⁴ Kategorisert etter type; statlige aktører, konkurrenter/næring, vinningskriminelle, aktivister samt insider/utro tjenere. I vurderingen tok enhetene utgangspunkt i denne listen, og skulle ikke utdype den ytterligere.

Arbeidet med rapporten på fakultetene og Universitetsbiblioteket

Rapportene viser at de fleste enhetene har gjort et grundig og godt arbeid med materien. Vedlagt følger rapporten fra hver enhet, se vedlegg 6-13. Skjemaene med komplett oversikt over informasjonsverdier og enhetenes vurdering av disse er imidlertid ikke vedlagt her.

De vurderinger som er gjort i rapporten og hvilke informasjonsverdier som er identifiserte viser også en økt modenhet i kunnskapen om informasjonssikkerhet ute blant enhetene. Da UiT arbeidet med ny informasjonssikkerhetsstrategi ble det gjennomført en rekke intervjuer med sentrale interessenter på UiT, både i toppledelse og fra enhetene. Blant de utfordringer som ble identifisert på virksomhetsnivå var blant annet lite forståelse av hva informasjonssikkerhet innebærer og et utbredt syn på at ansvaret ligger hos Avdeling for IT. Jevnt over har det vært en gjentakende utfordring de senere år at store deler av virksomheten har ansett informasjonssikkerhet som en «IT-sak». Dette medfører en stor risiko for UiT; både fordi man fort overser viktigheten av informasjonssikkerhet for ikke-digitale informasjonsverdier, samt at dersom enhetsledelsen unnlater å ta det ansvaret de har kan ikke informasjonssikkerheten ivaretas på en god måte. Den kartlegging og de betraktninger de fleste enhetene har gjort viser at denne misoppfatningen langt på vei har snudd i ledelseslinjen på enhetene. Dette gjelder imidlertid ikke alle, og ett fakultet som var sterkt kritisk til måten kartleggingen ble gjennomført på trakk blant annet inn sentraliseringen av IT-avdelingen for en rekke år siden som argument for hvorfor de ikke har de nødvendige ressurser og kompetanse til å gjennomføre kartleggingen og vurderingen som etterspurt:

«Under dannelsen av IT-avdelingen ble IKT-ressursene på fakultetene trukket inn, mens fakultetene skulle få dekket sine behov for IKT-støtteressurser fra den nye IT-avdelingen. Dermed har ikke fakultetene hverken ressurser eller kompetanse for å gi gode svar på slike bestillinger som den IT-avdelingen sendte 25. september, ei heller å utarbeide en saksframstilling til fakultetsstyret av den kvalitet og format som vil forventes.»

Dette representerer en grunnleggende misforståelse av hva informasjonssikkerhet er, hvilken kompetanse som kreves og hvem som er nødt til å dra dette arbeidet på enhetene. De ressursene som ble sentraliserte drev ikke med de oppgavene som nå etterspørres, og kunne heller ikke blitt satt til det om de fremdeles var ute på enhetene. I det videre må UiT derfor fortsette å fokusere på opplæring og kompetanseheving for å klare å fullt ut snu slike misoppfatninger, og få arbeidet med informasjonssikkerhet inn i et bærekraftig spor.

Gjennom 2020 vil faggruppen for personvern og informasjonssikkerhet arbeidet aktivt med de innleverte statusrapportene, og analysere svarene og vurderingene som er kommet inn slik at denne viktige informasjonsressursen benyttes aktivt i sikkerhetsarbeidet. Dette vil deretter bli løftet frem i kommende årsrapporter til Universitetsstyret. Faggruppen vil videre ha dialog med enhetene for hva gjelder deres svar, og eventuelle uklarheter. For statusrapporten for 2020 vil fellesnevnerne trekkes ut, og rapporten tilpasses slik at enhetene primært kan fokusere på det som er særskilt for dem.

8. Status på risikovurderinger

Risikovurderinger gjennomføres ikke i den grad de skal etter gjeldende lovverk.

De senere år har det blitt 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 ved UiT forekommer det også eksempler på at risikovurderinger er gjennomført og tiltak vedtatt uten at de følges ikke opp. Det mangler gode planer for prioritering og gjennomføring av tiltakene, samt faktisk oppfølging av de planene som fins.

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

For informasjonssikkerhetsrådgiverne ble fokus fra 2018 av dreid fra aktiv deltakelse i risikovurderinger over til rådgivning og utarbeidelse av materiell, veiledninger, maler etc., og dette vil fortsette. I en virksomhet som UiT, med høyt og ulikeartet aktivitetsnivå, er det svært mange risikovurderinger som må gjennomføres og disse spenner fra svært avgrensede og små vurderinger til svært omfattende som kan ta månedsvis å fullføre. Omfanget er såpass stort at det ikke er gjennomførbart å aktivt fasilitere dette fra *faggruppen for personvern og informasjonssikkerhet*. 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. *Faggruppe for personvern og informasjonssikkerhet* må imidlertid utvikle hjelpemidler (verktøy, maler etc) som kan bistå enhetene. I tillegg vil de selvsagt kunne få fortløpende rådgivning, men prosessen og gjennomføringen må tas på enhetsnivå. Dersom dette skal aktivt håndteres av faggruppen vil det bli tilnærmet umiddelbare kapasitetsutfordringer og enhetene vil oppleve store forsinkelser før de kan gå i gang med anskaffelser, forskningsprosjekter, utdanningsaktiviteter etc.

Høsten 2019 ble fakultetene og Universitetsbiblioteket for første gang bedt om å levere en statusrapport for informasjonssikkerhet, som beskrevet ovenfor i pkt. 7. I UiTs virksomhetsplan for 2020 er det fastsatt at det skal gjennomføres risikovurderinger på hver enhet som for UiT som sådan, og kartleggingen og vurderingene i statusrapportene fra enhetene er i denne sammenheng helt avgjørende for å kunne gjennomføre disse risikovurderingene.

9. 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, med tilhørende klassifisering av kritikalitet og verdi, noe som den ovennevnte statusrapporten bidrar til å skaffe. 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. Dette verktøyet bør være likt i sektoren, og det vises her til kommentarer til *tiltak 1.3* i pkt 2 ovenfor.

10. Ressurs- og kompetansebehov

Det har over flere år vært for få ressurser tilknyttet informasjonssikkerhetsarbeidet, både på forvaltningssiden og den operative siden. Her blir det imidlertid en bedring fra 1.1.2020 når ny faggruppe for personvern og informasjonssikkerhet opprettes. Da økes kapasiteten til fem heltidsstillinger (tre med teknisk bakgrunn og to jurister), og dette er en markant bedring fra høsten 2018 da det kun var én heltidsstilling på forvaltningsdelen av informasjonssikkerhet. Dette vil gi utslag i en bedre evne til å besvare henvendelser, utvikle opplæringsprogram, utføre operativt arbeid samt utvikle regelverk, materiell og rammeverk. Enhetene vil da få mer støtte til å utføre sitt arbeid innenfor informasjonssikkerhet, men det er viktig å understreke at det er enhetene som sitter med ansvaret for ivaretagelsen av informasjonssikkerheten på sin enhet (jf ledelsessystemet kapittel fire) og de må ha tilstrekkelig med kompetanse og fokus på feltet.

Etter ledelsessystemet 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 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. Risikovurderinger må gjennomføres i et langt større antall enn i dag, og dette må skje der aktiviteten foregår. Informasjonssikkerhetsfunksjonen ved Avdeling for IT vil som nevnt 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).

Ut fra det Avdeling for IT/informasjonssikkerhetsrådgiverne 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 UiT. Blant annet får informasjonssikkerhetsrådgiverne nokså ofte tilbakemelding om at informasjonssikkerhet er en «IT-sak», og at brukeren anser dette som noe Avdeling for IT håndterer fullt ut 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. 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. Her kan det nevnes at statusrapporten fakultetene og UB leverte høsten 2019 viser en klar bedring på dette feltet, og de fleste enhetene identifiserte i stor grad informasjonsverdier, sårbarheter og tiltak som gikk utover det rent IT-tekniske.

11. Revisjon av ledelsessystemet

Gjennom arbeidet med strategien vil det bli gjennomført revideringer av ledelsessystemet.

Innledningsvis i denne rapporten ble det nevnt at det er ønskelig å bygge ut ledelsessystemet til å også omfatte personvern, slik at begge disse områdene ses i sammenheng. Dette vil kreve et forholdvis omfattende arbeid.

12. Vedlegg

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

- Styrende prinsipper for informasjonssikkerhet (vedlegg 2)
- Periodisert handlingsplan for oppnåelse av målbildet i strategien (vedlegg 3)
- Statusrapport 2019
 - o Oversendelsesbrev (vedlegg 4)
 - o Spørsmålene (vedlegg 5)
- Statusrapportene
 - o Det juridiske fakultet (vedlegg 6)
 - o Fakultet for humaniora, samfunnsvitenskap og lærerutdanning (vedlegg 7)
 - o Fakultet for naturvitenskap og teknologi (vedlegg 8)
 - o Norges arktiske universitetsmuseum og akademi for kunstfag (vedlegg 9)
 - o Fakultet for biovitenskap, fiskeri og økonomi (vedlegg 10)
 - o Fakultet for ingeniørvitenskap og teknologi (vedlegg 11)
 - o Det helsevitenskapelige fakultet (vedlegg 12)
 - o Universitetsbiblioteket (vedlegg 13)
- Personvernombudets årsrapport 2019 (vedlegg 14)
- Årsrapport informasjonssikkerhet 2018 (vedlegg 15)

