



## Møteinncalling

Utvalg: **Fakultetsstyret for Det helsevitenskapelige fakultet**  
Møtested: Digitalt møte  
Møtedato: 30.09.2022  
Tidspunkt: 09:00-13.00

Eventuelt forfall må meldes snarest på tlf. 77 64 46 01 eller mobil 915 47 421.  
Vararepresentanter møter etter nærmere beskjed.

**Saksliste**

<i>Saksnr</i>	<i>Tittel/beskrivelse</i>	<i>U.off.</i>	<i>Arkivref.</i>
FS 27/22	Godkjenning av møteinnkalling og saksliste		
FS 28/22	Møtereferat fra fakultetsstyremøte 17. juni 2022		2022/261
FS 29/22	Møtereferat fra behandling av sak på sirkulasjon i perioden 2.-6. september 2022		2022/261
OS 13/22	Muntlig orientering ved dekan Gunbjørg Svineng		
OS 14/22	Saker behandlet av dekanen på fullmakt i perioden 7. mai - 23. september 2022		2022/261
FS 30/22	Endringer i studieprogramporteføljen for studieåret 2023/2024		2021/4227
FS 31/22	Rapport forskning 2021 - Det helsevitenskapelige fakultet		2022/5750
FS 32/22	Behandling av årsrapport for informasjonssikkerhet og personvern 2021		2022/4345

**FS 27/22 Godkjenning av møteinnkalling og saksliste /**  
**OS 13/22 Muntlig orientering ved dekan Gunbjørg Svineng /**

## ORIENTERINGSSAK

Til:  
Fakultetsstyret for Det helsevitenskapelige fakultet

Møtedato:  
30.09.2022

Sak:  
14/22

### Saker behandlet av dekanen på fullmakt i perioden 7. mai - 23. september 2022

#### 12-22 Tildeling av Forskning- og utdanningstermin og økonomisk støtte til utenlandsopphold høst 2022 og vår 2023

(Ephorte 2022/1585-14)

Dekanen har innvilget følgende søknader om FoU-termin, med eller uten økonomisk støtte:

Institutt	Navn	Tidsrom for innvilget FoU-termin	Økonomisk støtte til utenlandsopphold
IPS	James McCutcheon	h2023	118 400
IMB	Maria Perander	h2023-v2024	168 000
ISM	Erik Eik Anda	h2023-v2024	296 000
IFA	Beate Hennie Garcia	h2023-v2024	296 000
IHO	Nina Emaus	2023-2024, 2024-2025	148 000
IFA	Guro Forsdahl	v2023-v2024	84 000
IH	Rune Waaler	h2023-v2024	148 000
IHO	Filip Maric	1.10.23-28.2.24 (fem mnd)	148 000
IKM	Hege Sagstuen Haugnes	h2023-v2024	Avslag
ISM	Guri Skeie	h2023-v2024	Avslag
IHO	Henriette Riley	h2023	Avslag
IKM	Rolf Wynn	h2023	Avslag
IMB	Ole-Jakob How	h2023-v2024	Avslag
ISM	Tom Wilsgaard	h2023-v2024	Avslag
IKM	John-Bjarne Hansen	h2023-v2024	Avslag
IHO	Bente Norbye	h2023-v2024	Avslag
IKM	Brita Ellevåg	h2023-v2024	Avslag
IMB	Johanna U Ericson	h2022-v2023	Ikke søkt
IMB	Ellen Aasum	v2023-h2023	Ikke søkt
IHO	Gunn Pettersen	h2023-v2024	Ikke søkt
IPS	Monika Abels	v2023-h2023	Ikke søkt
IPS	Mikolaj Hernik	vår2024	Ikke søkt
IHO	Inger Pauline Landsem	h2023-v2024	Ikke søkt
IHO	Solrunn Hansen	h2023-v2024	Ikke søkt
ISM	Unni Ringberg	h2023-v2024	Ikke søkt
RKBU	Jeanette Skoglund	h2023-v2024	Ikke søkt

IVP	Gunn-Tove Minde	h2023	Ikke søkt
RKBU	Charlotte Reedtz	h2023-v2024	Ikke søkt
IKO	Anne Margrete Gussgard	h2023-v2024	Ikke søkt
RKBU	Henriette Kyrrestad	v2023	Videreføring av tidl. midler
ISM	Tonje Braaten	h2022/v2023	Videreføring av tidl. midler på nytt sted
<b>Total</b>			<b>1 406 400</b>

1. Avslagene om økonomisk støtte skyldes begrensede midler tilgjengelig for fordeling. Tildelingene er gjort etter kriteriene for økonomisk støtte, samt etter instituttens prioriteringer.
2. Søknaden til **Johanna U. Ericsson** innvilges med to semesters FoU-termin, ett år tidligere enn utlyst, fra 1.juli 2022 – 31.juni 2023
3. Søknaden til **Filip Maric** innvilges med utsatt oppstart av FoU-termin til den 1. oktober 2023 for å ivareta undervisningen han er hovedlærer ved i første halvdel av høstsemesteret.
4. Søknaden til **Monika Abels** innvilges med framskyndet oppstart vår 2023 og høst 2023 innvilges med begrunnelse i undervisningsansvar og FG-ledelse.
5. Søknaden til **Ellen Aasum** innvilges med framskyndet oppstart vår 2023 og høst 2023 med bakgrunn i arbeids- og budsjettssituasjonen ved enheten.
6. Søknaden til **Guro Forsdahl** innvilges med framskyndet og oppdelt oppstart våren 2023 og våren 2024 for å kunne ivareta egen undervisning høsten 2023. Forsdahl innvilges økonomisk støtte til utenlandsopphold under vilkår at hun snarest, og senest 15. august 2022 ettersender invitasjonsbrev fra vertsinstitusjonen.
7. **Rune Waaler** sin søknad om FoU-termin innvilges under vilkår at IH har økonomisk handlingsrom i 2023/2024 for å dekke opp undervisningsaktiviteten. Dette skal løses innen én måned etter tildeling, for å gi søker forutsigbarhet og rom til å planlegge og gjøre praktiske forberedelser.
8. **Mikolaj Hernik** innvilges FoU-termin for våren 2024. Fakultetet gjør Hernik oppmerksom på at dersom han takker ja til dette, vil han ikke kunne søke på FoU-termin for høsten 2024 da ny opptjeningsstid regnes fra sist innvilget FoU-termin.
9. **Unni Ringberg** sin søknad innvilges under vilkår at arbeidsplanen er gjennomførbar innenfor instituttets budsjett eller andre prosjektmidler.
10. **Nina Emaus** innvilges økonomisk støtte til utenlandsopphold under vilkår at hun snarest, og senest 15. august 2022 ettersender invitasjonsbrev fra vertsinstitusjonen.
11. **Tonje Braatens** søknad om endret oppholdssted for FoU-termin høst 2022 innvilges under vilkår at invitasjonsbrev fra vertsinstitusjon ettersendes snarest, og innen 1. juli 2022.

### 13-22 Fullføringsstipend for kandidater med bestått forskerlinje i medisin, odontologi og psykologi ved Det helsevitenskapelige fakultetet

Dekanen har besluttet følgende:

1. *Forskerlinjen i medisin, odontologi og psykologi får tildelt midler tilsvarende to hjemler i basis*
2. *Programstyret for forskerutdanning vedtar kriterier for prioritering av fullføringsstipend til kandidater med bestått forskerlinje i medisin, odontologi og psykologi*

## 14-22 Endringer i emneportefølje våren 2023

(Ephorte 2021/4227)

Dekanen har godkjent opprettelsen av følgende nye emner, samt revisjon og nedlegging av emner ved Det helsevitenskapelige fakultet:

### Oppretting av nye emner:

PSY-3035 Programming and Data Visualization for Researchers  
PSY-3034 Developmental perspectives on psychological phenomena – a virtual exchange course  
FAR-2401 Legemiddelfremstilling og kvalitetskontroll  
FAR-2206 Anvendt farmakologi 1  
FAR 2505 Klinisk farmasi og apotekpraksis  
VPL-1202/1302 Introduksjon til vernepleieyrket; menneskets psykologi, utvikling og læring

### Nedlegging av emner:

VPL-1201/1301 Faget, yrket og yrkesrollen. Den helse- og sosialfaglige kompetansen.  
VPL-1203/1303 Menneskets psykologi, utvikling og læring  
VPL-2530 Aktør i organisasjoner  
VPL-2540 Vernepleiefaglig fordypning  
VPL-2531 Aktør i organisasjoner  
VPL-2541 Vernepleiefaglig fordypning

### Revisjon av emner:

PSY-3015 Qualitative Methods  
PSY-2553/2554 Cognitive Psychology and dissemination of science  
FAR-2101 Legemidler og samfunn  
VPL-1206/1306 Kommunikasjon og samhandling  
VPL-1208/1308 Miljøterapi, habilitering og rehabilitering  
VPL-1209/1309 Helse og omsorg  
VPL-1211/1311 Likeverd i kultur og samfunnsdeltakelse  
VPL-2015/2315 Profesjonsutøvelse i organisasjoner  
VPL-2316 Vernepleiefaglig fordypning

## 15-22 Endringer i emneporteføljen våren 2023 – Institutt for helse- og omsorgsfag

(Ephorte 2021/4227)

Dekanen godkjenner revisjon av følgende emner ved Institutt for helse- og omsorgsfag, Det helsevitenskapelige fakultet.

### Revisjon av emner:

RAD-2620 *Praktisk radiografi – spesialisering*  
SYP-3502 *Vitenskapsteori, forskningsmetoder, metodologi og forskningsetikk*  
HEL-3168 *Kroppsforståelse, kunnskap og kommunikasjon*  
SYP-2511-N *Integrert sykepleiefaglige, naturvitenskapelige og samfunnsvitenskapelige emner*  
SYP-2511-D *Integrert sykepleiefaglige, naturvitenskapelige og samfunnsvitenskapelige emner*  
SYP-2511 *Integrert sykepleiefaglige, naturvitenskapelige og samfunnsvitenskapelige emner*

### Revisjon av emner:

RAD-2620 *Praktisk radiografi – spesialisering*  
SYP-3502 *Vitenskapsteori, forskningsmetoder, metodologi og forskningsetikk*  
HEL-3168 *Kroppsforståelse, kunnskap og kommunikasjon*  
SYP-2511-N *Integrert sykepleiefaglige, naturvitenskapelige og samfunnsvitenskapelige emner*  
SYP-2511-D *Integrert sykepleiefaglige, naturvitenskapelige og samfunnsvitenskapelige emner*

Gunbjørg Svineng  
Dekan

*Dokumentet er elektronisk godkjent og krever ikke signatur*

Saksansvarlig: Kjetil Kvalsvik  
Saksbehandler: Åshild Strømmesen

## SAKSFRAMLEGG

Til:	Møtedato:	Sak:
Fakultetsstyret for Det helsevitenskapelige fakultet	30.09.2022	30/22

### Endringer i studieprogramporteføljen for studieåret 2023/2024

#### Innstilling til vedtak:

1. Revidert studieplan for bachelor i radiografi godkjennes
2. Revidert studieplan for master i sykepleie godkjennes

#### Bakgrunn:

##### 1. Bachelorprogrammet i radiografi

Institutt for helse og omsorgsfag (IHO) ved bachelorprogrammet i radiografi (RADIOGRAF) ønsker å sette inn et læringsutbytte under generell kompetanse i studieplanens overordnede felles læringsutbytter.

Det gjelder følgende læringsutbytte:

*«innsikt i sammenheng mellom helse, utdanning, arbeid og levekår for å bidra til god folkehelse og arbeidsinkludering».*

Begrunnelsen er at det er en mangel at ovenfor nevnte læringsutbytte ikke står i studieplanen. Læringsutbyttet var utarbeidet, men ble fjernet etter beskjed fra fakultet om at det kunne være inntil 20 felles læringsutbytter. Utdanningen hadde utarbeidet 21 felles læringsutbytter. Studieleder sier at: *«I ettertid har sakkyndig utvalg i NOKUT kritisert at det ble satt strek på 20 LUBer, noe ergoterapi utdanningen har fått beskjed i sin RETHOS gjennomgang».* Studieleder ber nå om å få sette inn nevnte læringsutbytte i de overordnede felles læringsutbyttene i studieplanen. Endringen gjelder fra opptaket høsten 2023.

Ovenfor nevnte læringsutbytte ønskes også satt inn under kunnskap i emnebeskrivelsen til RAD-2620 Praktisk Radiografi 4 – spesialisering. Endringen i emnebeskrivelsen er godkjent på fullmakt av instituttleder ved IHO (i sak 19-22 med e-Phorte referanse 2022/22-13). Endringen i emnebeskrivelsen oversendes fakultetet i egen sak for emneendringer ved IHO innen neste frist for oversendelse som er 15. august.

#### Tilstedeværelse:

Studieleder ønsker å ha krav om obligatorisk oppmøte ved all undervisning i studieplanen. Formuleringen under er satt inn i delen om faglig innhold og beskrivelse av studiet:



«Tilstedeværelse: krav om obligatorisk oppmøte ved all undervisning. Fravær over 20 % i emnet fører til tap av eksamensrett og endret studieprogresjon».

## **2. Master i sykepleie (M-SYKEPL)**

Institutt for helse- og omsorgsfag (IHO) har oversendt ny revidert studieplan for M-SYKEPL (Master i sykepleie) til godkjenning. Studieprogrammet er organisert som en paraplymaster med studieretninger innen anestesi, barn-, intensiv-, operasjon og kreftsykepleie (ABIOK).

Den nye studieplanen er fundamentert i forskriftene om nasjonal retningslinje for [anestesisykepleieutdanning](#), [barnesykepleieutdanning](#), [intensivsykepleieutdanning](#), [operasjonssykepleieutdanning](#) og [kreftsykepleieutdanning](#) av 01.01.2022.

Studieplanen er kvalitetssikret og i tråd med kvalitetssystemet ellers.

I forhold til den reviderte studieplanen vil IHO fortsatt operere med samme ressurser som ved tidligere studieplan.

Gunbjørg Svineng  
dekan

—

*Saksansvarlig: Astrid Gramstad, prodekan utdanning*

*Saksbehandler: Rådgiver Reidar D. Arnesen, Seksjon for forskning, utdanning og formidling*

*Dokumentet er elektronisk godkjent og krever ikke signatur*

## SAKSFRAMLEGG

Til:  
Fakultetsstyret for Det helsevitenskapelige fakultet

Møtedato:  
30.09.2022

Sak:  
31/22

### Rapport forskning 2021 - Det helsevitenskapelige fakultet

#### Innstilling til vedtak:

Fakultetsstyret tar Rapport forskning 2021 til etterretning og godkjenner foreslåtte tiltak.

#### Bakgrunn:

Fakultetet har etter vedtak i FS (7.3.2019) årlig utarbeidet en forskningsrapport. Arbeidet med forskningsrapporten er ressurskrevende, og ett år mellom to rapporter er for kort tid til å kunne følge opp tiltakene. Fakultetet foreslår derfor forskningsrapport hvert annet år, tilsvarende nylig vedtak for kvalitetsmeldingen for utdanning.

Årets Rapport forskning tar for seg perioden 2017 til 2021, og ser på resultater for søknader om ekstern finansiering, ekstern inntekt, publikasjonspoeng, Open Access og allmenrettet formidling. Resultatene ses i lys av KDs målsetninger for forskning; 1) kvalitet i forskning, 2) forskning for velferd, verdiskapning og omstilling og 3) effektivt, mangfoldig og solid forskningssystem. I 2023 blir de nasjonale målene og indikatorene erstattet av institusjonsvise indikatorer basert på universitetenes mål i egen strategi. Årets resultater diskuteres derfor også i lys av UiTs nye strategi Eallju – drivkraft i nord. Ut fra rapporten er følgende tiltak definert:

TILTAK	ANSVAR
<b><i>Tilføyer til tiltak fra Rapport forskning 2020</i></b>	
1) Helsefak viderefører implementering av forskningsgruppens utviklingsplaner. Kortsiktige og langsiktige planer om ekstern forskningsfinansiering skal konkretiseres ved å inkludere «one-pagere» for alle typer søknader i et appendix til utviklingsplanene.	Fakultetet og instituttene
2) Helsefak viderefører arbeidet med enhetenes handlingsplan for økte eksterne inntekter og økt publisering. Forskningsgruppens utviklingsplan inkluderes som en del av dette arbeidet, slik at det er sammenheng mellom instituttens handlingsplan og forskningsgruppens planlagte aktiviteter. Oppfølging av instituttens planer endres til et felles lederseminar ved årsskifte i stedet for dialogmøtene.	Fakultetet og instituttene
<b><i>Kvalitet i forskning</i></b>	

3) Helsefak skal ha som ambisjon om å øke antall søknader og tilslag til EU. Herunder arbeide for å mobilisere og legge til rette for miljøer som kan gå sammen om å søke EUs Horizont Europa, Cluster 1- Health generelt, og Mission Cancer spesielt.	Fakultetet og instituttene
4) Helsefak må jobbe for et økt økonomisk handlingsrom til støtte for prestisjetunge senter søknader, samt jobbe opp mot nivå 1 med hensyn til egenandelskravet.	Fakultetet
5) Alle institutter skal tilby faglige mentorgrupper (2-3 personer med erfaring fra eksternfinansiering) som kan rådgi på søknadsplaner slik de framkommer i forskningsgruppens utviklingsplaner.	Instituttene
<b><i>Forskning for velferd, verdiskapning og omstilling</i></b>	
6) Fakultetet mener det skal være en del av vår forskningskultur at flest mulig søker mindre stiftelser/fond om driftsmidler (til forsknings-, innovasjons-, utdannings- og formidlingsprosjekter). Dette gir ekstra midler til drift i prosjekter, gir økt erfaring med søknadsskriving og virker positivt for CV-bygging med hensyn til å hente større midler.	Instituttene
7) Fakultetet utreder muligheten for jevnlig å kunne tilby formidlingskurs for ansatte, spesielt i de mest brukte formene p.t. som intervju, kronikk og populærvitenskapelige foredrag, men også andre aktuelle formidlingsformer.	Fakultetet
<b><i>Effektivt, mangfoldig og solid forskningssystem</i></b>	
8) Helsefak skal fortsette arbeidet med å bygge og utvikle en sterk forskningskultur innen toppforskning og breddesatsning. Helsefak vil undersøke ulike modeller som kan være nyttig i dette arbeidet, f.eks. «Researcher Career Wheel» og som gjør at alle kan «ta et steg til». Et undermål i dette er i større grad å inkludere UFF uten forskning i forskningsgruppens arbeid, på stillingskategoriens egne premisser.	Fakultetet
9) Helsefak skal ha en helhetlig rekrutteringspolitikk som ivaretar både forskningsambisjoner og undervisningskvalitet.	Fakultetet og instituttene
10) Helsefak skal ha en uttalt kultur for anerkjennelse av forskningsinnsats – f.eks. hvordan ansatte skal bli sett ved innsendelse av publikasjoner og søknader, tilbudt veiledning ved avslag, og ikke bare få anerkjennelse ved oppnådde resultater.	Fakultetet og instituttene

Gunbjørg Svineng  
dekan

—  
gunbjorg.svineng@uit.no

Saksansvarlig: Prodekan Morten Bøhmer Strøm

Saksbehandlere: Seniorrådgiver Marita Pedersen, seniorrådgiver Stian Røberg, seniorrådgiver Oliver Holman, rådgiver Elisabeth Leite Eriksen og rådgiver Marit Olsvik Opsahl

*Dokumentet er elektronisk godkjent og krever ikke signatur*

## Rapport forskning 2021

Det helsevitenskapelige fakultet

Seksjon for forskning, utdanning og formidling

30.9.2022



<b>Utgiver:</b>	Det helsevitenskapelige fakultet, UiT - Norges arktiske universitet
<b>Dato:</b>	September 2022
<b>Ansvarlig prodekan:</b>	Morten Bøhmer Strøm (prodekan forskning og innovasjon)
<b>Utarbeidet av:</b>	Stian Røberg, Marit Olsvik Opsahl, Oliver Holman, Elisabeth Leithe Eriksen og Marita Pedersen (prosjektleder)

## FORKORTELSER

AAM	Author's accepted manuscript
ABE-reformen	Avbyråkratiserings- og effektiviseringsreformen
AKM	Avdelingen for komparativ medisin
Andre-BoA	Bidrags- og oppdragsfinansiert aktivitet foruten EU og Forskningsrådet
BoA	Bidrag- og oppdragsfinansierte aktiviteter
Bufdir	Barne-, ungdoms- og familiedirektoratet
DIKU/SIU	Direktoratet for internasjonalisering og kvalitetsutvikling i høyere utdanning /Senter for internasjonalisering av utdanning
DOFI	Disclosure of invention
ERC	European Research Council
EU	European Union
FGL	Forskningsgruppeleder
FRIPRO	Program for banebrytende forskning, Forskningsrådet
HDir	Helsedirektoratet
HK-dir	Direktoratet for høyere utdanning og kompetanse
IFA	Institutt for farmasi
IH	Idrettshøgskolen
IHO	Institutt for helse og omsorg
IKM	Institutt for klinisk medisin
IKO	Institutt for klinisk odontologi
IMB	Institutt for medisinsk biologi
IPS	Institutt for psykologi
ISM	Institutt for samfunnsmedisin
IVP	Institutt for vernepleie
KD	Kunnskapsdepartementet
MSCA	Marie Skłodowska-Curie Actions
NFR	Forskningsrådet
PI	Prosjektleder (principal investigator)
PP	Publikasjonspoeng
RKBU	Regionalt kunnskapssenter for barn og unge, Nord
SANKS	Samisk nasjonal kompetansetjeneste
UFF	Undervisnings-, forsknings- og formidlingsstilling (Inkluderer stillingskategoriene dosent, forsker, førsteamanuensis, førstelektor, postdoktor, professor, professor II, stipendiat, amanuensis, høgskolelektor, høgskolelærer og universitetslektor)
UH-sektoren	Universitets- og høgskolesektoren
UiB	Universitetet i Bergen
UiO	Universitetet i Oslo
UiT	UiT - Norges arktiske universitet
UNN	Universitetssykehuset i Nord-Norge
WP-leder	Leder for arbeidspakke (work-package leader)

## INNHALDSFORTEGNELSE

---

1	OPPSUMMERING	4
2	RESULTATER	6
2.1	Undervisnings-, forsknings- og formidlingsstillinger	6
2.2	Søknadsaktivitet	6
2.3	Eksterne inntekter	12
2.4	Publisering, open access og allmenn- og brukerrettet formidling	16
2.5	Innovasjon	20
3	DISKUSJON	21
3.1	Har Helsefak høy kvalitet i forskning? (KD1)	22
3.2	Bidrar Helsefak til forskning for velferd, verdiskapning og omstilling? (KD2)	23
3.3	Har Helsefak et effektivt, mangfoldig og solid forskningssystem? (KD4)	24
4	FORSLAG TIL TILTAK	26
4.1	Overgang til ny strategi og veien videre	26
4.2	Nye tiltak for kvalitet i forskning (KD1)	26
4.3	Nye tiltak for forskning for velferd, verdiskapning og omstilling (KD2)	27
4.4	Nye tiltak for et effektivt, mangfoldig og solid forskningssystem (KD 4)	27
5	APPENDIX	28



# 1 OPPSUMMERING

---

I denne rapporten har vi tatt utgangspunkt i Kunnskapsdepartementets (KD) overordna mål for høyere utdanning og forskning, og har her vektlagt de tre målene som omhandler forskning: KD1) Høy kvalitet i utdanning og forskning, KD2) Forskning og utdanning for velferd, verdiskapning og omstilling, og KD4) Effektivt, mangfoldig og solid utdanningssektor og forskningssystem. I 2023 blir de nasjonale indikatorene erstattet av institusjonsvise indikatorer basert på universitetenes mål i egen strategi. Årets resultater diskuteres derfor i lys av UiTs nye strategi Eallju – drivkraft i nord<sup>1</sup>. Måltallene som ble satt for 2025 i forbindelse med strukturreformen er imidlertid uendret, og for UiT er dette 1,2 publikasjonspoeng per UFF, 365.000 kr. eksterne inntekter per UFF og 60% internasjonal sampublisering.

I strategien står det eksplisitt at vi «skal øke vår deltagelse i nasjonale og internasjonale konkurranseutsatte finansieringsordninger», og dette er et viktig premiss i årets rapport. Sammen med den økonomiske situasjonen i Forskningsrådet, UH-sektoren og for fakultetet spesielt (budsjettkutt og merkostnader) betyr dette at vi i enda større grad må gjøre strategiske prioriteringer for å nå disse målene. De eksterne inntektene blir enda viktigere for forskningsaktiviteten fremover, samtidig som vi også må bli mer bevisste på hvor vi søker midler fra, og hvor mye egenkapital vi kan stille i fremtidige prosjekter.

## Kvalitet i forskning (KD1)

Den økonomiske situasjonen i Forskningsrådet medfører at Helsefak må gjøre et skifte fra Forskningsrådet til EU og andre nasjonale og internasjonale konkurransearenaer for prosjekter som gir høy kvalitet og prestisje. Helsefak har hatt en vekst i EU-inntekter hele perioden, og har i 2021 en inntekt per UFF fra EU på 13.000 kr. Til tross for dette har vi enda en vei å gå for å nå måltallet for 2025, som er på 25.000 kr pr UFF. Det er behov for å jobbe strategisk for flere samarbeidssøknader i EU. Helsefak bør spesielt rette en innsats mot Mission Cancer, EUs største satsning innenfor helse.

Publikasjonspoengene ved fakultetet er på vei opp igjen, og er i 2021 0,99 pp pr UFF. Andelen internasjonal sampublisering er 57,5%, og Helsefak har rundt 40% av publiseringer på nivå 2, som tilsvarer fordelingen ved UiO og UiB. Helsefak vil fortsette tiltak fra fjorårets rapport for fortsatt økt publisering mot måltallet på 1,2 pp per UFF.

## Forskning for velferd, verdiskapning og omstilling (KD2)

Andre BoA-inntekter er vår største finansieringskategori (198 mill.kr.). Inntekten herfra går ned 7% i perioden, og antall innvilgede søknader i denne kategorien tilsier ikke økning framover. Inntektene fra Forskningsrådet har gått ned i perioden. Antall innvilgede søknader derfra økte i 2021 til 14, og det vil ha positiv effekt på inntekter i noen år framover. Målet fakultetet har hatt om å øke eksterne inntekter fra Forskningsrådet blir mer utfordrende i 2023 og 2024, pga 20% kutt i rammen til helseprogrammene<sup>2</sup>. For denne perioden bør andre større nasjonale og internasjonale kilder fra Andre-BoA kategorien også vurderes.

Instituttene som har aktiv styring av søknader for eksternfinansiering ser ut til å ha positiv utvikling av indikatorene, til dels uavhengig av hvilken tilnærming de har. I tillegg mener fakultetet det vil være nyttig å utarbeide mentormodeller for å ivareta av tilbakemelding på det faglige innholdet i søknadsskisser. Helsefak bør ha som mål at flest mulig søker de mindre stiftelsene; her er det lav innsats, stor læring og med mulighet for positiv tilsats til driftsøkonomien.

Åpen tilgang til Helsefaks publikasjoner er god. Allmenn- og brukerrettet formidling varierer noe fra år til år, og jamfør antall publikasjoner er potensialet for formidling stort. For å trygge de ansatte i formidlingsaktivitet, ønsker fakultetet å tilby formidlingskurs.

---

<sup>1</sup> <https://uit.no/om/strategi2030>

<sup>2</sup> <https://khrono.no/forskningsradets-rode-liste-disse-programmene-skal-kuttes-med-inntil-20-prosent/696228>



Selvrapportering viser at tjeneste-, produkt- og utdanningsinnovasjon alle er aktuelle i forskningsgruppene, for tiden rapporteres det mest innovasjon i utdanning. Over perioden er det en økning i antall sendte innovasjons- og utdanningssøknader ved Helsefak. Søknader om disse midlene utgjør ikke en stor andel av Helsefaks aktivitet, men innvilgelsesraten er høy. En sentral gruppe utarbeider for tiden handlingsplan for videre innovasjonsarbeid (UiT Talent). Helsefak vil basere egne tiltak på dette.

**Effektivt, mangfoldig og solid forskningssystem (KD4)**

Det er flere positive tegn til en mer aktiv holdning ved instituttene til søknadsarbeid og ekstern finansiering. Helsefak har de to siste årene sendt over 20 flere søknader per år enn tidligere i femårsperioden, veksten er i alle søknadsarenaene, og spesielt øker det til EU. Aktivitet per UFF har imidlertid ikke økt i og med at antall UFF-ansatte også øker, svak utvikling i eksterne inntekter reduserer også inntektene per UFF den siste femårsperioden. Helsefak må fortsette å bygge en sterk forskningskultur, og ha en rekruttering som ivaretar både forskningsambisjoner og undervisningskvalitet.

Konkrete tiltak er beskrevet i kapitel 4.

## 2 RESULTATER

### 2.1 UNDERVISNINGS-, FORSKNINGS- OG FORMIDLINGSSTILLINGER

I 2021 hadde Helsefak 752 UFF-årsverk, 71% av disse årsverkene hadde forskningsoppgaver som en større eller mindre del av sin stillingsbeskrivelse. I perioden fra 2017 til 2021 har det vært en 15% økning i antall UFF, samtidig er andel UFF med forskning som arbeidsoppgave stabil. Det er stor variasjon i kompetansesammensetningen blant vitenskapelige ansatte mellom instituttene. IHO har en reel vekst i andel UFF med forskning siden nedgangen i 2019 – for første gang har de over 60 ansatte med forskningsoppgaver.

Tabell 1 Undervisnings-, forsknings- og formidlingsstillinger (UFF)-årsverk med og uten forskningsoppgaver i stillingsbeskrivelsen

	UFF-årsverk total*					Antall UFF-årsverk forskning					Andel UFF-forskning**				
	2017	2018	2019	2020	2021	2017	2018	2019	2020	2021	2017	2018	2019	2020	2021
IMB	107	107	109	113	106	94	97	99	103	98	88%	91%	91%	91%	92%
ISM	91	85	92	93	98	83	76	82	83	90	91%	89%	89%	90%	92%
IKM	100	112	121	118	119	83	92	100	100	99	82%	82%	82%	85%	84%
IFA	44	49	55	56	55	42	47	52	53	51	96%	95%	96%	94%	94%
IKO	26	28	27	27	25	19	20	22	21	19	73%	73%	82%	77%	77%
IPS	61	62	70	65	72	52	50	58	54	60	84%	80%	83%	83%	83%
IHO	170	163	153	167	180	57	58	51	54	63	34%	35%	33%	33%	35%
IH		26	30	33	31		14	16	20	20		55%	55%	60%	63%
IVP		29	30	28	28		10	12	12	11		36%	41%	44%	40%
RKB	29	31	34	36	31	21	24	19	28	22	74%	77%	57%	76%	70%
Fakultetsnivå	8	8	7	7	8	5	4	4	4	5	61%	43%	52%	55%	58%
<b>Total</b>	<b>638</b>	<b>699</b>	<b>727</b>	<b>742</b>	<b>752</b>	<b>457</b>	<b>491</b>	<b>515</b>	<b>532</b>	<b>538</b>	<b>72%</b>	<b>70%</b>	<b>71%</b>	<b>72%</b>	<b>71%</b>

\*UFF-total = Dosent, forsker, førsteamanuensis, førstelektor, postdoktor, professor, professor II, stipendiat, amanuensis, høgskolelektor, høgskolelærer og universitetslektor

\*\* UFF-forskning = Dosent, forsker, førsteamanuensis, postdoktor, professor, professor II, stipendiat

### 2.2 SØKNADSAKTIVITET

I perioden 2017 til 2021 har Helsefak sendt 940 søknader og 268 av disse har blitt innvilget. Det betyr at det i snitt har vært sendt 188 søknader og innvilget 53 søknader per år, som gir en gjennomsnittlig innvilgelse på 28% over perioden. I 2021 ble det sendt 206 søknader, det er omtrent likt som i 2020, og med det har Helsefak de to siste årene sendt mer enn 20 flere søknader i året enn i de tre første årene i perioden. I 2020 så vi en nedgang i antall og andel innvilgede søknader, men denne øker igjen i 2021 og er nå på gjennomsnittet for perioden.

I denne perioden har antall søknader der Helsefak er samarbeidspartner økt, og utgjør i snitt 24% av søknaden vi sender. Det har ofte vært flere søknader med ukjent vurdering der vi er samarbeidspartner, men i 2021 har vi gode data også her og de viser at nesten en fjerdedel av innvilgede søknader er samarbeidssøknader.

Innvilgelsesprosenten i 2021 for samarbeidspartner-søknader er 33%, for PI/koordinator/WP-leder er innvilgelsesprosenten 26%.

#### 2.2.1 Fordeling av søknader og tilslag til EU, Forskningsrådet og andre

Tabell 2 viser at antall søknader til Forskningsrådet ble nesten doblet fra 2019 til 2020 etter en nær halvering av søknader til Forskningsrådet i 2019. I 2021 sender vi litt færre søknader igjen, men holder oss på nivået før 2019. I 2021 overdobles antall innvilgede søknader fra Forskningsrådet, og innvilgelsesprosenten går fra 8 til 25% fra 2020 til 2021. Søknader til EU er omtrent som de to foregående år, og til Andre-BoA (bidrags- og oppdragsfinansiert aktivitet foruten EU og Forskningsrådet) går det noe opp. Antall innvilgede søknader er stabilt over perioden, men for EU synker den litt i år fra de to tidligere år hvor vi så en liten vekst. I fjorårets rapport ble det lagt til en ekstra

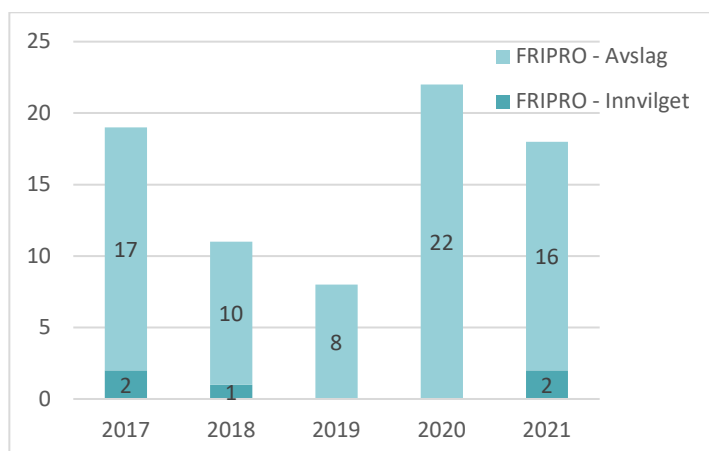
kategori, søknader på interne (UiT) konkurransemidler. I 2019 ble det sendt 10 slike søknader, mens det i 2020 ble sendt 17. I 2021 sendte vi 9 slike. Innvilgelsesprosenten øker i denne gruppen, og er i 2021 på 56%.<sup>3</sup>

Tabell 2 Antall søknader sendt og innvilget i 2017-2021

Finansieringskilde	Antall søknader sendt					Antall søknader innvilget					Andel søknader innvilget				
	2017	2018	2019	2020	2021	2017	2018	2019	2020	2021	2017	2018	2019	2020	2021
Forskningsrådet	56	55	32	63	56	7	8	7	5	14	13%	15%	22%	8%	25%
EU	15	10	20	21	21	3	2	7	4	2	20%	20%	35%	19%	10%
Andre-BoA	113	106	112	104	120	33	40	49	34	37	29%	38%	44%	33%	31%
UiT			10	17	9			3	8	5			30%	47%	56%
<b>Total</b>	<b>184</b>	<b>171</b>	<b>174</b>	<b>205</b>	<b>206</b>	<b>43</b>	<b>50</b>	<b>66</b>	<b>51</b>	<b>58*</b>	<b>23%</b>	<b>29%</b>	<b>38%</b>	<b>25%</b>	<b>28%</b>

\*3 søknader venter enda på svar (ERC Synergy Grant, World Cancer Research Fund og UiT-Aurora senter)

I 2020 brøt vi trenden fra de forrige årene med færre og færre FRIPRO-søknader, se figur 1. Det ble sendt litt færre søknader i 2021, men det er fremdeles et høyt antall sammenlignet med 2018 og 2019. Det ble sendt 18 FRIPRO-søknader som PI fra Helsefak. I 2021 fikk vi for første gang siden 2018 innvilget søknader i FRIPRO – to forskerprosjekt til IMB. I 2021 er det IFA, IKM, IMB, ISM og IPS som søker i FRIPRO. Det er i tillegg sendt tre søknader der vi er samarbeidspartner på søknaden.



Figur 1 Innvilgede og avslåtte søknader til FRIPRO, der søker er PI

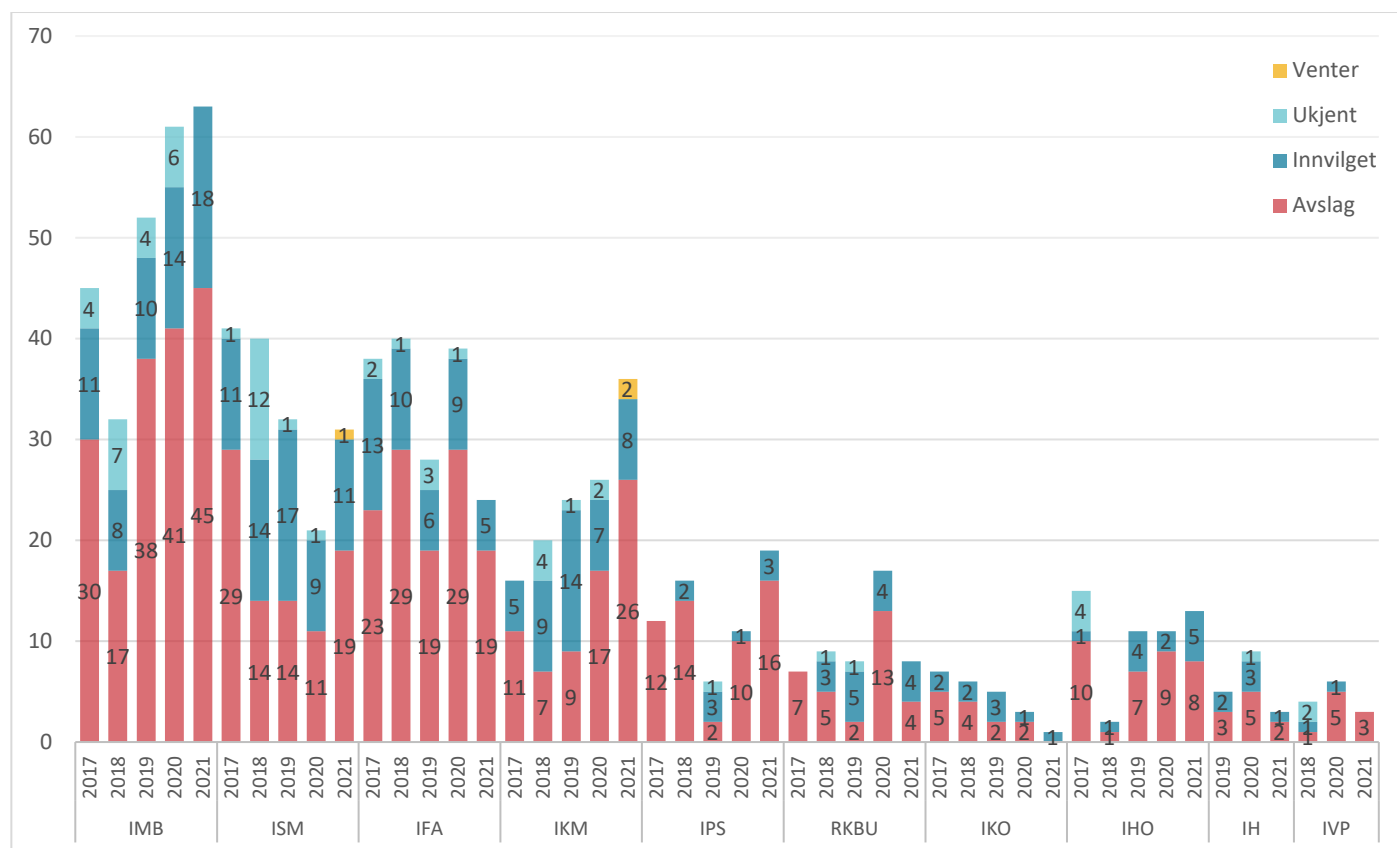
Søknadskilden Andre-BoA utgjør 58% av alle søknadene, av innvilgede søknader utgjør denne kategorien 64%. I Andre-BoA-kategorien inngår et stort antall ulike finansieringskilder. Helse Nord (36), Kreftforeningen (12), DIKU/SIU (7), Stiftelsen Dam (5), Odd Berg Gruppens Medisinske Forskningsfond (5), KG Jebsen (4) og Hdir (4) er de største kildene i denne kategorien i 2021. Over perioden er det sendt søknader til nærmere 100 ulike finansieringskilder under kategorien Andre-BoA. Innvilgelsesprosenten går enda litt ned, til 31%, men det er fremdeles her vi har flest innvilgede søknader (n=37). Søknader fra de siste tre årene viser også en økende aktivitet mot interne utlysninger, men litt færre søknader i 2021 enn de to forrige.

### 2.2.2 Sendt og innvilget – Instituttnivå

For fakultetet har det i denne perioden vært en målsetning om å øke antall søknader til EU og Forskningsrådet. Samlet har Helsefak de siste fem årene sendt 9% av søknadene til EU, 28% av søknadene til Forskningsrådet og 63%

<sup>3</sup> Til EU ble det i 2021 sendt 21 søknader totalt. Det ble sendt 9 søknader til bi- og multilaterale programmer. Til Horizon Europe ble det sendt 12 søknader, hvorav 2 MSCA søknader, 3 ERC (to PI og en WP-leder), og 7 søknader til Research and Innovation Actions (RIA) – fire som WP-leder, tre som samarbeidspartner. Det er to innvilgede søknader i EU-kategorien, et EEA Portugal Grants (bi- og multilateralt program) og ett RIA, der Helsefak er WP-leder. En ERC Synergy Grant søknad ved IKM er videre til steg to og avventer enda endelig vurdering. Det ble sendt 56 søknader til Forskningsrådet. Av disse var 23 sendt til FRIPRO (fire søknader ble sendt til fellesløftet, to til unge forskertalent og en til mobilitet, resten til forskerprosjekt), og det ble sendt 10 søknader om forskerprosjekt som PI, to som WP-leder og 8 som samarbeidspartner til ulike andre programmer. Det ble sendt fem søknader om innovasjon som PI og to som samarbeidspartner, en søknad om drift og en om PES-midler. Det ble sendt fem søknader om forskerskoler som samarbeidspartner og én skisse til etablering av senter for klinisk behandling som samarbeidspartner. I 2021 er det innvilget fem forskerprosjekt fra Forskningsrådet (én PI og fire samarbeidspartnere). Det er innvilget fem innovasjonsprosjekt (tre PI), en søknad om PES-midler og en søknad om drift, og to FRIPRO forskerprosjekt der Helsefak er PI.

av søknadene til Andre-BoA. I 2021 sendte Helsefak 27% til Forskningsrådet, som er på det jevne med øvrige år i perioden foruten 2019 da vi var nede på 18%. I 2021 er fordelingen av innvilgede søknader fra EU 3%. Innvilgede søknader fra Forskningsrådet utgjør 23% av alle innvilgede søknader, som er et meget godt resultat hele 8 prosentpoeng over gjennomsnittlig andel av innvilgede i perioden. Innvilgede søknader fra andre finansieringskilder utgjør da 74%, i dette er også søknader til sentrale virkemidler ved UiT. Tabell i appendiks viser fordelingen også for instituttene. Figur 2 viser antall søknader sendt og innvilget fordelt per institutt i perioden 2017-2021, alle kilder sett under ett.



Figur 2 Antall søknader pr år pr institutt - Innvilget og avslag. Avviste søknader er tatt ut av figuren, disse utgjør i 2021  $n=1$ . Søknader som på tidspunktet data ble hentet inn ikke har fått svar på søknaden vises som ukjent (2017-2020) og venter (2021). Søknader uten vurdering utgjør i 2021 1,5% ( $n=3$ ).

### 2.2.3 Søknadstyper

Det sendes flest søknader om forskerprosjekt over perioden, men likevel med en nesten halvering av antallet fra 2020 til 2021. Dermed ble det sendt 65 slike søknader – det laveste antallet i perioden og likt med 2019. Det ble sendt 34 forskersøknader under kategorien Andre-BoA, hvorav Helse Nord (8), Kreftforeningen (11), Kavli (3) og SANKS (2) er de største kildene. Det ble sendt 19 forskerprosjektsøknader til programmene i Forskningsrådet, og 12 til EU. Trenden vi har sett siden 2015 med at vi sender færre søknader i excellent-kategorien, ble snudd i 2020 og i 2021 sendes det også mange slike søknader. Det ble sendt totalt 25 slike søknader, 22 til FRIPRO<sup>4</sup> og tre til ERC<sup>5</sup>. I 2019 og 2020 så vi en nedgang i antall sendte mobilitetsstipend etter en periode med positiv utvikling fra 2015 til 2018, i 2021 er det tredje år på rad vi sender 6 mobilitetssøknader<sup>6</sup>.

Helsefak har flest innvilgede forskerprosjekt ( $n=15$ ) i 2021, men det er en nedgang fra foregående år. Etter forskerprosjekt har vi flest innvilgede søknader i kategorien «Driftsmidler» og «Innovasjon» (8 og 7 innvilgede

<sup>4</sup> hvorav 18 søknader til FRIPRO var som PI, to som WP-leder og tre som samarbeidspartner.

<sup>5</sup> hvorav to søknader til ERC var som PI, en som WP-leder.

<sup>6</sup> f.o.m. mars 2020 og gjennom store deler av 2021 har det vært store reiserestriksjoner ifbm korona-pandemien, som har påvirket muligheten til å planlegge for framtidige mobilitet utover landegrensene.

søknader). Av de innvilgede innovasjonsprosjektene er fem fra Forskningsrådet, tre som PI og to som samarbeidspartner. Helsefak har sendt 11 søknader om senterstatus, av disse er fem registrert som «skisse». Ingen fullskala søknader ble innvilget. Det er tre innvilget mobilitetsstipend i 2021, alle fra Helse Nord. I excellent-kategorien har vi etter tre år uten innvilgelse, fått tilslag på to søknader, som tidligere nevnt under avsnitt om FRIPRO.

Tabell 3 Antall sendt og innvilgede søknader etter hvilken type søknad det er snakk om, samt innvilgelsesprosenten i de ulike kategoriene

	Innsendt						Innvilget						Andel innvilget					
	2017	2018	2019	2020	2021	Tot	2017	2018	2019	2020	2021	Tot	2017	2018	2019	2020	2021	Tot
Forskerprosjekt	80	81	66	112	65	404	16	21	18	26	15	96	20%	26%	27%	23%	23%	24%
Ph.d./postdokstip.	32	28	32	13	38	143	4	7	13	3	4	31	13%	25%	41%	23%	11%	22%
Excellence	24	14	9	29	25	101	2	--	--	--	2	4	8%	0%	0%	0%	8%	4%
Driftsmidler	8	6	28	7	15	64	2	6	12	5	8	33	25%	100%	43%	71%	53%	52%
Utdanningsprosjekt	--	--	2	8	13	23	--	--	1	6	2	9	--	--	50%	75%	15%	39%
Senter	3	1	4	7	11	26	1	1	--	--	3	5	33%	100%	0%	0%	27%	19%
Innovasjon	1	1	3	2	8	15	--	1	2	1	7	11	0%	100%	67%	50%	88%	73%
Nettverk og arrang.	8	7	6	4	6	31	7	3	4	1	5	20	88%	43%	67%	25%	83%	65%
Oppdragsprosjekt	--	2	--	--	4	6	--	1	--	--	3	4	--	50%	--	--	75%	67%
Mobilitet	7	12	6	6	6	37	3	6	5	2	3	19	43%	50%	83%	33%	50%	51%
Infrastruktur	4	11	--	8		23	--	--	--	1		1	0%	0%	--	13%		4%
Annet	17	8	18	9	15	67	8	4	11	6	6	35	47%	50%	61%	67%	40%	52%
Total	184	171	174	205	206	940	43	50	66	51	58	268	23%	29%	38%	25%	28%	29%

## 2.2.4 Antall søknader pr UFF årsverk

Det er sendt 1,3 søknader pr UFF årsverk over hele perioden (2017-2021), eller 1,9 pr UFF årsverk med forskning<sup>7</sup>. Pr år sendes det i gjennomsnitt 0,4 søknader pr UFF årsverk med forskning. Det er ingen tegn til økt aktivitet. I 2021 var det registrert 116 unike søkere, det vil si at 15% av alle UFF-årsverk, eller 22% av UFF-årsverk med forskning, sendte en eller flere søknader. Det siste året er det 26 nye søkere, altså søkere som ikke tidligere (fom 2015) er registrert med en søknad. Samlet sett for hele perioden fra 2017-2021 har det vært totalt 264 unike søkere. Basert på et gjennomsnitt av antall UFF-årsverk for perioden vil det si at 37% av alle disse har søkt om ekstern finansiering på ett eller flere tidspunkt de siste fem årene. Ser man kun på UFF-årsverk med forskningsoppgaver er det litt over halvparten (52%) som er registrert med en eller flere sendte søknader. Se tabell 4.

Tabell 4 Søknadsaktivitet de siste fem år, pr UFF totalt og per UFF med forskningsoppgaver.

	2017	2018	2019	2020	2021	Tot/gj.snitt
Sendt søknader	184	171	174	205	206	940 <i>tot</i>
Innvilget søknader	43	50	66	51	58	268 <i>tot</i>
Innvilget til unike	35	44	52	42	44	140 <i>tot</i>
UFF-forsk	457	491	515	532	538	507 <i>snitt</i>
UFF årsverk	638	699	727	742	752	712 <i>snitt</i>
Innvilget pr UFF (unike)	5%	6%	7%	6%	6%	20% <i>tot</i>
Innvilget pr UFF-forsk (unike)	8%	9%	10%	8%	8%	28% <i>tot</i>
Innvilget pr UFF-forsk (ikke unike)	9%	10%	13%	10%	11%	53% <i>tot</i>
N søknader pr UFF	0,3	0,2	0,2	0,3	0,3	1,3 <i>tot</i>
N søknader pr UFF-forsk	0,4	0,3	0,3	0,4	0,4	1,9 <i>tot</i>
Unike søkere	110	105	104	118	116	264 <i>tot</i>
UFF-forsk m søknadsaktivitet	24%	21%	20%	22%	22%	52% <i>tot</i>
UFF m søknadsaktivitet	17%	15%	14%	16%	15%	37% <i>tot</i>
Nye søkere (beregnet fra 2015)	44	33	33	29	26	33 <i>snitt</i>

<sup>7</sup> Definisjon av UFF-årsverk med forskning: UFF forskning = Dosent, forsker, førsteamanuensis, postdoktor, professor, professor II, stipendiat.

Helsefak er PI<sup>8</sup> på 75% av søknadene sendt i 2021. Av de 116 unike søkerne, er det 67% som har sendt PI-søknader, 17% står oppført som samarbeidspartner og 16% har sendt søknader både som PI og samarbeidspartner. Dette er likt med tidligere år.

I femårsperioden fordeler søknadene seg på 120 mannlige søkere som til sammen har sendt 454 søknader og 143 kvinnelige søkere som til sammen har sendt 485 søknader. Over perioden er det en relativt lik andel søknader sendt av kvinner og menn når man ser på fakultetet som helhet. Når det gjelder antall sendte søknader i 2020 og 2021, år preget av korona-pandemien, viser tabellen under at ved IPS, IHO og IKO var det i 2020 en ganske stor negativ endring for kvinner, ved ISM og RKBUE for menn. Ved IMB og IFA var det en moderat negativ endring for kvinnene. I 2021 ser vi at IFA sender færre søknader totalt, og at andelen sendt av kvinner synker ytterligere, mens ved IMB er nivået oppe på gjennomsnittet før pandemien. Ved IPS nærmer andelen kvinner seg gjennomsnittet fra før pandemien, mens ved IKO er det ingen kvinner blant søkerne i 2020 og 2021, dog har de få søknader totalt disse årene. Ved ISM og RKBUE sender mennene færre søknader i begge pandemiårene enn det som var gjennomsnittet før pandemien. Ved IHO har andelen sendt av kvinner i 2021 steget 10 prosentpoeng over gjennomsnittet for perioden. Se tabell under.

Tabell 5 Andel innsendte søknader fordelt på kjønn i perioden 2015-2021.

Enhet	2015-2019		2020		2021	
	Gjennomsnittlig antall sendte søknader	Gjennomsnittlig andel søknader sendt av kvinner	Antall sendte søknader	Andel søknader sendt av kvinner	Antall sendte søknader	Andel søknader sendt av kvinner
IFA	31,8	45%	39	41%	24	33%
IH*	1	60%	9	67%	3	33%
IHO	7,6	76%	11	64%	14	86%
IKM	25,8	36%	26	35%	38	34%
IKO	6,4	25%	3	0%	1	0%
IMB	46	45%	62	40%	63	44%
IPS	14,4	60%	11	27%	19	53%
ISM	38,4	60%	21	86%	31	81%
IVP*	0,8	100%	6	67%	3	100%
RKBUE	7,8	54%	17	71%	9	78%
Total	180	49%	205	49%	205	52%

\*Har kun data fra 2019 (IH) og 2018/2019 (IVP)

Tabell 6 viser planlagte søknader som likevel ikke ble sendt inn. Her er det i hele perioden noen flere kvinner som trekker søknader enn menn. Samtidig stiger kvinnes andel i 2020 og 2021.

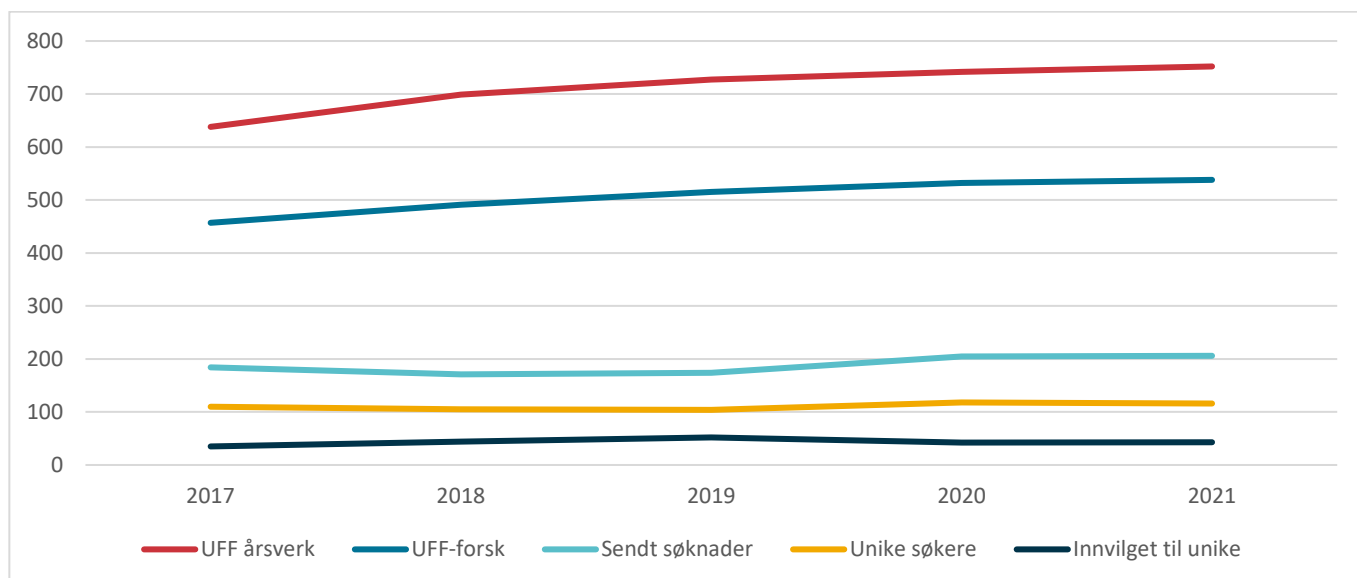
Tabell 6 Antall planlagte/påbegynte søknader som ikke ble sendt likevel, for perioden 2017-2021, total og fordelt på kjønn.

Enhet	2017		2018		2019		2020		2021	
	Total	%kv	Total	%kv	Total	%kv	Total	%kv	Total	%kv
IFA			2	100%	4	50%	1	0%		
IH							3	100%		
IHO							2	50%	1	100%
IKM	1	0%					1	0%	4	75%
IKO					7	14%			1	0%
IMB					2	50%	2	0%		
IPS							1	0%	2	50%
ISM	12	67%	4	50%	15	60%	15	93%	4	100%
IVP									1	100%
RKBUE							1	100%	2	50%
Total	13	62%	6	67%	28	46%	26	73%	15	73%

<sup>8</sup> Her regnet koordinator, PI og WP-leder samlet som PI vs. Samarbeidspartner.

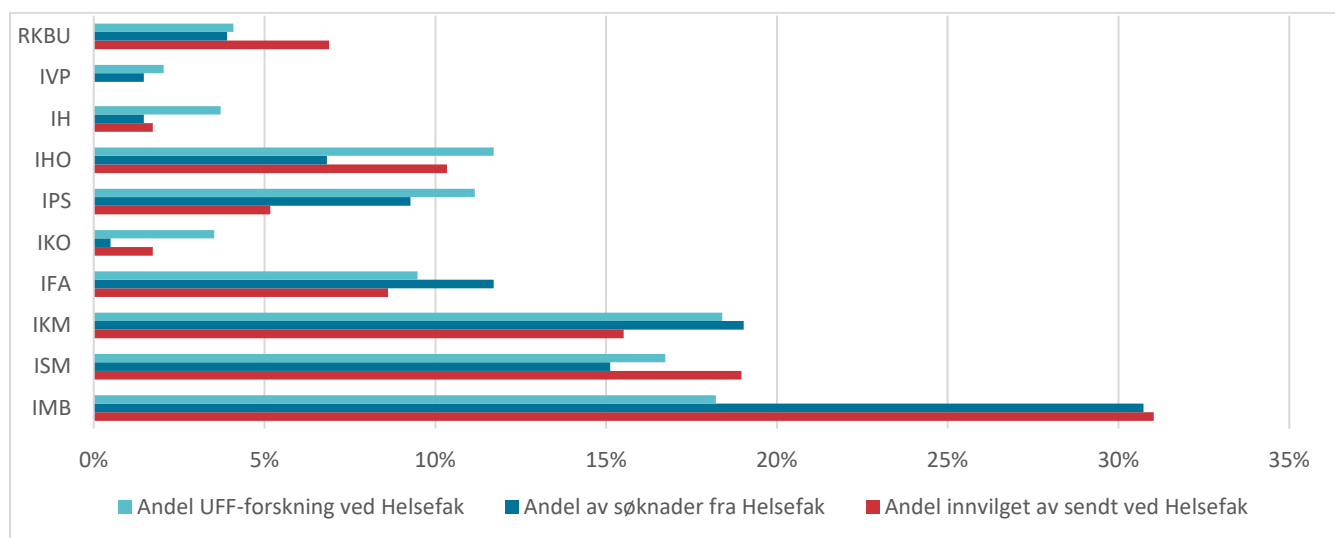
## 2.2.5 Andel innvilgede søknader pr UFF-årsverk

Det er innvilget 58 søknader fordelt på 44 unike søkere i 2021. Av alle UFF-årsverk er det dermed 6% som har oppnådd en form for ekstern finansiering av sin forskning i 2021, mens det samme tallet for UFF-årsverk med forskningsoppgaver er 8%. For hele perioden 2017-2021 er det innvilget 268 søknader fordelt på 140 unike søkere, dvs. at litt mer enn 1 av 4 forskningsansatte har fått ekstern finansiering til sin aktivitet den siste femårsperioden<sup>9</sup>. Ser man ikke på unike søkere, men alle søknader fordelt på alle UFF-årsverk med forskning er andelen 53% med innvilgede søknader. Figuren under viser hvor mange enkeltvis søkere det er pr år sammenlignet med antall UFF-total og UFF med forskningsoppgaver.



Figur 3 Antall UFF-årsverk pr år, UFF-årsverk som har forskning i sin stillingsbeskrivelse, antall sendte søknader totalt, antall unike søkere og antall unike søkere som har fått innvilget en eller flere søknader.

Figuren under viser forholdet mellom potensialet, innsats og resultat for eksternfinansiering. Den viser instituttens andel av UFF med forskning på Helsefak, hvor stor andel av søknadene som er sendt av de respektive instituttene, og instituttens andel av de innvilgede søknadene.



Figur 4 viser instituttens andel av UFF med forskningsoppgaver, andel av de sendte og innvilgede søknadene i 2021.

<sup>9</sup> Basert på gjennomsnittlig antall UFF årsverk med forskning i perioden 2017 til 2021.

## 2.3 EKSTERNE INNTEKTER

### 2.3.1 Inntektsutvikling Helsefak

Eksterne inntekter<sup>10</sup> (korrigert for prisutvikling) hadde toppår i 2019, med en nedgang 2020 og 2021. Fordi inntekt periodiseres inn i regnskapet når kostnader påløper, kan vi si at nedgangen skyldes lavere aktivitet i prosjektene enn foregående år. Ekstern finansiering som andel av total inntekt varierer i 5-årsperioden mellom 21% og 25%, og endte på 21% i 2021. Ekstern finansiering er under målet til KD av 25%.

Helsefak overførte drøye 14 mill. kr. i 2018 og drøye 5 mill. kr. i 2019 av interne midler til eksternt finansierte prosjekter, for å kompensere for merkostnader i forbindelse med stenging av Avdelingen for komparativ medisin (AKM). Denne overføringen forskyver periodisert inntekt med tilsvarende beløp. Fra 2020 har overføringer for å kompensere for merkostnader blitt gjort etterskuddsvis. Når egeninnsatsoverføringer gjøres i et annet år enn tilsvarende kostnader, blir periodisert inntekt forskjøvet. Ca. 3 mill. kr. av AKM merkostnader i 2021 blir dekt av egeninnsats i 2022, slik at 2021-tallet er 3 mill. kr. høyere enn det hadde vært hvis overføringen hadde funnet sted i 2021.

Tabell 7 Periodisert inntekt per finansieringskilde og andel ekstern finansiering av totale inntekter. Beløp i mill. kr. oppgitt i 2021-kroner

Kilde	2017	2018	2019	2020	2021
Forskningsrådet	45	27	42	38	34
EU	2	3	7	7	10
Andre-BoA	213	208	222	212	198
<b>Sum ekstern finansiering</b>	<b>260</b>	<b>238</b>	<b>270</b>	<b>257</b>	<b>242</b>
<b>Ekstern finansiering som andel av total inntekt</b>	<b>24%</b>	<b>21%</b>	<b>25%</b>	<b>22%</b>	<b>21%</b>

### 2.3.2 Inntektsutvikling på instituttnivå

Instituttene ved Helsefak har ulik utvikling av total ekstern inntekt. IMB opplevde et inntektsfall både i kroner og prosent fra 2020 til 2021. IMB er den største mottakeren av interne midler pga AKM-merkostnader i 2018 (ca. 8 mill. kr.) og 2019 (ca. 5 mill. kr.). Disse innbetalinger forskyver forbruk av eksterne inntekter, og kan forklare noe av nedgangen de opplevde fra 2017 til 2018 og noe av oppgangen fra 2018 til 2020. Eksterne inntekter i kroner hos ISM reduseres fra 73,7 til 59,6 mill. kr i 5-års perioden, mens som prosentandel har de økt fra 50% i 2017 til 51% i 2021 grunnet reduksjon av interne inntekter. Eksterne inntekter til sentre (57%) og Tromsøundersøkelsen (18%) utgjorde en stor andel av ISMs eksterne inntekter i 2021. Sett bort fra disse, hadde ISM en nedgang fra 19 mill.kr i 2020 til 15 mill.kr i 2021. IKM hadde den største økning fra 2018 til 2019 som var kontering av en stor gave fra Trond Mohn (ca. 24 mill. kr.). Sett bort fra denne gaven har IKM hatt en svak nedgang i ekstern finansiering. Gaven fra Trond Mohn er også en medvirkende faktor i at Helsefak som en helhet hadde toppår i 2019. RKBU snudde i 2020 sin nedgang, og er i 2021 nesten tilbake til nivået fra 2017. I 2021 er ca. 44 mill.kr. av RKBU 49,1 mill.kr. i periodiserte eksterne inntekter tilskudd fra Hdir og Bufdir<sup>11</sup>.

IFA skillet seg ut med en nokså jevn stigning i de eksterne inntektene fra 11,5 mill. kr. i 2017 til 20,3 mill. kr. i 2020, og er i 2021 kun 1,2 mill. kr under dette, med 19,1 mill. kr. IPS og IH hadde en negativ utvikling frem til 2019, men har opplevd en stor økning i både 2020 og 2021. IHO snudde også en negativ trend frem til 2020 med en stor økning av inntekter i 2021, fra 4,8 mill. kr til 13,2 mill. kr. IKO og IVP har en mindre andel eksterne inntekter enn resten av fakultetet, og mens IKO har hatt en positiv utvikling har IVP hatt en negativ utvikling.

<sup>10</sup> Eksterne inntekter inkluderer i tillegg til forskningsprosjekter, også ekstern finansiering av undervisningsprosjekter, infrastruktur og (bi)stillinger. Finansiering av sentre utenom Kunnskapsdepartement-finansiering telles også som eksterne inntekter.

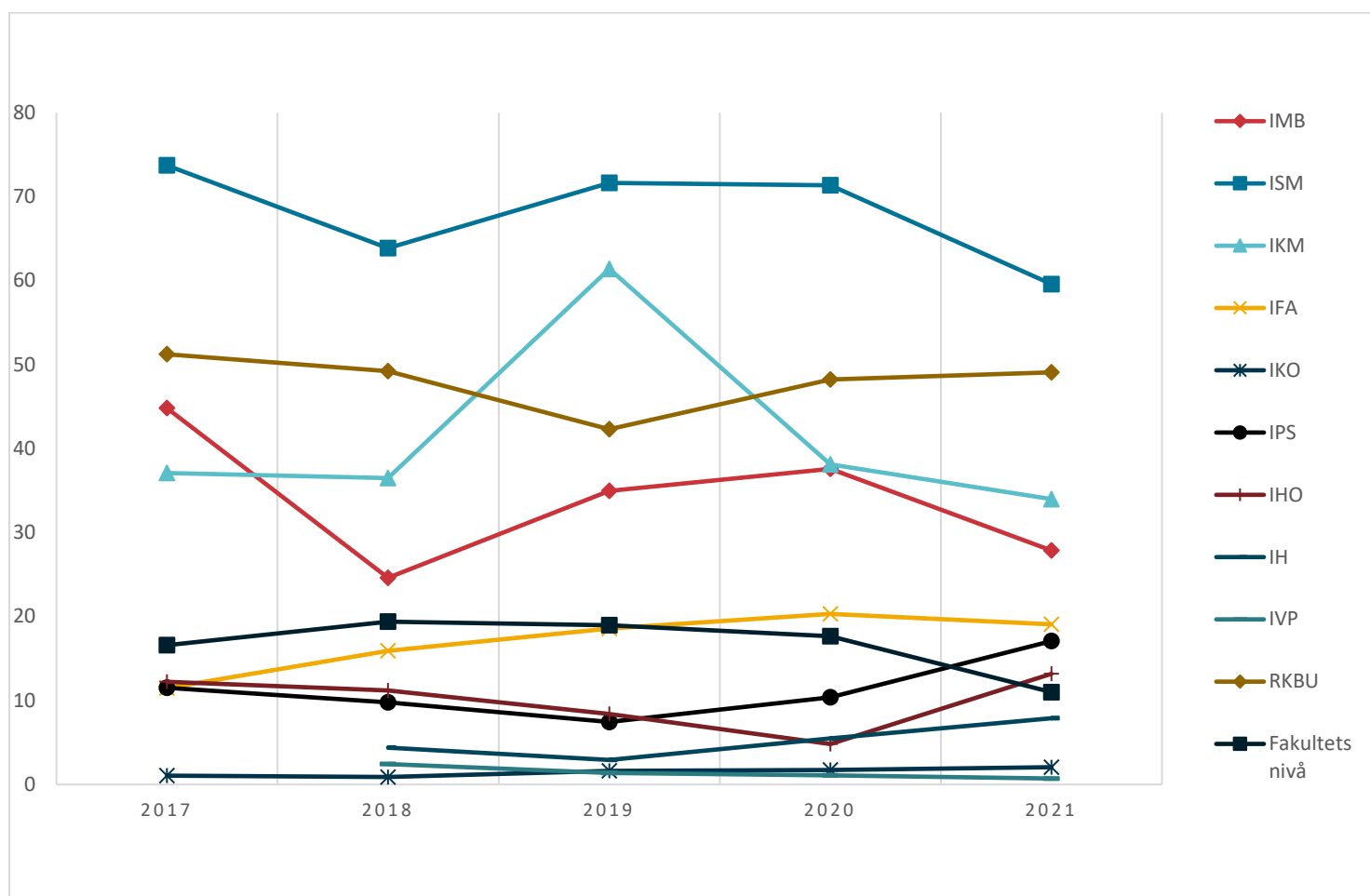
<sup>11</sup> Måltallet på 25% inkluderer også midler som ikke er konkurranseutsatt. Regnskapssystemet skiller ikke mellom konkurranse- og ikke konkurranseutsatte midler i kategorien Andre-BoA. Det vil derfor være en noe subjektiv vurdering av hvilke eksterne midler som kan regnes som konkurranseutsatt.



Tabell 8 Totale periodiserte eksterne inntekter per enhet. Beløp i mill. kr oppgitt i 2021-kroner.  
Eksterne inntekter som prosentandel av enhetens totale inntekter i parentes.

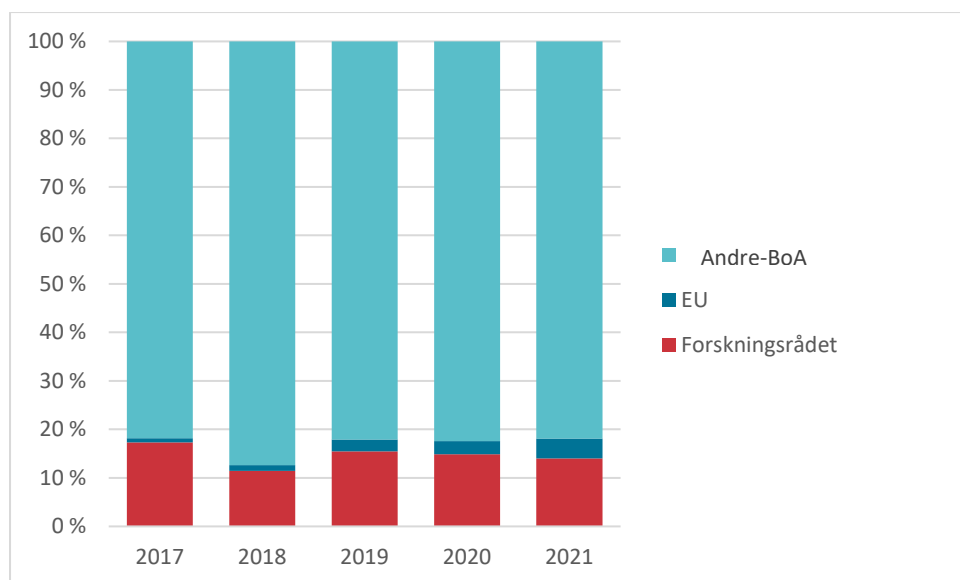
Institutt/enhet	2017	2018	2019	2020	2021
IMB	44,8 (29%)	24,6 (19%)	34,9 (25%)	37,6 (26%)	27,9 (20%)
ISM	73,7 (50%)	63,9 (50%)	71,7 (55%)	71,4 (51%)	59,6 (51%)
IKM	37,1 (34%)	36,5 (33%)	61,4 (42%)	38,1 (31%)	34,0 (29%)
IFA	11,5 (20%)	15,9 (25%)	18,6 (29%)	20,3 (32%)	19,1 (29%)
IKO	1,1 (1%)	0,9 (1%)	1,6 (2%)	1,7 (2%)	2,1 (3%)
IPS	11,5 (15%)	9,8 (12%)	7,4 (9%)	10,4 (12%)	17,1 (19%)
IHO	12,2 (7%)	11,2 (7%)	8,4 (5%)	4,8 (3%)	13,2 (7%)
IH		4,4 (16%)	2,9 (11%)	5,5 (18%)	7,9 (23%)
IVP		2,4 (8%)	1,4 (4%)	1,1 (3%)	0,7 (2%)
RKB	51,2 (92%)	49,2 (89%)	42,3 (84%)	48,2 (85%)	49,1 (88%)
Fakultetsnivå	16,6 (7%)	19,4 (8%)	19,0 (11%)	17,7 (7%)	11,0 (4%)
<b>Totalt</b>	<b>260 (24%)</b>	<b>238 (21%)</b>	<b>270 (25%)</b>	<b>257 (22%)</b>	<b>242 (21%)</b>

Figur 5 Ekstern finansiering i perioden 2017-2021 per enhet. Beløp i million kroner, oppgitt i 2021-kroner



### 2.3.3 Forskningsrådet og EU-kontrakter

Forskningsrådet og EU er satsningsområder for KD, og er dermed fremhevet i denne rapporten. I 2021 var andelen inntekt fra Forskningsrådet 14% og EU 4,1%. Andre-BoA, som også inkluderer andre prestisjetunge finansieringskilder (bl.a. Kreftforeningen), utgjør 81,9% av den totale eksterne finansieringen i 2021, se figur 6. Inntekt fra Forskningsrådet ved fakultet har hatt en negativ utvikling mens inntekt fra EU har hatt en positiv utvikling i hele perioden (se også tabell 4 ovenfor).



Figur 6 Andel av ekstern finansiering bevilget fra EU, Forskningsrådet og Andre-BoA, 2017-2021

IFA utmerker seg med hele 5,3 mill. kr. (av totalt 10 mill. kr.) periodiserte EU-inntekter i 2021, og har hatt en positiv utvikling hvert år siden 2017. IMB (1,5 mill. kr.), ISM (1,2 mill. kr.), IPS (1,1 mill. kr.) og IKM (0,9 mill. kr.) bidrar også med EU-inntekt til fakultetet. Inntekt fra EU vises ikke i egen tabell per institutt da omfanget er minimalt.

Helsefak har svingninger i inntekt fra Forskningsrådet over 5-årsperioden, med reduksjon fra 2020 til 2021, men høyere enn bunnår 2018. IMB og ISM hadde kraftig reduserte inntekter fra 2017 til 2018, stor økning til 2019/2020, med nytt fall i 2021. IFA har hatt en nokså høy andel Forskningsrådfinansiering siden 2018. IPS, som hadde et toppår i 2017 med 5,1 mill. kr Forskningsråd-inntekt, hadde en nedgang frem til 2021, men økte Forskningsrådsfinansiert aktivitet i 2021. IHO hadde en negativ utvikling frem til 2020 (registret negativ inntekt i 2020, altså ført inn mer egeninnsats enn aktivitet i prosjektene), men hadde 3,5 mill. kr av periodiserte inntekter i 2021, nesten like mye som toppår 2017.

Tabell 9 Periodiserte inntekter fra Forskningsrådet per enhet i perioden 2017-2021. Beløp i mill. kr, oppgitt i 2021-kroner

Institutt/Enhet	2017	2018	2019	2020	2021
IMB	17,6	4,4	12,0	14,3	8,9
ISM	11,7	5,3	13,6	12,0	7,6
IKM	2,2	2,3	2,2	3,6	4,0
IFA	2,9	5,0	5,4	5,0	4,7
IKO	0,0	0,0	0,1	0,2	0,0
IPS	5,1	4,0	3,1	1,1	3,5
IHO	4,6	2,8	2,5	-0,7	3,5
IH		0,3	0,0	0,0	0,0
IVP		1,4	0,9	1,1	0,4
RKBU	-0,1	0,0	0,0	0,0	0,0
Fakultetsnivå	1,1	2,2	2,1	2,1	1,0
<b>Totalt</b>	<b>45</b>	<b>28</b>	<b>42</b>	<b>39</b>	<b>34</b>

### 2.3.4 Ekstern finansiering per UFF-årsverk

Gjennomsnittlig ekstern inntekt per UFF er betydelig redusert de siste 5 årene. De medisinske instituttene, med høyt antall UFF (IMB = 106, ISM = 98 og IKM = 119) har en negativ utvikling av ekstern inntekt per UFF. IHO som har høyest antall UFF (180), har snudd en negativ trend og er tilbake til 2017 nivå, men nivået er fortsatt lavt i forhold til gjennomsnitt på fakultetet. IFA, IPS og IKO har økende ekstern finansiering per UFF i denne perioden. IVP viser en stor nedgang i inntekt per UFF siden de ble inkludert i 2018, mens IH etter en nedgang i 2019 har hatt en økning i 2020 og igjen i 2021.

Tabell 10 Ekstern finansiering per UFF, per enhet og samlet for Helsefak. Beløp oppgitt i 2021-kroner, avrundet til nærmeste 1000 kr

Institutt/Enhet	2017	2018	2019	2020	2021
IMB	418 000	231 000	320 000	333 000	262 000
ISM	808 000	753 000	778 000	772 000	606 000
IKM	370 000	325 000	506 000	322 000	286 000
IFA	260 000	323 000	340 000	362 000	350 000
IKO	41 000	32 000	59 000	65 000	83 000
IPS	188 000	159 000	106 000	159 000	238 000
IHO	72 000	69 000	55 000	29 000	73 000
IH	0	169 000	99 000	166 000	252 000
IVP	0	85 000	47 000	39 000	26 000
RKBU	1 767 000	1 609 000	1 244 000	1 325 000	1 569 000
Fakultetsnivå	2 023 000	2 308 000	2 747 000	2 717 000	1 429 000
<b>Gjennomsnittlig ekstern finansiering per UFF, Helsefak</b>	<b>407 000</b>	<b>341 000</b>	<b>371 000</b>	<b>346 000</b>	<b>321 000</b>

Tabellen under viser Helsefaks eksterne inntekter per UFF i 2021 sammenlignet med UiT, det nasjonale gjennomsnittet for UH-institusjoner, og måltall 2025. Inntekt per UFF ved Helsefak er lavere enn ved UiT som en helhet og det nasjonale gjennomsnittet for UH-sektoren. EU- og Forskningsrådsinntekt per UFF er lavere enn alle sammenligningsgrunnlag, mens inntekt fra Andre-BoA er høyere.

Tabell 11 Gjennomsnittlig ekstern finansiering i 2021 per UFF ved Helsefak, UiT og UH-sektoren totalt, mot måltall 2025, avrundet til nærmeste 1000 kr.

Finansieringskilde	Helsefak	UiT	Nasjonalt snitt UH-sektor <sup>12</sup>	Måltall 2025
Forskningsrådet	45 000	118 000	157 000	150 000
EU	13 000	28 000	34 000	25 000
Andre-BoA	263 000	186 000	164 000	190 000
<b>Totalt</b>	<b>321 000</b>	<b>332 000</b>	<b>355 000</b>	<b>365 000</b>

<sup>12</sup> Tall fra Tilstandsrapport for høyere utdanning 2022, rapport nr 9/2022, Direktoratet for høyere utdanning og kompetanse

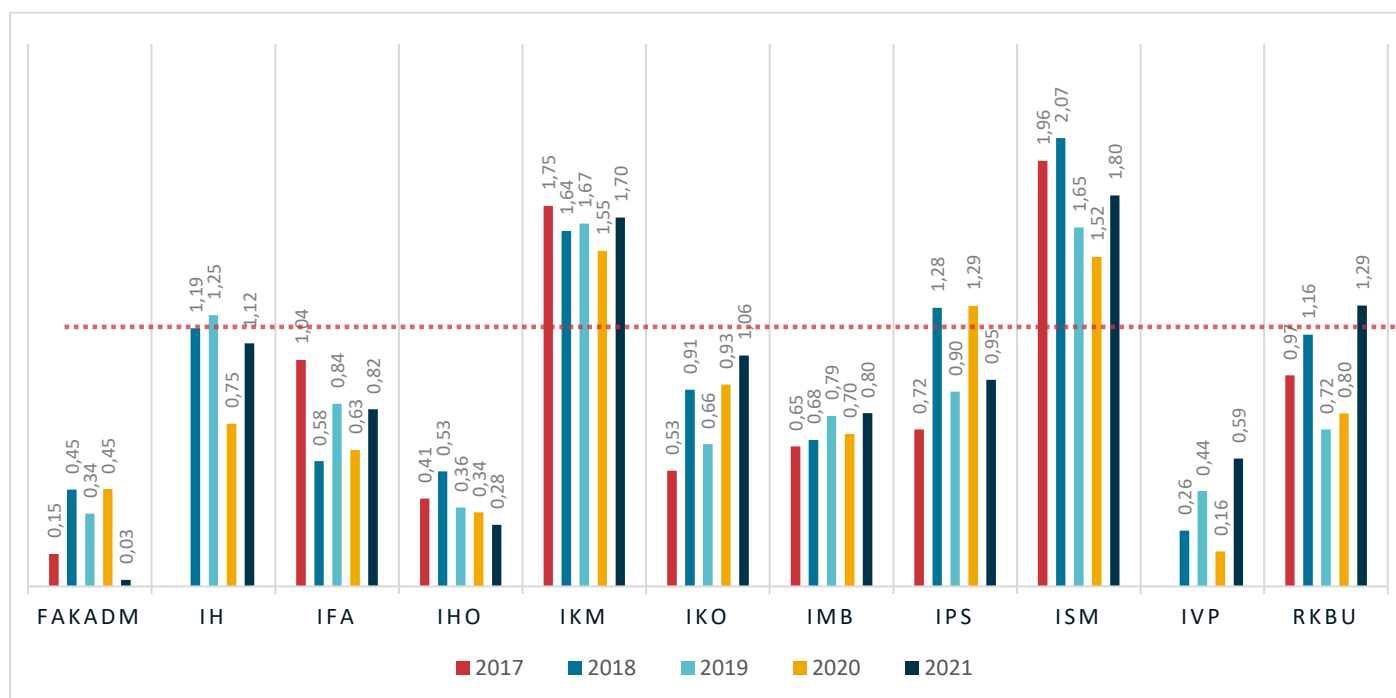
## 2.4 PUBLISERING, OPEN ACCESS OG ALLMENN- OG BRUKERRETTET FORMIDLING

I 2021 hadde Helsefak som helhet en solid økning i antall publikasjonspoeng (pp). Totalt oppnådde Helsefak 745 pp i 2021, og dette er et nytt toppår for fakultetet. Det har vært betydelige svingninger i fakultetets publikasjonspoeng i perioden: etter det siste toppåret med 723 pp i 2018, gikk antall publikasjonspoeng ned med rundt 30 pp hvert år i 2019 (698 pp) og 2020 (664 pp).

Når det gjelder rene publikasjonspoeng på instituttnivå, går åtte av ti institutter opp fra 2020. IKM og ISM har i flere år vært de to mestpubliserende instituttene på fakultetet, og etter en nedgang i 2020 er begge igjen på høyde med mestpubliserende år i perioden.

På lik linje med økt antall publikasjonspoeng, har også publikasjonspoeng per UFF økt på fakultetet som helhet. I 2021 lå tallet på 0,99 pp, som er en oppgang siden 2020 (0,9 pp). I femårsperioden har tallet vært på 0,98 (2017), 1,04 (2018) og 0,96 (2019). Fakultetet har likevel litt igjen før det når UiTs måltall på 1,2 pp per UFF årsverk.

Om vi ser på instituttene, er det i 2021 tre institutt som ligger over UiTs måltall per UFF årsverk (1,2 pp): ISM (1,80 pp), IKM (1,70 pp) og RKBU (1,29 pp), og ISM er igjen instituttet med flest publikasjonspoeng per UFF.



Figur 7 Oversikt publiseringspoeng per UFF total per institutt 2017-2021. Den stiplede linja viser UiTs måltall for 2025 (1,2 pp)

Utgledning av publikasjonspoeng per UFF kan gi et misvisende bilde av instituttene som har en stor andel undervisningsstillinger, siden UFF årsverk inneholder stillingskategorier som ikke har forskning som arbeidsoppgave, bl.a. førstelektor, høgskolelektor og universitetslektor.

Vi har derfor sett på utviklingen i UFF forskning når det kommer til publikasjonspoeng, der vi har delt antall publikasjonspoeng på andel UFF forskning ved instituttene. I denne oversikten ser vi at institutt som IHO får et oppsving, og med denne utgledning er IHO i 2021 med sine 0,80 publiseringspoeng per UFF forskning på nivå med både IFA (0,88) og IMB (0,86). Merk at UiTs måltall på 1,2 pp er satt for UFF total, og at vi her sammenligner publikasjonspoeng per UFF total med UFF forskning for å få et bilde på hvor langt unna vi er måltallet.

**Tabell 12 Publikasjonspoeng fordelt på undervisnings-, forsknings- og formidlingsstillinger (UFF)-årsverk med og uten forskningsoppgaver i stillingsbeskrivelsen**

	Publikasjonspoeng totalt					Publikasjonspoeng per UFF total*					Publikasjonspoeng per UFF forskning**				
	2017	2018	2019	2020	2021	2017	2018	2019	2020	2021	2017	2018	2019	2020	2021
IMB	69	72	86	79	85	0,65	0,68	0,79	0,70	0,80	0,73	0,74	0,86	0,76	0,86
ISM	177	171	150	139	175	1,96	2,07	1,65	1,52	1,80	2,13	2,25	1,82	1,67	1,94
IKM	175	184	203	183	202	1,75	1,64	1,67	1,55	1,70	2,11	2	2,03	1,83	2,04
IFA	46	28	46	35	45	1,04	0,58	0,84	0,63	0,82	1,09	0,59	0,88	0,66	0,88
IKO	14	25	18	25	27	0,53	0,91	0,66	0,93	1,06	0,73	1,25	0,81	1,19	1,42
IPS	44	79	63	84	68	0,72	1,28	0,90	1,29	0,95	0,84	1,58	1,09	1,55	1,13
IHO	69	86	55	57	51	0,41	0,53	0,36	0,34	0,28	1,21	1,48	1,08	1,05	0,80
IH	-	31	37	25	35	-	1,19	1,25	0,75	1,12	-	2,21	2,31	1,25	1,75
IVP	-	7	13	5	16	-	0,26	0,44	0,16	0,59	-	0,7	1,08	0,41	1,45
RKBU	29	35	25	29	40	0,97	1,16	0,72	0,80	1,29	1,38	1,46	1,31	1,03	1,81
Fakultets-nivå	1	4	2	3	0,2	0,15	0,45	0,34	0,45	0,03	0,2	1	0,5	0,75	0,04
<b>Total Helsefak</b>	<b>624</b>	<b>723</b>	<b>698</b>	<b>664</b>	<b>744</b>	<b>0,98</b>	<b>1,04</b>	<b>0,96</b>	<b>0,90</b>	<b>0,99</b>	<b>1,37</b>	<b>1,47</b>	<b>1,36</b>	<b>1,24</b>	<b>1,38</b>
<b>Total UiT</b>	<b>2011</b>	<b>2048</b>	<b>2112</b>	<b>2233</b>	<b>2360</b>	<b>0,99</b>	<b>0,98</b>	<b>0,97</b>	<b>1,01</b>	<b>1,03</b>	-	-	-	-	-

\*UFF-total = Dosent, forsker, førsteamanuensis, førstelektor, postdoktor, professor, professor II, stipendiat, amanuensis, høgskolelektor, høgskolelærer og universitetslektor

\*\* UFF-forskning = Dosent, forsker, førsteamanuensis, postdoktor, professor, professor II, stipendiat

I tillegg til at antall publikasjonspoeng, samt publikasjonspoeng per UFF øker, er forskerne våre også med på mange publikasjoner. Antallet har her økt fra 992 i 2020 til 1069 i 2021. Publikasjonene preges for en stor del av mange medforfattere og doble affiliasjoner, og dermed blir ikke poenguttellinga på det jevne med antallet publikasjoner. Internasjonalt medforfatterskap gjør likevel sitt til at Helsefak har en svakt stigende kurve med tanke på internasjonal sampublisering, der UiTs måltall for 2025 er 60%. Helsefak nådde i 2021 57,5%. På topp tre når det kommer til samarbeidspartnere finner vi Karolinska instituttet, Umeå universitet og London Imperial College.

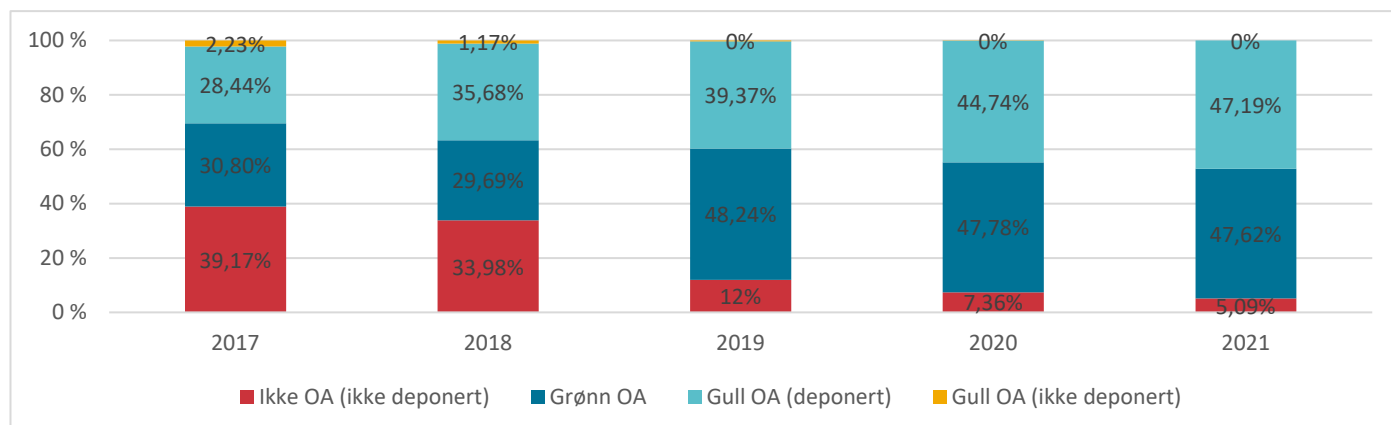
#### 2.4.1 Tilgjengeliggjøring av publikasjoner

Tilgjengeliggjøring av publikasjoner menes i denne sammenheng at vitenskapelige publikasjoner er lastet opp i UiTs egenarkiv, Munin. Forskeren er i hovedsak ansvarlig for at publikasjonen lastes opp i Munin, via Cristin. Dette betyr at en publisering som er gitt ut på forlag eller i tidsskrifter med åpen tilgang eller siste versjon av en vitenskapelig publikasjon (AAM, author's accepted manuscript), også skal gjøres tilgjengelig i et egenarkiv.

For 2020 var 92,6% av totalandelen av mulig opplastbare publikasjoner ved Helsefak lastet opp i Munin. For 2021 er dette gått opp til 94,91%, og fakultetet er på god vei til å nå målet om 100 % offentlig tilgjengelige publikasjoner.

Måltall fra KD tilsier at 100% av forskning finansiert av det offentlige skal være offentlig tilgjengelig. Dette ser ut til å ha nådd ut til forskerne, og samtidig har et fortsatt godt samarbeid mellom UB og superbrukere på de ulike fakultetene ved UiT gjort at vi har klart å få såpass mye egenarkivert. Rene open access-publikasjoner har for en stor del blitt lastet opp av UB eller superbruker, mens forfatterne har blitt bedt om å laste opp AAM selv eller sende disse

til UB/superbruker for opplasting. Dette gjelder da publikasjoner som ikke er rene open access, og hvor det ikke er mulig å laste opp publisert artikkel pga. copyrights.



Figur 8 Oversikt over OA-status for Helsefak 2017-2021

## 2.4.2 Allmenn- og brukerrettet formidling

Helsefak har en egen ordning med belønning for allmenn- og brukerrettet formidling, og på lik linje med vitenskapelig publisering brukes Cristin som system for å føre oversikt over antall formidlingsbidrag. De tellende kategoriene for dette er bl.a. intervju, kronikk, populærvitenskapelig foredrag, faglige artikler m.m.<sup>13</sup> Beløpet til fordeling ble vedtatt av fakultetsstyret i 2020, og ble satt til 1,2 millioner kroner for fordeling i 2021.

Antall formidlingsposter (tellende formidlingsbidrag som er registrert) har de siste årene variert, med en topp i 2019 på totalt 1243 poster. I 2020 gikk tallene nedover til 1051 poster, og i 2021 er det registrert 1020 tellende poster. Når det kommer til type tellende formidling som har blitt registrert, er det på fakultetet som helhet i 2021 en overvekt av intervjuer (36%), etterfulgt av faglig foredrag (15%), kronikk (15%) og populærvitenskapelig foredrag (9%).

På instituttnivå ser vi en variasjon av hvilken type formidling som registreres, der intervju, kronikk og faglig foredrag er på topp hos flere.

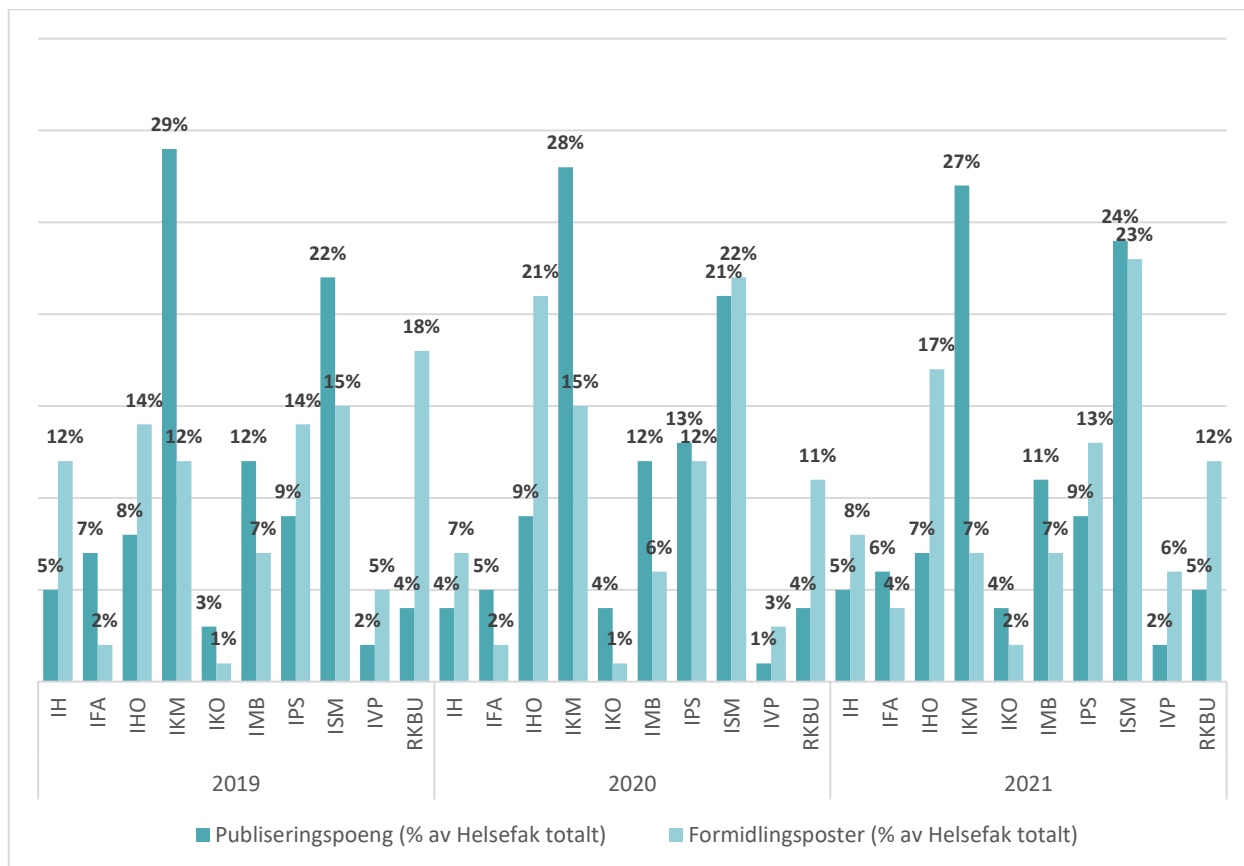
Tabell 13 Oversikt over de tre mest vanlige formene for allmenn- og brukerrettet formidling ved instituttene, samt prosentandel av type formidling.

Institutt/formidling	Andel	Institutt/formidling	Andel	Institutt/formidling	Andel
<b>RKB</b>		<b>IVP</b>		<b>IH</b>	
Intervju	46%	Intervju	35%	Intervju	43%
Faglig foredrag	14%	Popvit. foredrag	24%	Popvit foredrag	12%
Kronikk	9%	Popvit. artikkel	12%	Popvit artikkel	9%
<b>IFA</b>		<b>ISM</b>		<b>IHO</b>	
Faglig foredrag	41%	Intervju	52%	Kronikk	42%
Popvit foredrag	38%	Faglig foredrag	13%	Fagartikkel	11%
Fagartikkel	15%	Kronikk	10%	Faglig foredrag	11%
<b>IPS</b>		<b>IKO</b>		<b>IKM</b>	
Intervju	42%	Intervju	47%	Kronikk	20%
Popvit. foredrag	11%	Fagartikkel	18%	Intervju	16%
Faglig foredrag	11%	Kronikk	18%	Faglig foredrag og rapport	10%
<b>IMB</b>					
Intervju	38%				
Faglig foredrag	23%				
Popvit artikkel	13%				

<sup>13</sup> Om Helsefaks belønningsordning for allmenn- og brukerrettet formidling på Intranett: [https://intranett.uit.no/intranett/vis-artikkel/730381/belonningsordning\\_registrering\\_av\\_allmennrettet?p\\_dimension\\_id=88108&p\\_menu=42374](https://intranett.uit.no/intranett/vis-artikkel/730381/belonningsordning_registrering_av_allmennrettet?p_dimension_id=88108&p_menu=42374)

Om vi ser på andel registrerte, tellende formidlingsposter opp mot andel vitenskapelig publisering, kan vi få et bilde på om forskningen formidles eller ikke. I 2021 har IKM, IFA, IKO, IMB og ISM en større andel vitenskapelig publisering enn allmenn- og brukerrettet formidling. Forskjellen er aller størst ved IKM, som har 27 % av den vitenskapelige publiseringen og 7 % av den allmenn- og brukerrettede formidlingen. Det er ellers stor variasjon i hvor mye som formidles ved hvert institutt når vi sammenligner det med potensialet for formidling med utgangspunkt i det som publiseres av vitenskapelige artikler. Merk at formidlingspostene ikke bare inkluderer formidling av forskning, men også formidling av fagkunnskap, som for eksempel ekspertuttalelser i media.

Figur 9 Instituttene andel vitenskapelige publisering (publiseringspoeng) sett opp mot andelen av allmenn- og brukerrettet formidling (formidlingsposter)



## 2.5 INNOVASJON

Tallene for innovasjon er basert på innrapporterte DOFI til UiT sentralt, og selvrappoterer av aktivitet i forskningsgruppene fem år bakover i tid. Det er forskningsgruppeleder (FGL) som har svart på vegne av forskningsgruppene. Det varierer hvor lenge sittende FGL har vært leder i sin gruppe, og rapporteringen viser litt færre innovasjoner i de tre første årene. Vi har mottatt svar fra 36 av 69 forskningsgrupper, som vil si en svarprosent på 52%. Både det å huske alle tiltak tilbake fem år, og det å ikke ha vært FGL de årene, vil innvirke på underrapportering. Tabellen kan dermed ikke brukes til å vise utvikling over tid, men gir et bilde av hvilken type innovasjonsaktivitet Helsefak har.

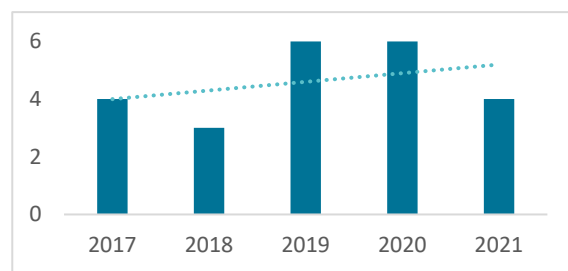
Innovasjon er en av UH-sektorens fire kjerneoppgaver, ved siden av forskning, utdanning og formidling. Innovasjon er nye eller forbedrede produkter, tjenester eller prosesser som tas i bruk og som gir økt verdiskaping og/eller samfunnsnytte. I UH-sektoren er FoU, utdanning og formidling fundamentet for innovasjon og samtidig midler for å fremme innovasjon.

Tabell 14 Svar på spørsmål om hvilke typer innovasjon som er aktuell for forskningsgruppen, med mulighet til å velge flere svaralternativer.

Aktuell innovasjonsform i FG	Antall FG	Andel av FG (%)
Tjenesteinnovasjon	17	47,2
Produktinnovasjon	15	41,7
Utdanningsinnovasjon	16	44,4
Annet	3	8,3

På spørsmål om hvilken type innovasjon som er aktuell i forskningsgruppen, med mulighet til å oppgi flere svar, er det 47% som oppgir tjenesteinnovasjon, 44% som oppgir utdanningsinnovasjon, 41% som oppgir produktinnovasjon og 8% som oppgir annen type innovasjon (intervensjonsstudier, forskningsmetode, etc.), se tabell 14.

I selvrappoterer av hvilken type innovasjon som er gjort de siste fem årene, rapporteres det om mest utdanningsinnovasjon (53%), dernest tjeneste innovasjon (34%), lavest selvrappotert er produktinnovasjon (13%). Selvrappotert Dofi fra 2021 stemmer ganske bra med registrerte Dofi (3 vs. 4), men bakover i tid er det større diskrepans. Kontinuerlig innhenting av data og større svarprosent vil kunne gjøre disse data mer kvalitetssikret. Se tabell 15 og figur 10.



Figur 10 Registrerte DOFI ved Helsefak pr år i perioden

Tabell 15 Etter-rapportert innovasjon ved Helsefak siste fem år

	2017		2018		2019		2020		2021		Total	
	N	%	N	%	N	%	N	%	N	%	N	%
<b>Tjenesteinnovasjon</b>												
Apper	1	9	1	9	1	5	2	7	1	2		
Behandling forebygging (endringer, skjema)	2	18	2	18	3	14	5	17	5	12		
Kvalitetsforebedrende	1	9	1	9	2	9	4	14	6	14		
Annet	0	0	0	0	0	0	1	3	1	2		
<b>Totalt</b>	<b>4</b>	<b>36</b>	<b>4</b>	<b>36</b>	<b>6</b>	<b>27</b>	<b>12</b>	<b>41</b>	<b>13</b>	<b>30</b>	<b>39</b>	<b>34</b>
<b>Produktinnovasjon</b>												
Dofi	1	9	0	0	2	9	1	3	3	7		
Patent	0	0	1	9	0	0	0	0	1	2		
Apper	0	0	0	0	0	0	1	3	0	0		
Lisens	0	0	0	0	0	0	0	0	0	0		
Annet	1	9	0	0	1	5	1	3	2	5		
<b>Totalt</b>	<b>2</b>	<b>18</b>	<b>1</b>	<b>9</b>	<b>3</b>	<b>14</b>	<b>3</b>	<b>10</b>	<b>6</b>	<b>14</b>	<b>15</b>	<b>13</b>
<b>Utdanning</b>												
Undervisningsformer	3	27	3	27	5	23	5	17	6	14		
Undervisningsmetoder	1	9	1	9	4	18	4	14	6	14		
Digitalisering/fleksibilisering	1	9	1	9	3	14	4	14	9	21		
Annet	0	0	1	9	1	5	1	3	3	7		
<b>Totalt</b>	<b>5</b>	<b>45</b>	<b>6</b>	<b>55</b>	<b>13</b>	<b>59</b>	<b>14</b>	<b>48</b>	<b>24</b>	<b>56</b>	<b>62</b>	<b>53</b>



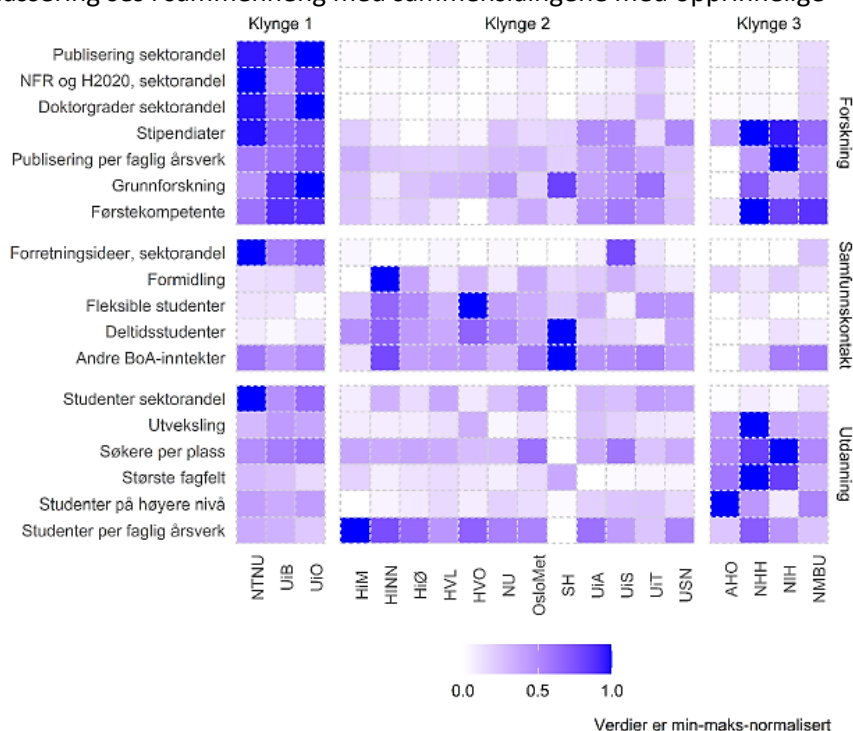
### 3 DISKUSJON

UiT og Helsefak sitt oppdrag for forskning fra Kunnskapsdepartementet (KD) er at vi skal ha høy kvalitet i forskning (KD1), gjøre forskning for velferd, verdiskaping og omstilling (KD2) og at det skal være et effektivt, mangfoldig og solid forskningssystem (KD4).

Året 2022 er siste år hvor KDs mål består med denne utformingen. Fra og med 2023 vil de nasjonale målene for sektoren være 1) Høy kvalitet i utdanning og forskning, 2) Bærekraftig samfunnsutvikling, velferd og innovasjon og 3) God tilgang til utdanning og kompetanse i hele landet. Dagens mål 4 vil bli lagt til utviklingsavtalene og økonomiregelverket<sup>14</sup>. Nasjonale indikatorer vil da også bli avvirket til fordel for institusjonsvise indikatorer basert på universitetenes mål i egen strategi. Disse indikatorene skal stadfestes i universitetets utviklingsavtale, og er p.t. ikke avklart. I årets rapport bruker vi derfor enda de nasjonale indikatorene, men vi vil i stor grad diskutere resultatene opp mot ny strategi, dette også med tanke på ny handlingsplan som skal utformes for fakultetet.

En av hovedargumentasjonen for denne endringen i mål og indikatorer er at regjeringen ønsker å sikre mangfold, tydelige institusjonsprofiler og bedre arbeidsdeling i sektoren. I den forbindelse ble det i årets «Tilstandsrapport for høyere utdanning» gjort en klyngeanalyse av mangfoldet i sektoren. De identifiserte tre klynger, klynge 1: de forskningsintensive, klynge 2: institusjonene med høy samfunnskontakt og klynge 3: de utdanningsintensive.

HK-dir skriver i rapporten at UiT savnes i klynge 1 blant de opprinnelige universitetene. Variablene de har brukt, plasserer UiT sammen med nåværende og tidligere høyskoler i klynge 2. De størrelsesbaserte forskningsvariablene som vises i de tre øverste radene i diagrammet, gjør at UiT plasseres nærmere de andre institusjonene i klynge 2 enn de gamle universitetene i klynge 1. UiTs plassering ses i sammenheng med sammenslåingene med opprinnelige høyskoler. Samtidig viser den mørkere fargen for UiT på variablene for forskning at UiT skiller seg noe ut fra de øvrige i klynge 2. HK-dir påpeker at UiT er blant de institusjoner som har vært vanskeligere for algoritmene å plassere i klynger enn andre. Likevel er det interessant å ta med seg dette i diskusjonen av resultatene for Helsefak, som utgjør rundt 40% av UiT, og som har fått inn mange av profesjonsfagene etter fusjonene. Figur 11 viser klyngeanalysen fra Tilstandsrapporten<sup>15</sup>.



Figur 11 Klynger i UH-sektoren basert på institusjonsvise verdier innen forskning, samfunnskontakt og utdanning. Hentet fra «Tilstandsrapport for høyere utdanning 2022», utarbeidet av ideas2evidence for HK-dir<sup>15</sup>.

Fjorårets resultat og evt. tiltak må også ses i sammenheng med en endret økonomisk situasjon for sektoren som helhet, og for fakultetet spesielt. Regjeringen innfører i budsjettåret 2022 et pensjonskutt, og reduserer tildelingen pga. endrede reisevaner. Dette kommer i tillegg til det allerede pågående ABE-kuttet og økt intern husleie. For Helsefak må også merkostnader på 40 millioner i forbindelse med stengingen og forsinkelsen ved AKM dekkes inn i perioden 2023-2025. Dette betyr i hovedsak kutt i fakultetets

<sup>14</sup> [Sektormål for universiteter og høyskoler og rammeverk for utviklingsavtaler](#)

<sup>15</sup> [Tilstandsrapport for høyere utdanning 2022](#) og [variabeloversikt til klyngeanalyse](#)

strategiske midler og muligheter til å støtte aktiviteter ved instituttene. Høsten 2022 vil vi måtte jobbe med omstillinger, og eksterne inntekter blir viktigere enn noen gang. Oppi dette har regjeringen varslet og satt i gang en gjennomgang av Forskningsrådets økonomi, og det har gått ut melding om at tildelinger framover vil bli redusert med 20%, samt at FRIPRO stoppes helt i 2023, og muligens lengre. Bildet for hvor vi søker, og hvor mye egenkapital vi kan stille vil derfor være i endring i tiden framover.

### 3.1 HAR HELSEFAK HØY KVALITET I FORSKNING? (KD1)

Publikasjonspoeng per UFF viser omfang og kvalitet på vitenskapelig publisering, mens deltakelse i EU antas å gi økt kvalitet i norsk forskning<sup>16</sup>. Tilslag i ERC og FRIPRO sier noe om hvor mange internasjonalt ledende forskere, eller forskere med potensiale til å bli internasjonalt ledende, fakultetet har. Internasjonalt samarbeid regnes som kjennetegn på god kvalitet i forskningen, derfor er internasjonal mobilitet en ønsket politikk for å få fram samarbeid og sier noe om forventet framtidig kvalitet ved fakultetet. Det samme gjelder internasjonal sampublisering.

#### 3.1.1 Et nødvendig skifte fra Forskningsrådet til EU og andre nasjonale og internasjonale konkurransekilder

Det er liten sannsynlighet for at vi vil nå måltallet for inntekt fra Forskningsrådet med de inntektsreduksjoner de har varslet. Fakultetet blir nødt til å se på alternative strategier for innhenting av eksterne toppmidler. Kutt i bevilgningsøkonomien til sektoren betyr at eksternfinansiering blir enda viktigere enn før for å opprettholde aktiviteten. I tillegg til den direkte inntekten utgjør resultatbaserte tildelinger for doktorgrader, publisering og BoA-inntekter i 2022 ca. 35 mill. kr. Den største andelen kommer fra doktorgrader (16 mill. kr), publisering (10 mill. kr) og andre-BoA (12 mill. kr). Resultatbasert finansiering i internøkonomien utløst av Forskningsrådsmidler utgjør 3 mill. kr. og utløst av EU-midler 4 mill. kr. EU-midler er relativt godt belønnet og burde prioriteres når Forskningsrådsmidler blir vanskeligere å få. All økning på resultatbaserte tildelinger øker handlingsrommet i bevilgningsøkonomien til fakultetet og instituttene. Det bør likevel påpekes at status for resultatbasert omfordeling er usikker etter at «Finansieringutvalget» har foreslått å fjerne disse i sin rapport om «Finansiering av universiteter og høyskoler»<sup>17</sup>

Helsefaks resultater i 2021 med økte midler fra EU, økt internasjonal sampublisering og tildeling av FRIPRO-søknader burde legge til rette for at Helsefak skal kunne vri enda mer aktivitet mot EU de neste årene. I følge UiTs strategi for 2030 skal vi «utvikle flere ledende fagmiljøer i front av den internasjonale kunnskapsutviklingen. Vi skal løfte forskningsspørsmål som er relevante for utviklingen i nord. Vi skal utvikle og opprettholde vitenskapelig infrastruktur og tidsserier av data som muliggjør kunnskapsutvikling om og for Arktis og nordområdene». Miljøer som kan nå opp i EU-systemet bør motiveres til å søke; spesielt de som har hatt MSCA-finansiering de siste årene, eller andre EU-midler. Helsefak har også flere enkeltindivider som kan nå opp i MSCA og ERC, som bør være en del av inntekten framover. Det er behov for å jobbe strategisk mot å få opp miljøer som kan delta i større samarbeidssøknader i EU, og aller helst koordinere EU-prosjekter. Helsefak har en relativt høy prosentandel (57.5%) internasjonal sampublisering, og har dermed et nettverk å jobbe ut fra. Andre internasjonale og nasjonale prestisjetunge arenaer, og andre nasjoners forskningsråd i samarbeidssøknader er aktuelt å utnytte i større grad. Spesielt vil en satsning mot Mission Cancer i EU kunne utløse tildeling fra Kreftforeningen ved gjenbruk av gode søknader som ikke oppnår finansiering fra EU, men som oppnår «seal of excellence». Kreftforeningen har også signalisert regionale midler som kan øke innvilgelsesprosenten til UiT. Interne midler for mobilitet bør styrkes og fortsatt prioriteres til opphold som vil føre til EU-søknader. Fakultetet vil også arbeide aktivt med å følge opp tiltaksområdene i UiTs ambisjonsnotat for Horisont Europa (2021-2027)<sup>18</sup>, her står det at deltakelse i Horisont Europa skal «integreres i fakultetenes strategier, og forventningene skal være forankret i relevante forskningsgrupper på instituttnivå». Dette skal følges opp i samarbeid med instituttene. Mobilitet er viktig for å nå opp i fri forskningsstøtte, men her er aktiviteten dessverre ikke tatt seg opp etter pandemien. Rektoratet utarbeider for tiden en handlingsplan for mobilitet (sak 28/22 - felles

<sup>16</sup> DIKU - Tilstandsrapport for høyere utdanning 2020

<sup>17</sup> <https://www.regjeringen.no/no/dokumenter/finansiering-av-universiteter-og-hoyskoler/id2904847/>

<sup>18</sup> [UiTs ambisjonsnotat for Horisont Europa](#) (ephorte 2021/1815)

Forskningsstrategisk utvalg (FSU) 30.8.2022). Handlingsplanen skal styrebehandles i november 2022 og blir viktig å følge opp for Helsefak.

## 3.2 BIDRAR HELSEFAK TIL FORSKNING FOR VELFERD, VERDISKAPNING OG OMSTILLING? (KD2)

Inntekt fra Forskningsrådet er en indikator på forskningskvalitet gjennom evne til å vinne frem i nasjonale konkurranser om forskningsmidler<sup>19</sup>. Forskningsrådets programmer er også rettet mot å løse samfunnsutfordringer, og nivået på finansiering fra Forskningsrådet sier dermed noe om både kvalitet og formål for forskningen. Bidrags- og oppdragsfinansiert aktivitet utenom Forskningsrådet og EU (andre-BoA) er en indikasjon på samspillet med omverdenen. Åpen tilgang til forskningsartikler sikrer bedre kunnskapsutvikling og mer bruk av kunnskap ved at forskersamfunnet i sin helhet, profesjonelle brukere i arbeids- og næringsliv og allmenheten får del i resultatene fra forskning. Allmennrettet formidling er en forlengelse av dette. I årets rapport har vi også definert innovasjon som en del av dette målet.

### 3.2.1 Behov for å legge ny strategi for eksterne inntekter framover

Andre BoA-inntekter er fremdeles vår største finansieringskategori (198 mill. kr.), men den går ned 7% i perioden. En økning i antall innsendte søknader har ikke gitt flere innvilgede til nå, men gir et potensial for økt tilslag framover ved å forbedre og sende inn søknader på nytt. I 2021 økte antall innvilgede søknader i Forskningsrådet fra fem til 14, som vil ha innvirkning på inntekter derfra i noen år framover. Målet fakultetet har hatt om å øke eksterne inntekter fra Forskningsrådet blir mer utfordrende i 2023 og 2024, der det er vedtatt 20% kutt i rammen til helseprogrammene<sup>20</sup>. Det bør likevel være et mål å opprettholde dagens nivå. For denne perioden bør andre større nasjonale og internasjonale kilder fra Andre-BoA kategorien vurderes i tillegg. Denne strategien ble også diskutert under Arendalsuken 2022, og i Khrono<sup>21</sup> deles en liste over de 20 største stiftelsene som finansierer forskning. En ytterligere gjennomgang av aktuelle stiftelser og fond bør gjøres i miljøene, i appendiks listes de mest søkte kildene i andre-kategorien for Helsefak. Det kan vurderes om Helsefak skal ha som mål at flest mulig ansatte skal søke de mindre stiftelsene; her er det lav innsats, stor læring og med mulighet for positiv tilsats til driftsøkonomien.

### 3.2.2 Åpen publisering og allmenn- og brukerrettet formidling

Åpen tilgang til forskningspublikasjoner fortsetter å øke ved Helsefak, kun 5% av publikasjonene er ikke blitt deponert i 2021. Målet er at alle publikasjoner skal være åpent tilgjengelig innen 2024<sup>22</sup>. Helsefak har siden 2019 sendt melding til forskerne om å deponere publikasjonene sine i Cristin i forbindelse med Cristin-rapporteringen. Vi ser markant økning i deponering etter denne rutineendringen. UiT har vært langt fremme i dette arbeidet, og Forskningsrådet har innført krav om deponering av forfatters aksepterte manuskript fra og med 2022. I tillegg har andre institusjoner, for eksempel UNN/Helse Nord, begynt å innhente de aksepterte manuskriptene. Det har dermed blitt bedre kjent blant forskerne at de må ha disse tilgjengelig. Open Access har også blitt stadig mer aktuelt i den vestlige verden og det er stor mulighet for å nå målet om 100% åpen publisering.

Det er stor variasjon mellom instituttene når det kommer til registrerte og tellende formidlingsposter. Det er også stor variasjon når vi sammenligner potensialet for allmenn- og brukerrettet formidling med utgangspunkt i vitenskapelige publikasjonspoeng. Dette synliggjør et potensial for økt formidlingsaktivitet. For å øke allmenn- og brukerrettet formidling ved fakultetet kan formidlingskurs for ansatte være nyttig, for eksempel intervjuutrustning og kronikkskriving.

### 3.2.3 Liten, men god aktivitet innen innovasjon

Søknader om innovasjonsmidler, hhv. innovasjonssøknader og utdanningssøknader, utgjør ikke en stor andel av Helsefaks søknadsaktivitet (4%), men kvaliteten synes bra med en høy innvilgelsesrate på henholdsvis 73% og 39%.

<sup>19</sup> DIKU – Tilstandsrapport for høyere utdanning 2020

<sup>20</sup> <https://khrono.no/forskningsradets-rode-liste-disse-programmene-skal-kuttes-med-inntil-20-prosent/696228>

<sup>21</sup> <https://khrono.no/forskningen-ser-mot-private-for-a-lose-finansieringsbehov/710674>

<sup>22</sup> 2021/5912 Prinsipper for åpen tilgang til vitenskapelige publikasjoner ved UiT

Forskningsgruppene selvrapportering gir en indikasjon på hvilken innovasjon som gjøres ved fakultetet. Fram til nå har Dofi (produktinnovasjon) vært eneste tellekant ved UiT, men svarene på fakultetets undersøkelse gir et bilde av at innovasjon i utdanning og tjeneste er mer utpreget ved Helsefak. Det betyr at Helsefak må ha en bred innfallsvinkel til framtidig strategisk innovasjonsarbeid. I UiTs strategi<sup>23</sup> behandles innovasjon særlig under «De store samfunnsutfordringene». Der står det at vi skal «legge til rette for innovasjon og samskaping internt og med samfunnet rundt oss» gjennom å «Fremme tverrfaglighet, samskaping og innovasjon [og] skape arenaer og fjerne barrierer for samarbeid på tvers av fagområder, sektorer og landegrenser. Vi skal prioritere og dra nytte av mulighetene i digital omstilling (...)». Det er nærliggende å tenke på UNN, de øvrige helseforetakene i Helse Nord og primærhelsetjenestene i kommunene i vårt nedslagsfelt, som viktige partnere der vi må skape ytterligere arenaer for innovasjonsprosjekter. Det gjøres for tiden et sentralt arbeid som ser på hvordan UiT skal jobbe videre med innovasjonsarbeidet (UiT Talent). Helsefak vil følge opp dette og avventer å foreslå egne tiltak for videreutvikling av området i årets rapport.

### 3.3 HAR HELSEFAK ET EFFEKTIVT, MANGFOLDIG OG SOLID FORSKNINGSSYSTEM? (KD4)

Aktiviteten og resultatene som oppnås fordelt på de vitenskapelige ansatte (UFF) med forskningsoppgaver sier noe om hvor godt rustet Helsefak er til å nå de forventninger som vårt eierdepartement har til oss. Vi har i årets rapport i tillegg undersøkt om koronapandemien har hatt forskjellig effekt på kvinner og menn, men finner ingen klare forskjeller og vil ikke kommentere videre på det.

#### 3.3.1 Flere ansatte gir flere søknader, uten en relativ vekst i søknadsaktivitet

Helsefak har de to siste årene sendt over 20 søknader mer per år enn tidligere i perioden. Veksten er i alle søknadsarenaene, og spesielt øker det til EU. Det høye antallet innvilget fra Forskningsrådet, med en innvilgelsesprosent på 25% i 2021 er spesielt positivt, og er den høyeste innvilgelsesraten fra Forskningsrådet vi har hatt i perioden. Til sammenligning var den nasjonale innvilgelsesprosenten i Forskningsrådet for fagområdet medisin og helse 32% i 2021<sup>24</sup>. I snitt er det årlig 22% av UFF med forskning som sender en søknad, økningen i sendte søknader er dermed i tråd med økning i antall ansatte. Totalt i femårsperioden har 52% av UFF med forskning sendt en søknad, og det er dermed rom for mer vekst i søknadsaktivitet.

Helsefak har en svak negativ utvikling i eksterne inntekter og er under måltallet om 25% eksterne inntekter. Over perioden har det variert mellom 21% og 24% eksterne inntekter, og i 2021 utgjør eksterne inntekter 21%. Nedgangen skyldes blant annet fortsatt stengt AKM, samt økt undervisningsbelastning og forsinkelser i prosjektarbeid grunnet koronapandemien. Dette påvirker periodiserte eksterne inntekter. Samtidig med negativ inntektsutvikling har Helsefak økt i antall UFF årsverk, som derfor resulterer i at Helsefak er under måltallet for inntekt per UFF.

#### 3.3.2 Ulike tilnærminger til søknadsarbeid ved enhetene

Det er flere positive tegn til en mer aktiv holdning ved enhetene til søknadsarbeid og ekstern finansiering. Instituttene praktiserer ulike strategier for å bedre eksternøkonomien, som hver på sin måte har bidratt til utvikling. For eksempel har IMB og ISM omtrentlig lik uttelling i inntekt pr UFF (sett bort fra senterinntekten og estimert andel årsverk i senter) til tross for to forskjellige strategiske tilnærminger. IMB har oppmuntret flere til å søke, og ISM har hatt en aktiv seleksjon på hvilke søknader som kan sendes når. ISM har høyere innvilgelsesprosent, men i 2020 og 2021 har IMB flere antall innvilgede søknader. Innvilgelsesprosenten til IMB er også økende. ISM topper statistikken i antall trukket søknader. De ser det ikke som bortkastet arbeid, heller som grunnlag for senere utlysninger. Ansatte ved IFA har en relativt stor aktivitet mot søknader, lykkes også godt i EU og Forskningsrådet og har størst andel ekstern inntekt per UFF. IFA har over tid jobbet med rekruttering og kulturbygging for søknadsarbeid i

<sup>23</sup> <https://uit.no/om/strategi2030>

<sup>24</sup> Forskningsrådet i tall

forskningsgruppene. Et fjerde eksempel er IPS som viser økt søknadsaktivitet i perioden og som samtidig øker inntekt per UFF de tre siste årene. IPS har hatt fokus på finansieringsgraden i eksterne prosjekter de siste årene.

Fortsatt aktiv tilnærming til søknadsarbeid er viktig for at Helsefak som helhet skal klare å nå målene som er satt, et arbeid som blir viktig å understøtte og videreføre framover.

### 3.3.3 Helsefaks sammensetning av UFF og forutsetninger for å oppfylle målene i strukturreformen

Ved Helsefak er det 30% av UFF-ansatte som ikke har forskning som del av sin stilling, men har mellom 10 og 30% avsatt tid til fagoppdatering. En relativ økning i andel UFF med forskning vil kunne bidra til at Helsefak når sine måltall, spesielt de som måles per UFF. Disse måltallene er satt i forbindelse med strukturreformen for å akademisere profesjonsfagene, jmf Stortingsmelding 18 (2014-2015)<sup>25</sup>: «[det er] nødvendig å endre strukturen på universitets- og høgskolesektoren, og samle ressursene på færre, men sterkere institusjoner. (...) Universitetene og høyskolene må gjennom forskning og utvikling bidra til en positiv, kunnskapsbasert videreutvikling av profesjonsfagene og praksisfeltet». En slik tilnærming alene vil imidlertid være svært ressurskrevende, slik at andre alternativer for økt aktivitet også bør vurderes. For eksempel har et prosjekt ved Amsterdam University of Applied Sciences utarbeidet «The Researcher Career Wheel» (se appendix), som er et redskap for å blant annet utvikle undervisere til akademikere, men også å løfte alle erfaringsnivå ett steg videre. Dette handler om kulturendring og underbygning av ansatte som ønsker faglig utvikling. Mange av tiltakene som foreslås her er et utgangspunkt for å løfte flere til bidrag; med f.eks. blogginnlegg, lærebokkapitler og review-artikler. Helsefak ønsker å se videre på dette verktøyet, og se hvordan det kan brukes ved vårt fakultet for å nå målet med strukturreformen.

---

<sup>25</sup> <https://www.regjeringen.no/no/dokumenter/meld.-st.-18-2014-2015/id2402377/?ch=1>

## 4 FORSLAG TIL TILTAK

### 4.1 OVERGANG TIL NY STRATEGI OG VEIEN VIDERE

Selv om KD endrer praksis for oppfølging av nasjonale indikatorer, har det ikke kommet kontrabeskjed på måltall i forbindelse med strukturreformen. Det vil si at UiT fremdeles forventes å oppnå en publisering pr UFF på 1,2 publikasjonspoeng, og en eksternfinansiering pr UFF på 365.000 kr i 2025. Helsefaks resultater viser størst måloppnåelse under mål 2 (innen andre BoA, open access og formidling), og er i stor grad i tråd med klyngeanalysen gjort i Tilstandsrapporten 2021. Denne grupperer UiT sammen med institusjoner som har en tyngde innen samfunnskontakt (basert på høy uttelling på indikatorene forretningsideer, formidling, fleksible studenter, deltidsstudenter og andre BoA-inntekter). UiTs nye strategi, Eallju – drivkraft i nord mot 2030<sup>26</sup>, er helt eksplisitt på at vi «skal øke vår deltakelse i nasjonale og internasjonale konkurranseutsatte finansieringsordninger» og vi skal utvikle «flere ledende fagmiljøer i front av den internasjonale kunnskapsutviklingen». Dette tilsier at indikatorer på søknader og inntekt fra Forskningsrådet og EU vil bestå (mål 1). Sammen med den økonomiske situasjonen i sektoren og i Forskningsrådet betyr det enda større grad av ledelse og strategiske prioriteringer for å nå disse målene.

#### 4.1.1 Status på tiltak fra tidligere rapport

Fakultetsstyret vedtok etter fjorårets Rapport forskning 2020 tre tiltak hvorav de to første tiltakene var at instituttene skulle 1) jobbe med utviklingsplanen til forskningsgruppene og sende en kopi til Prosjektkontoret for oppfølging av søknadsplaner, og 2) jobbe internt med å identifisere egne hindringer for å søke og oppnå ekstern finansiering, samt hindringer i å øke publisering. Dette arbeidet er påbegynt, men ikke ferdigstilt. Det anbefales at dette arbeidet videreføres, og at hensynet til den økonomiske situasjonen innarbeides i dette. Det tredje tiltaket fattet av FS var at fakultetet skulle utrede registrering og belønning av formidling og innovasjon, dette arbeidet er i oppstartsfasen.

Forslag:

1. Helsefak viderefører implementering av forskningsgruppenes utviklingsplaner. Kortsiktige og langsiktige planer om ekstern forskningsfinansiering skal konkretiseres ved å inkludere «one-pagere» for alle typer søknader i et appendix til utviklingsplanene<sup>27</sup>.
2. Helsefak viderefører arbeidet med enhetenes handlingsplan for økte eksterne inntekter og økt publisering. Forskningsgruppenes utviklingsplan inkluderes som en del av dette arbeidet, slik at det er sammenheng mellom instituttens handlingsplan og forskningsgruppenes planlagte aktiviteter. Oppfølging av instituttens planer endres til et felles lederseminar ved årsskifte i stedet for dialogmøtene.

### 4.2 NYE TILTAK FOR KVALITET I FORSKNING (KD1)

EU er en arena der Helsefak bør ha et større trykk mens Forskningsrådet har redusert kapasitet. EUs Mission Cancer er den største satsningen innen helse i Horisont Europa, og Kreftforeningen har varslet økt trykk på å styrke forskning på kreft i Nord-Norge. De er bl.a. opptatt av at det skal være kreftforskning ved alle nærsykehus, som vil forde tett samarbeid med UNN og de øvrige helseforetakene tilknyttet Helse Nord. EUs satsning på «Mission Cancer» for perioden 2021-2027 kan i så måte ses i sammenheng med Kreftforeningens satsning, og Helsefak bør ha som mål å hente inn midler i begge disse arenaene for finansiering av høykvalitetsprosjekter.

I tillegg til EUs «Horisont Europa» er andre internasjonale og nasjonale prestisjetunge arenaer, og andre nasjoners forskningsråd i samarbeidssøknader også aktuelt å utnytte i større grad. Disse krever i noen tilfeller en større grad av egenkapital, som Helsefak må søke å løse. Helsefak har en relativt høy internasjonal sampublisering, og burde

<sup>26</sup> <https://uit.no/om/strategi2030>

<sup>27</sup> jmf. UiTs ambisjonsnotat for EU der det stadfestes av EU-strategien skal forankres i forskningsgruppene



dermed ha et godt nettverk å jobbe ut fra. Fakultetet mener også det vil være nyttig å utarbeide mentormodeller for ivaretagelse av tilbakemelding på det faglige innholdet i søknadsskisser for å forbedre søknadskvalitet. Det er også viktig at instituttene følger opp ansatte som får avslag på sine søknader med tanke på søknadsforbedring.

Forslag:

3. Helsefak skal ha som ambisjon om å øke antall søknader og tilslag til EU. Herunder arbeide for å mobilisere og legge til rette for miljøer som kan gå sammen om å søke EUs Horizont Europa, Cluster 1- Health generelt, og Mission Cancer<sup>28</sup> spesielt.
4. Helsefak må jobbe for et økt økonomisk handlingsrom til støtte for prestisjetunge sentersøknader, samt jobbe opp mot nivå 1 med hensyn til egenandelskravet.
5. Alle institutter skal tilby faglige mentorgrupper (2-3 personer med erfaring fra eksternfinansiering) som kan gi råd på søknadsplaner slik de framkommer i forskningsgruppens utviklingsplaner.

#### 4.3 NYE TILTAK FOR FORSKNING FOR VELFERD, VERDISKAPNING OG OMSTILLING (KD2)

Instituttene som oppgir en mer aktiv styring av søknader for eksternfinansiering, ser ut til å ha positiv utvikling av indikatorene. Tiltak for økte eksterne inntekter bør derfor være å bygge kultur for søknadsarbeid. Det er viktig for fakultetet å synliggjøre vår forskning utad, og for å trygge de ansatte i formidlingsaktivitet ønsker fakultetet å vurdere muligheten for å kunne tilby formidlingskurs på fast basis.

Forslag:

6. Fakultetet mener det skal være en del av vår forskningskultur at flest mulig søker mindre stiftelser/fond om driftsmidler (til forsknings-, innovasjons-, utdannings- og formidlingsprosjekter). Dette gir ekstra midler til drift i prosjekter, gir økt erfaring med søknadsskriving og virker positivt for CV-bygging med hensyn til å hente større midler.
7. Fakultetet utreder muligheten for jevnlig å kunne tilby formidlingskurs for ansatte, spesielt i de mest brukte formene p.t. som intervju, kronikk og populærvitenskapelige foredrag, men også andre aktuelle formidlingsformer.

#### 4.4 NYE TILTAK FOR ET EFFEKTIVT, MANGFOLDIG OG SOLID FORSKNINGSSYSTEM (KD 4)

Helsefak må fortsette å bygge en sterk kultur for forskning blant de ansatte. Dette inkluderer å jobbe med kontinuerlig kompetanseheving for ansatte, og ha en uttalt rekrutteringspolicy og en bevisst holdning til ledelse.

Forslag:

8. Helsefak skal fortsette arbeidet med å bygge og utvikle en sterk forskningskultur innen toppforskning og breddesatsning. Helsefak vil undersøke ulike modeller som kan være nyttig i dette arbeidet, f.eks. «Researcher Career Wheel» og som gjør at alle kan «ta et steg til». Et undermål i dette er i større grad å inkludere UFF uten forskning i forskningsgruppens arbeid, på stillingskategoriens egne premisser.
9. Helsefak skal ha en helhetlig rekrutteringspolitikk som ivaretar både forskningsambisjoner og undervisningskvalitet.
10. Helsefak skal ha en uttalt kultur for anerkjennelse av forskningsinnsats – f.eks. hvordan ansatte skal bli sett ved innsendelse av publikasjoner og søknader, tilbudt veiledning ved avslag, og ikke bare få anerkjennelse ved oppnådde resultater.

<sup>28</sup> EU Mission Cancer ([link](#)) - The Horizon Europe programme will provide €378.2 million in seed funding during the period 2021-23 to support the implementation of the mission. The 4 Mission objectives: 1) Understanding of cancer 2) Prevention and early detection 3) Diagnosis and treatment 4) Quality of life for patients & their families.

## 5 APPENDIX

---

### 5.1.1 Utdrag fra ny strategi mot 2030 – Ambisjoner og mål rettet mot forskning

Strategien består av tre hovedambisjoner med tilhørende fire punkter hver som skal bidra til å nå disse ambisjonene, under er et utdrag av strategien som retter seg mot forskningsaktiviteten:

1. UiT skal være internasjonalt ledende på kunnskap og kompetanse om og for Arktis og nordområdene.

- Utvikle flere ledende fagmiljøer i front av den internasjonale kunnskapsutviklingen. Vi skal løfte forskningsspørsmål som er relevante for utviklingen i nord. Vi skal utvikle og opprettholde vitenskapelig infrastruktur og tidsserier av data som muliggjør kunnskapsutvikling om og for Arktis og nordområdene.
- Styrke kompetanse om og for samiske og kvenske forhold (...) og på møtet mellom majoritets- og minoritetssamfunnet.
- (...) Vi skal være (...) en foretrukket samarbeidspartner for nærings- og samfunnsliv og internasjonale samarbeidspartnere

2. UiT skal bidra til nyskapende, demokratiske og bærekraftige løsninger på store samfunnsutfordringer.

- Praktisere åpen vitenskap [og] fremme åpenhet i forskning, utdanning og innovasjon (...).
- Utvikle kunnskap, metoder og virkemidler som bidrar til å løse store samfunnsutfordringer. Vi skal fremme banebrytende kunnskapsutvikling, og prioritere infrastruktur og metodeutvikling som muliggjør arbeid med komplekse problemstillinger og bærekraftige løsninger. (...).
- Fremme tverrfaglighet, samskaping og innovasjon. Vi skal skape arenaer og fjerne barrierer for samarbeid på tvers av fagområder, sektorer og landegrenser. (...).
- (...) Vi skal forbedre utnyttelse og prioritering av ressursene våre. Vi skal øke vår deltakelse i nasjonale og internasjonale konkurranseutsatte finansieringsordninger for forskning, utdanning og innovasjon.

3. Talentutvikling og mangfold: UiT skal være et arnested for utvikling av studenter og ansattes kompetanse og talent, med mangfold som drivkraft og ressurs.

- (...) Vi skal etablere virkemidler for å legge til rette for utvikling av ansatte og fagmiljø sin kapasitet og kompetanse. (...)
- Rekruttere og utruste studenter som lærer hele livet. Vi skal legge til rette for mobilitet, styrke samhandling med arbeidslivet og bidra til at flere unge tiltrekkes til og blir i landsdelen. Vi skal fremme nysgjerrighet, delaktighet og framtidsansvar
- Prioritere kunnskapsutvikling og innovativ formidling som fremmer mangfold. Vi skal styrke studenter og ansattes deltagelse i dialog og samfunnsdebatt (...).



## 5.1.2 Søknadskilder i andre BoA, med mer enn 2 sendte søknader de siste fem år (utgjør 85% av kildene)

Kilde	Sendt (n)						Innvilget (n)					
	2017	2018	2019	2020	2021	Totalt	2017	2018	2019	2020	2021	Totalt
Helse Nord	44	39	28	29	36	176	11	10	13	9	9	52
Kreftforeningen	12	16	9	11	12	60	2	3			1	6
Extrastiftelsen/Stiftelsen Dam	6	8	3	9	5	31		1	1	1		3
Odd Berg Gruppens Medisinske Forskningsfond	4		6	2	5	17			1	1	2	4
DIKU/SIU		1	3	6	7	17			1	4	1	6
Nasjonalforeningen for folkehelsen	2	1	3	6	1	13						0
TFS	5	1	5	1		12			4	1		5
HOD	4	3	2	2	1	12	4	3	2	2	1	12
KG Jebsen	3	1	1		6	11	1	1			2	4
Fysiofondet	2		4	2	2	10	1		1		1	3
NordForsk	5	2	2	1		10	1			1		2
Barnekreftforening	1	2	1	3	2	9		2	1	2		5
Hdir	1		2	2	4	9	1		2	1	4	8
Norske Kvinners Sanitetsforening (NKS)	1	1	2	1	3	8				1		1
MABIT	1	2	1	3	1	8		2	1		1	4
KAVLI		2		3	3	8		2			1	3
SANKS		1	2	2	2	7			2	2	1	5
Barentssekretariatet	4	2	1			7	3	2				5
Aakre stiftelsen			6			6			6			6
Helse Sør Øst			3	1	1	5					1	1
Troms og Finnmark fylkeskommune	1		1	1	1	4			1		1	2
AMFF (allmennmedisinsk forskningsfond)	2	1	1			4			1			1
Novo Nordisk Fonden	1		2	1		4	1					1
Det norske universitetssenteret i St. Petersburg	3	1				4	2					2
Familien Blix Fond			2		2	4						0
Bergens Forskningsstiftelse		2	2			4						0
NORAD				4		4						0
Diabetesforbundet	1	2	1			4		2				2
NORM		2	2			4						0
Erasmus +		1		1	1	3		1		1	1	3

## 5.1.3 The Research Career Wheel



Towards a practice-oriented and scholarly-active culture:

# The Research Career Wheel

**Author:** Lucy Kerstens, MSc, Manager Centre for Applied Research in Business and Economics, Faculty of Business and Economics, Amsterdam University of Applied Sciences, Amsterdam, The Netherlands. EARMA Travel Grant Awardee 2019.

## Names and affiliations of all Co-authors:

**Professor Lori DiVito**, Chair of Collaborative Innovation and Entrepreneurship, Amsterdam International Business School, Amsterdam University of Applied Sciences, Amsterdam, The Netherlands.

**Professor Diane Sloan**, Professor of Learning and Teaching, PFHEA, Northumbria University, Newcastle upon Tyne, United Kingdom.

## Introduction

The Research Career Wheel is a developmental concept that shows different routes along which research careers can develop within institutional and societal frameworks. Starting with the intrinsically motivated individual at the heart of the wheel, one's career grows outwards via different lines: from being a lecturer to assistant professor level through to associate and full professor levels. The wheel also points out some internal and external enablers that support career growth from a 'restricted' to an 'extended' research professional. These numerous and individual-oriented enablers offer a starting point of discussion on career growth: where do you stand and where does your organisation stand?

## How to read the wheel

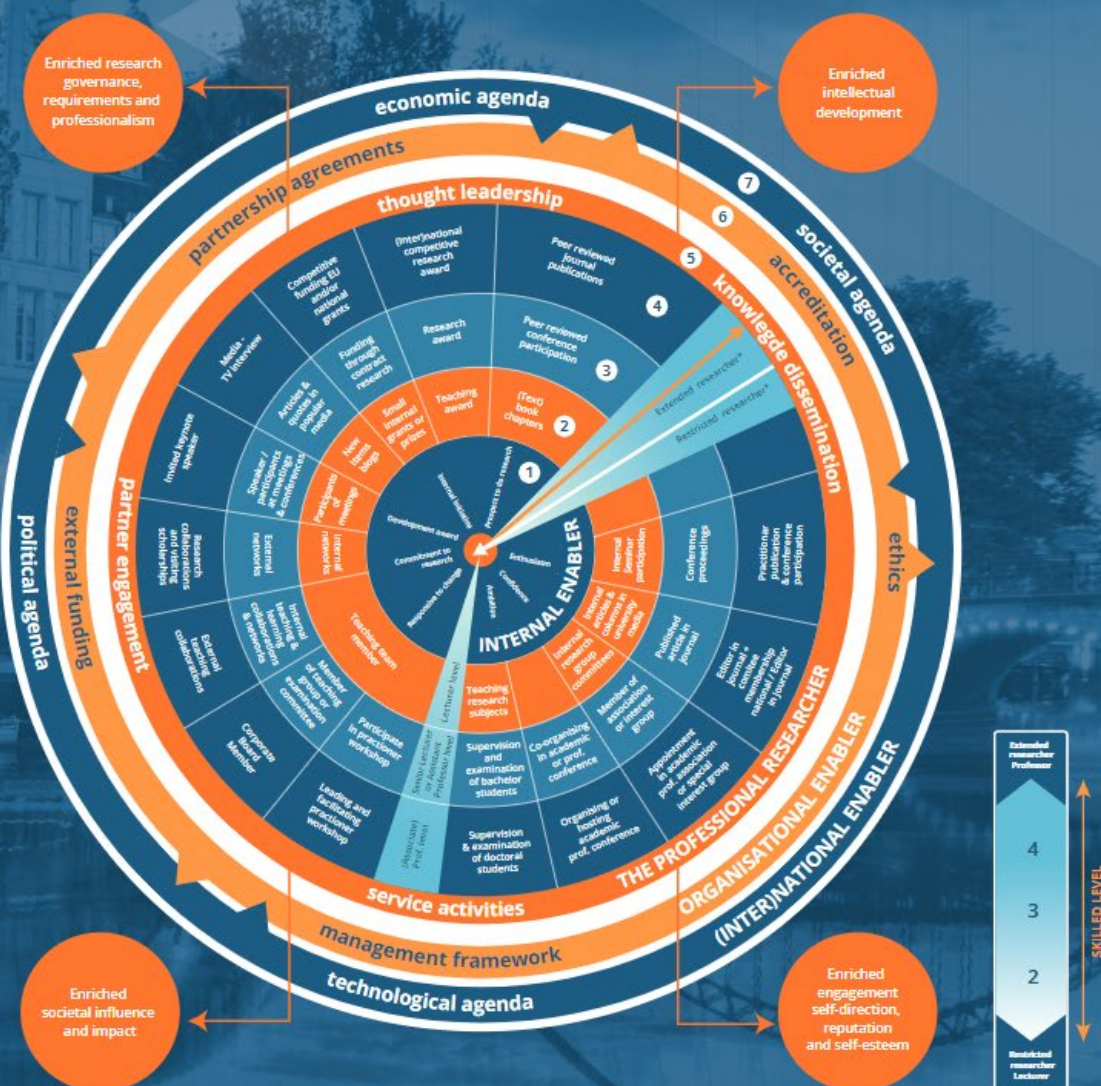
The Research Career Wheel illustrates how increased research quality can be achieved by developing the internal enablers first, helping researchers increase confidence and develop expertise with mentoring and encouragement from experienced teacher-researchers. The development of internal support is subsequently mapped to external enablers (conferences, presentations, funded fellowships, etc). Formal external bodies thus provide recognition of this professional development and this helps teaching-oriented universities such as universities of applied sciences to actively promote a culture of academic development. The wheel helps identify different activities and the next steps that enable growth and development.

## References:

\*Evans, L. (2015) *Enhancing the quality of research in Europe: theoretical perspectives on and guiding principles for researcher development*. In A. Carel, L. Motet, R. Pricopie, J. Solmi & P. Scott (Eds.) *The European Higher Education Area: Between critical reflections and future policies*. Part II, pp. 583-602. Dordrecht, Springer. (Also in Springer Open Access: <http://link.springer.com/book/10.1007/978-93-319-20877-0>)

## For more general information:

<https://www.amsterdamuas.com/amsib> - <https://www.amsterdamuas.com/carem>  
- <https://www.northumbria.ac.uk/>



#### 5.1.4 Publiseringspoeng fordelt på kjønn i perioden 2017 - 2018

Vi har tidligere sett på om kvinneandelen på fakultetets søknadsaktivitet gikk ned under korona, og hvis vi gjør samme øvelse når det kommer til publikasjonspoeng ser vi at prosentandelen på fakultetet i sin helhet ligger på det jevne med rundt 50%.

	2017		2018		2019		2020		2021	
	Publiseringspoeng	Andel kvinner	Publiseringspoeng	Andel kvinner	Publiseringspoeng	Andel kvinner	Publiseringspoeng	Andel kvinner	Publiseringspoeng	Andel kvinner
Fakultetsnivå	1,22	0,22 (18%)	3,74	3,74 (100%)	2,31	2,05 (89%)	2,92	2,92 (100%)	0,2	0 (0%)
IH	-	-	30,69	4,7 (15%)	36,99	15,43 (42%)	24,7	14,84 (60%)	34,91	14,3 (41%)
IFA	46,12	23,97 (52%)	28,47	13,82 (49%)	45,97	20,92 (46%)	35,27	17,89 (51%)	44,57	24,35 (55%)
IHO	68,96	58,37 (85%)	86,3	67,08 (78%)	55,45	48,71 (88%)	56,97	49,59 (87%)	50,92	43,61 (86%)
IKM	174,97	51,35 (29%)	183,71	53,84 (29%)	202,83	61,07 (30%)	183,11	57,57 (31%)	202,15	62,89 (31%)
IKO	13,81	4,81 (35%)	25,05	10,21 (41%)	17,8	8,14 (46%)	24,89	11,43 (46%)	26,51	11,96 (45%)
IMB	68,65	26,94 (39%)	72	34,53 (48%)	85,66	35,35 (41%)	79,28	38,06 (48%)	84,93	37,66 (44%)
IPS	44,38	20,56 (46%)	78,94	29,13 (37%)	63,15	24,31 (38%)	84,25	37,95 (45%)	68,47	32,36 (47%)
ISM	177,05	91,41 (52%)	171,16	97,79 (57%)	150,1	95,44 (64%)	138,91	75,47 (54%)	175,27	101,47 (58%)
IVP	-	-	7,12	7,12 (100%)	12,97	12,97 (100%)	4,5	3,5 (78%)	16,31	15,57 (95%)
RKBU	28,22	14,96 (53%)	35,48	21,45 (60%)	24,61	13,66 (56%)	29,01	17,6 (61%)	40,48	26,36 (65%)
<b>Helsefak totalt</b>	<b>623,52</b>	<b>292,72 (47%)</b>	<b>722,67</b>	<b>343,42 (48%)</b>	<b>697,83</b>	<b>338,04 (48%)</b>	<b>663,79</b>	<b>326,8 (49%)</b>	<b>744,88</b>	<b>370,53 (50%)</b>

### 5.1.5 Sendte og innvilgede søknader per institutt fordelt på kilde (2017-2021).

Institutt/ kilde	Antall sendte søknader						Andel av sendte søknader*						Innvilgelsesprosjenter					
	2017	2018	2019	2020	2021	Tot	2017	2018	2019	2020	2021	Tot	2017	2018	2019	2020	2021	Tot
<b>IFA</b>	<b>38</b>	<b>40</b>	<b>29</b>	<b>39</b>	<b>24</b>	<b>170</b>	<b>21%</b>	<b>23%</b>	<b>17%</b>	<b>19%</b>	<b>12%</b>	<b>18%</b>	<b>34%</b>	<b>25%</b>	<b>21%</b>	<b>23%</b>	<b>21%</b>	<b>25%</b>
EU	4	3	4	4	5	20	11%	8%	14%	10%	21%	12%	25%	33%	0%	0%	20%	15%
NFR	14	16	7	12	8	57	37%	40%	24%	31%	33%	34%	29%	6%	0%	8%	25%	14%
Andre	20	21	15	15	10	81	53%	53%	52%	38%	42%	48%	40%	38%	40%	27%	20%	35%
UiT			3	8	1	12	0%	0%	10%	21%	4%	7%			0%	50%	0%	33%
<b>IH</b>	<b>na</b>	<b>na</b>	<b>5</b>	<b>9</b>	<b>3</b>	<b>17</b>	<b>na</b>	<b>na</b>	<b>3%</b>	<b>4%</b>	<b>1%</b>	<b>2%</b>	<b>na</b>	<b>na</b>	<b>40%</b>	<b>33%</b>	<b>33%</b>	<b>35%</b>
NFR	na	na	1	3	1	5	na	na	20%	33%	33%	29%	na	na	0%	0%	100%	20%
Andre	na	na	3	6	2	11	na	na	60%	67%	67%	65%	na	na	67%	50%	0%	45%
UiT	na	na	1			1	na	na	20%	0%	0%	6%	na	na	0%			0%
<b>IHO</b>	<b>17</b>	<b>2</b>	<b>11</b>	<b>11</b>	<b>14</b>	<b>55</b>	<b>9%</b>	<b>1%</b>	<b>6%</b>	<b>5%</b>	<b>6%</b>	<b>6%</b>	<b>6%</b>	<b>50%</b>	<b>36%</b>	<b>18%</b>	<b>46%</b>	<b>26%</b>
EU	1					1	6%	0%	0%	0%	0%	2%	0%					0%
NFR	10	2	4	5	3	24	59%	100%	36%	45%	23%	44%	0%	50%	25%	0%	33%	13%
Andre	6		7	6	11	30	35%	0%	64%	55%	77%	54%	17%		43%	33%	45%	37%
<b>IKM</b>	<b>17</b>	<b>20</b>	<b>24</b>	<b>26</b>	<b>39</b>	<b>126</b>	<b>9%</b>	<b>12%</b>	<b>14%</b>	<b>13%</b>	<b>19%</b>	<b>13%</b>	<b>29%</b>	<b>45%</b>	<b>58%</b>	<b>27%</b>	<b>21%</b>	<b>34%</b>
EU	2	1	3	2	3	11	12%	5%	13%	8%	8%	9%	50%	0%	33%	0%	0%	18%
NFR	3	6	3	8	11	31	18%	30%	13%	31%	26%	24%	33%	17%	67%	13%	18%	23%
Andre	12	13	13	11	20	69	71%	65%	54%	42%	53%	55%	25%	62%	62%	45%	25%	42%
UiT			5	5	5	15	0%	0%	21%	19%	13%	12%			60%	20%	40%	40%
<b>IKO</b>	<b>7</b>	<b>6</b>	<b>5</b>	<b>3</b>	<b>1</b>	<b>22</b>	<b>4%</b>	<b>4%</b>	<b>3%</b>	<b>1%</b>	<b>0%</b>	<b>2%</b>	<b>29%</b>	<b>33%</b>	<b>60%</b>	<b>33%</b>	<b>100%</b>	<b>41%</b>
EU				1		1	0%	0%	0%	33%	0%	5%				0%		0%
NFR	1	2				3	14%	33%	0%	0%	0%	14%	0%	50%				33%
Andre	6	4	5	2	1	18	86%	67%	100%	67%	100%	82%	33%	25%	60%	50%	100%	44%
<b>IMB</b>	<b>45</b>	<b>34</b>	<b>52</b>	<b>62</b>	<b>63</b>	<b>256</b>	<b>24%</b>	<b>20%</b>	<b>30%</b>	<b>30%</b>	<b>31%</b>	<b>27%</b>	<b>24%</b>	<b>24%</b>	<b>19%</b>	<b>23%</b>	<b>29%</b>	<b>24%</b>
EU	3	1	5	5	6	20	7%	3%	10%	8%	10%	8%	33%	0%	0%	40%	17%	20%
NFR	13	12	7	20	18	70	29%	35%	13%	32%	29%	27%	8%	17%	0%	5%	39%	16%
Andre	29	21	39	33	36	158	64%	62%	75%	53%	57%	62%	31%	29%	26%	24%	19%	25%
UiT			1	4	3	8	0%	0%	2%	6%	5%	3%			0%	75%	100%	75%
<b>IPS</b>	<b>12</b>	<b>16</b>	<b>6</b>	<b>11</b>	<b>19</b>	<b>64</b>	<b>7%</b>	<b>9%</b>	<b>3%</b>	<b>5%</b>	<b>9%</b>	<b>7%</b>	<b>0%</b>	<b>13%</b>	<b>50%</b>	<b>9%</b>	<b>16%</b>	<b>14%</b>
EU		2	1	2	5	10	0%	13%	17%	18%	26%	16%		0%	100%	0%	0%	10%
NFR	4	4	2	5	4	19	33%	25%	33%	45%	21%	30%	0%	0%	0%	0%	0%	0%
Andre	8	10	3	4	10	35	67%	63%	50%	36%	53%	55%	0%	20%	67%	25%	30%	23%
<b>ISM</b>	<b>41</b>	<b>40</b>	<b>32</b>	<b>21</b>	<b>31</b>	<b>165</b>	<b>22%</b>	<b>23%</b>	<b>19%</b>	<b>10%</b>	<b>15%</b>	<b>18%</b>	<b>27%</b>	<b>35%</b>	<b>53%</b>	<b>43%</b>	<b>35%</b>	<b>38%</b>
EU	5	3	5	4	2	19	12%	8%	16%	19%	6%	12%	0%	33%	80%	0%	0%	26%
NFR	8	7	4	6	10	35	20%	18%	13%	29%	32%	21%	13%	29%	25%	33%	10%	20%
Andre	28	30	23	11	19	111	68%	75%	72%	52%	61%	67%	36%	37%	52%	64%	53%	45%
<b>IVP</b>	<b>na</b>	<b>4</b>		<b>6</b>	<b>3</b>	<b>13</b>	<b>na</b>	<b>2%</b>	<b>0%</b>	<b>3%</b>	<b>1%</b>	<b>1%</b>	<b>na</b>	<b>25%</b>		<b>17%</b>	<b>0%</b>	<b>15%</b>
NFR	na	2		1	1	4	na	50%		17%	33%	31%	na	0%		0%	0%	0%
Annet	na	2		5	2	9	na	50%		83%	67%	69%	na	50%		20%	0%	22%
<b>RKBU</b>	<b>7</b>	<b>9</b>	<b>8</b>	<b>17</b>	<b>9</b>	<b>50</b>	<b>4%</b>	<b>5%</b>	<b>5%</b>	<b>8%</b>	<b>4%</b>	<b>5%</b>	<b>0%</b>	<b>33%</b>	<b>63%</b>	<b>24%</b>	<b>44%</b>	<b>32%</b>
EU			1	3		4	0%	0%	13%	18%	0%	8%			0%	67%		50%
NFR	3	4	3	3		13	43%	44%	38%	18%	0%	26%	0%	0%	67%	0%		15%
Andre	4	5	4	11	9	33	57%	56%	50%	65%	100%	66%	0%	60%	75%	18%	44%	36%
<b>Tot</b>	<b>184</b>	<b>171</b>	<b>172</b>	<b>205</b>	<b>204</b>	<b>936</b>	<b>100%</b>	<b>100%</b>	<b>100%</b>	<b>100%</b>	<b>100%</b>	<b>100%</b>	<b>23%</b>	<b>29%</b>	<b>37%</b>	<b>25%</b>	<b>27%</b>	<b>28%</b>

\* Øverste linje (uthevet) viser instituttets andel av sendte total ved fakultetet, øvrige viser fordeling internt på instituttet.



---

## SAKSFRAMLEGG

---

Til:  
Fakultetsstyret for Det helsevitenskapelige fakultet

Møtedato:  
30.09.2022

Sak:  
32/22

---

### **Behandling av årsrapport for informasjonssikkerhet og personvern 2021**

#### **Innstilling til vedtak:**

1. Helsefak skal tydeliggjøre hvilke konkrete oppgaver fakultetet har ansvar for innen personvern og informasjonssikkerhet og hvem som har delegert ansvar til å løse oppgavene.
2. Helsefak skal formalisere hvordan fakultetet skal jobbe med informasjonssikkerhet og personvern gjennom å blant annet utarbeide retningslinjer. Retningslinjene bør også omfatte hvordan det skal jobbes med opplæringsaktiviteter og hvem som har ansvaret for dette.
3. Fakultetsstyret ber dekanen styrke arbeidet med informasjonssikkerhet og personvern med prioritering av ressurser til å følge opp rapportens hovedkonklusjoner.

#### **Bakgrunn:**

Avdeling for IT har oversendt årsrapport for informasjonssikkerhet og personvern til behandling i fakultetsstyret, jf. Vedlegg 1. I fakultetsstyrets behandling av årsrapporten, skal fokuset være på særskilte problemstillinger og forbedringsområder knyttet til Helsefak.

#### **Årsrapport for informasjonssikkerhet og personvern**

ITA har i sin rapport redegjort for at UiT de siste årene har jobbet målrettet og strukturert med informasjonssikkerhet og personvern. Det er fremhevet at man på UiT har hatt klare forbedringer i systematikk og helhet i arbeidet, og på flere felt har universitetet sterkt forbedret sin posisjon.

I tillegg beskrives det et risikobilde som er under utvikling. Trusselaktørene blir mer profesjonelle samtidig som ansatte og studenter ved UiT i økende grad jobber på systemer mot internett og har økt mobilitet. PST har trukket frem mål relatert til Nord- Norge, Svalbard og forsvars- og nordområdepolitikken som særlig utsatt. Nasjonal sikkerhetsmyndighet har trukket frem at trusselaktører har økt søkelys på forsknings- og utdanningsinstitusjoner. EOS tjenestene har særlig trukket frem at forskningsmiljøer innen forsvar, helse og maritim teknologi er særlig utsatt. Kunnskapsdepartementet forventer at arbeidet med informasjonssikkerhet og personopplysningsikkerhet gis høy prioritet i sektoren grunnet et skjerpet digitalt risikobilde. Sikkerhetshendelsen ved UiT i 2020/2021 viser at også UiT er

utsatt for konkrete hendelser noe som gjør det nødvendig at det jobbes strukturert og målrettet med informasjonssikkerhet og personvern.

ITA beskriver også status og utfordringer knyttet til avvikshåndtering, styring og kontroll og ressurs og kompetansebehov.

For å kunne belyse særlige problemstillinger og forbedringsområder knyttet til Helsefak har fakultetet utarbeidet en egen rapport særlig rettet mot fakultetet, se vedlegg 2. Rapporten er utarbeidet av fakultetets jurister som i det daglige mottar de fleste henvendelser knyttet til personvern og informasjonssikkerhet i fakultetsadministrasjonen. Innholdet gjengis ikke i saksfremlegget og det vises til rapporten i sin helhet.

### **Vurdering og tiltak**

Utfordringene som knytter seg til Helsefaks arbeid med informasjonssikkerhet og personvern knytter seg i stor grad til innføringen av personvernforordningen i 2018 og at man i etterkant av adm. 2020 har sett at Helsefak fortsatt har betydelige og krevende oppgaver knyttet til personvern og informasjonssikkerhet uten at det er tatt høyde for det i fakultetets daglige oppgaveløsning.

Det er i dag ikke avsatt tilstrekkelige ressurser til å arbeide med informasjonssikkerhet og personvern på fakultetet til å løse alle oppgavene som det stilles krav til at vi løser. Det må derfor tas i betraktning ved forslag til øvrige tiltak at det avsettes mer ressurser til dette arbeidet, enten ved nytilsetting eller omprioritering av eksisterende ressurser. Det er vanskelig å anslå hvor mye ressurser det er behov for, da det er mange av oppgavene som ikke løses i dag og fordi det er mye mørketall i forhold til avvik. Det foreslås derfor at ressursbehovet løses ved å øke bemanningen med én stilling i første omgang, og at det videre ressursbehovet evalueres samtidig som neste års årsrapport legges frem for fakultetsstyret.

Gunbjørg Svineng  
dekan

—

*Dokumentet er elektronisk godkjent og krever ikke signatur*

Saksansvarlig: Fakultetsdirektør Kjetil Kvalsvik

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

#### Vedlegg

- 1 Det helsevitenskapelige fakultets rapport for fakultetets arbeid med informasjonssikkerhet og personvern 2022
- 2 Årsrapport informasjonssikkerhet og personvern 2021



**UiT Norges arktiske universitet**

**Det helsevitenskaplige fakultets rapport for fakultetets arbeid med informasjonssikkerhet og personvern 2021-2022**



## Innhold:

1. Innledning .....	3
2. Definisjoner .....	3
3. Risikobildet .....	3
3.1 Risikobildet i et sikkerhetsaspekt. ....	3
3.2 Risikobildet utover sikkerhetsaspektet .....	4
4. Helsefaks ansvar og oppgaver .....	6
4.1 Ansvar .....	6
4.1.1 Enhetsleder.....	6
4.1.2 Leder av forskningsprosjekt.....	6
4.1.3 Systemeier .....	7
4.2 Oppgaver .....	8
5. Nærmere om oppgaver og utfordringer.....	10
5.1 Risikostyring .....	10
5.1.1 Informasjonsverdier .....	10
5.1.2 Risikovurderinger.....	12
5.2 Avviksmeldinger .....	14
5.2.1 Helsefaks avviksmeldinger.....	14
5.2.2 Avvikssystemer .....	15
5.3 Kontrollaktiviteter .....	16
5.4 Opplæringsaktiviteter.....	17
6. Organisering av arbeidet med personvern og informasjonssikkerhet på Helsefak.....	17
6.1 Ressurser .....	17
6.2 Organisering .....	18
7. Anbefalinger .....	19



## 1. Innledning

UiT- Norges arktiske universitets ledelsessystem for informasjonssikkerhet og personvern regulerer universitetets arbeid med personvern og informasjonssikkerhet på et overordnet nivå (styringsdokument). Det daglige ansvaret for at fakultetet oppfyller kravene som stilles til personvern og informasjonssikkerhet ligger til fakultetsdirektør og dekan. Fakultetet skal årlig utarbeide en statusrapport for informasjonssikkerhet og personvern som danner grunnlag for ITAs årsrapport for informasjonssikkerhet og personvern. Fakultetet skal årlig legge frem ITAs årsrapport for fakultetsstyret.

Fakultetets statusrapport for informasjonssikkerhet og personvern bygger på standardiserte spørsmål fra Faggruppen for informasjonssikkerhet og personvern. Denne rapporten tar for seg arbeidet med personvern og informasjonssikkerhet generelt og ikke kun knyttet til standardspørsmål. I denne rapporten gjøres det et forsøk på å gi en mer utfyllende beskrivelse av arbeidet med informasjonssikkerhet og personvern på fakultetet.

## 2. Definisjoner

ITA	Avdeling for IT
FPI	Faggruppe for personvern og Informasjonssikkerhet
PVO	UiTs personvernombud
GDPR	General data protection regulation (personvernforordningen)
ISMS	UiTs ledelsessystem for personvern og informasjonssikkerhet
DPIA	Data protection impact assesment (personvernkonsekvensvurdering)
Helsefak	Det helsevitenskaplige fakultet
Informasjonsverdi	Er et samlebegrep som inkluderer både selve informasjonen samt tilhørende støtteverdier som IKT-system, digitale tjenester, datautstyr av ulike varianter mv.
Informasjonssikkerhet	Informasjonssikkerhet handler om å håndtere risiko knyttet til UiT informasjonsverdier og personopplysninger. Informasjonssikkerhet innebærer at man sikrer opplysningenes integritet, konfidensialitet og tilgjengelighet.
Personvern	Personvern er en grunnleggende menneskerett, og handler om retten til privatliv og til å bestemme over egne personopplysninger.
Personopplysningssikkerhet	Personopplysningssikkerhet handler om å forhindre utilsiktet eller ulovlig tilintetgjøring, tap, endring, ulovlig spredning av eller tilgang til personopplysninger som er overført, lagret eller på annen måte behandlet.
HK-Dir	Direktoratet for høyere utdanning og kompetanse

## 3. Risikobildet

I ITAs årsrapport for 2021 omtales både risikoer knyttet til sikkerhetsaspektet, og andre risikoer som for eksempel risikoen for fysiske trusler eller at UiT begår lovbrudd.

### 3.1 Risikobildet i et sikkerhetsaspekt.

I årsrapporten vises det til PST<sup>1</sup> og NSMs<sup>2</sup> trusselvurdering. Det vises her særlig til at PST har trukket frem mål relatert til Nord- Norge, Svalbard og forsvars- og nordområdepolitikken som særlig utsatt for påvirkningsoperasjoner. I tillegg trekker ITA frem at NSM både i 2020 og i 2021 har pekt på et økt fokus mot forsknings- og utdanningssektoren.

De mest sannsynlige angrepene mot UiT anses å være informasjonsinnhenting og påvirkning, samt digital utpressing, hvor digital utpressing er oppgitt til å være angrepet som vil gi den potensielt største skaden for UiT.

Helsefaks risikobilde kan også illustreres ved at de tre EOS-tjenestene (PST, NSM og E-tjenesten) har trukket frem at «selskaper og forskningsmiljøer innenfor forsvars, helse og maritim teknologi» vil være særlige utsatte for cyberoperasjoner (kunnskapsspionasje) i 2022. Se for eksempel PST nasjonale trusselvurdering for 2022<sup>3</sup> og HK-dir risiko- og tilstandsvurdering for 2022<sup>4</sup>. I HK direktoratets risiko- og tilstandsvurdering vises det til at PST mener norsk forskning er interessant for Russland og Kina på grunn av gode finansieringsordninger, avanserte laboratorier og øvrig forskningsinfrastruktur. Det er videre pekt på at land som Kina og Russland benytter forskningssamarbeid for å skaffe seg tilgang til teknologi og kunnskap som faller inn under eksportkontroll. Dette må også ses i sammenheng med eksportregelverket, hvor nå også kunnskapsoverføring er omfattet av regelverket.

Selv om det operative ansvaret for informasjonssikkerhet og personvern ligger hos FPI, er det nødvendig at Helsefaks ledere og ansatte, i det praktiske arbeidet, er bevisste på hvilke risikoer som eksisterer, samt holder seg oppdatert på de til enhver tid gjeldende retningslinjer og rutiner knyttet til informasjonssikkerhet og personvern. For eksempel er det viktig at fakultetet gjør gode vurderinger knyttet til anskaffelse av avansert utstyr fra Kina og andre risikoland. Eksempelvis gjennomføres det nå en risikovurdering knyttet til å lease gensekvenseringsutstyr fra et kinesisk selskap på Helsefak. Fakultetet er kjent med at det eksisterer forskningssamarbeid med Russland. Dette er ikke samarbeid som fakultetet følger opp eller har kontroll med. Det er dermed opp til den individuelle forskeren som har samarbeid med Russland, som må vurdere risikoen for eksempelvis kunnskapsspionasje og sørge for at samarbeidet er i tråd med regelverket for eksportkontroll.

### 3.2 Risikobildet utover sikkerhetsaspektet

I ITAs årsrapport er «Schrems II» saken som ble avsagt i EU- Domstolen 16.07.2020 særlig trukket frem som en risiko hvor UiT risikerer å bryte lovkrav. Avgjørelsen er redegjort for i detalj i ITAs årsrapport, men i korte trekk gjør avgjørelsen det klart at dersom man skal overføre personopplysninger til land utenfor EU/EØS eller til internasjonale organisasjoner så krever det et overføringsgrunnlag i personvernforordningens kapittel V, i tillegg oppstiller avgjørelsen noen tilleggskrav til vurderingen av om opplysningene kan overføres.

For Helsefak innebærer dette at personopplysninger ikke kan overføres til land utenfor EU/EØS eller internasjonale organisasjoner før man har gjort en konkret vurdering i 5 steg.

---

<sup>1</sup> Politiets sikkerhetstjeneste

<sup>2</sup> Nasjonal Sikkerhetsmyndighet

<sup>3</sup> <https://pst.no/alle-artikler/trusselvurderinger/ntv-2022/>

<sup>4</sup> <https://hkdir.no/rapportar/informasjonssikkerhet-og-personvern-i-hoeyere-utdanning-og-forskning>

1. Kjenn overføringene	Det kreves at man har full oversikt over alle delene av overføringen. Dette innebærer full oversikt over alle prosesser, systemer, tjenester, løsninger, partnere, leverandører, databehandlere og databehandlers underleverandører som overfører personopplysninger ut av EØS.
2. Identifiser overføringsgrunnlag	Før man kan overføre personopplysninger må man finne et overføringsgrunnlag, eller ett unntak fra kravet til overføringsgrunnlag. Dette krever god kompetanse innenfor personvernregelverket. Ofte vil dette innebære inngåelse av omfattende standardavtaler, eller andre tidkrevende juridiske vurderinger. Ofte er det ikke mulig å finne et overføringsgrunnlag som kan benyttes. Unntakene fra kravet til overføringsgrunnlag er i tillegg svært begrensede og kan ikke benyttes for regelmessige overføringer.
3. Vurder om overføringsgrunnlaget vil være effektivt sett i lys av alle omstendighetene ved overføringen	I dette steget skal man vurdere lov og rettspraksis i mottakerlandet for å kunne vurdere om rettighetene til de registrerte ivaretas på samme måte som innenfor EU/EØS. Dette er krevende vurderinger som forutsetter at Helsefak har god kjennskap til et annet lands lover og rettssystem herunder hvordan regelverket håndheves i praksis. Dette er en krevende juridisk vurdering, og hvor Helsefak ikke har jurister med omfattende kompetanse knyttet til andre lands rettssystemer. I tillegg kan det også være språklige barrierer ettersom ikke alle land har lover og øvrig dokumentasjon om rettssystem oversatt til engelsk.
4. Iverksett ytterligere tiltak	Dersom man i steg 3 kommer til at rettighetene til de registrerte ikke er på samme nivå som innenfor EU/EØS må man se om det kan iverksettes tiltak for å sikre de registrerte de samme rettighetene som i EU/EØS. Dersom man ikke kan finne tilstrekkelige tiltak kan ikke overføringen gjennomføres. Slike tiltak kan eksempelvis være godkjent kryptering, anonymisering og pseudonymisering.
5. Re-evaluer	Lovgivningen i et tredjeland kan endre seg, og tiltak som har vært effektive tidligere, kan på grunn av den tekniske utviklingen ikke lengre ha samme effekt. På samme måte kan det komme nye tiltak som har bedre effekt og som derfor må innføres. Under punkt 5 forutsettes det at Helsefak regelmessig følger opp og re-evaluerer overføringer til tredjeland og internasjonale organisasjoner. Dette krever at Helsefak har

	gode rutiner for å følge opp tredjelandsoverføringer regelmessig, noe vi ikke har i dag.
--	--

Helsefak overfører regelmessig store mengder personopplysninger til land utenfor EU/EØS og internasjonale organisasjoner. I tillegg sendes Humant biologisk materiale til land utenfor EU/EØS for analyser hvor det utledes personopplysninger fra materialet. For Helsefak har derfor avgjørelsen fra EU domstolen i saken «Schrems II» stor betydning særlig i forhold til forskningssamarbeid, men den har også betydning i forbindelse med nye systemer, apper, teknologisk utstyr som Helsefak ønsker å ta i bruk.

For eksempel har Helsefak et utbredt forskningssamarbeid mot land som Russland, England, USA, Australia med flere. I tillegg har Helsefak samarbeid med internasjonale organisasjoner som IARC, som er en del av WHO og FN. Helsefak har også mange forskere som har forskningsterminen sin i land utenfor EU/EØS hvor «Schrems II» avgjørelsen også kan få betydning.

Når det gjelder ulike systemer og apper så utvikler og anskaffer Helsefak ulike systemer og apper i forbindelse med forskning og utdanning. Ofte benyttes utviklere som har underleverandører eller kundeservice i land utenfor EU/EØS. Dette er dataflyter som må kartlegges og vurderes i forhold til overføring av personopplysninger.

I forbindelse med anskaffelse av teknologisk utstyr som for eksempel gensekvenseringsutstyr fra land utenfor EU/EØS må Helsefak kartlegge og vurdere dataflytene for kunne ta stilling til hvorvidt leverandøren har tilgang til personopplysninger gjennom eksempelvis kundesupport, fjernaksess eller skjulte bakdører inn i systemet. Dette er krevende vurderinger og forutsetter at man setter seg godt inn i det som skal anskaffes og kobler på riktig kompetanse der det er behov for det, eksempelvis jurister fra Helsefak eller fagpersoner og jurister fra FPI.

Når det gjelder vurderinger knyttet til overføringer til land utenfor EU/EØS og internasjonale organisasjoner ser vi at Helsefak har utfordringer med å overholde lovkravene. I enkelte tilfeller overføres personopplysninger uten at man har gjort vurderingene som er beskrevet i de fem stegene ovenfor. Det finnes flere eksempler på at Helsefak har gjort tilgjengelig personopplysninger til land utenfor EU/EØS uten at det er vurdert, eller finnes lovlig overføringsgrunnlag. Vi er heller ikke kjent med at det gjøres vurderinger knyttet til forskere som har forskningstermin utenfor EU/EØS i dag.

Det omfattende samarbeidet mellom Helsefak og samarbeidspartnere utenfor EU/EØS innebærer at Helsefaks jurister i økende grad blir bedt om å gjøre kompliserte og tidkrevende vurderinger knyttet til overføringer av personopplysninger. Dette er oppgaver juristene tidligere ikke har hatt og som ikke er tatt inn i beregningen av behovet for juridiske ressurser. Juristene på Helsefak har en bred oppgaveportefølje som blant annet inkluderer kontraktsrett, veiledning innen helseforskningsloven, arbeid med helseregistrene, uredelighetssaker, diverse klager fra studenter m.m. Helsefaks jurister har derfor ikke samme muligheter til å holde seg faglig oppdatert som spesialiserte jurister på nivå 1.

Det overordnede ansvaret for at det gjennomføres vurderinger av overføringsgrunnlag ligger til enhetsleder. I forskningsprosjektene ligger det praktiske ansvaret på prosjektleder som behandlingsansvarlig på vegne av UiT i forbindelse med forskningsprosjektene. Når det gjelder ulike systemer, apper og dataløsninger som anskaffes må man legge til grunn at ansvaret følger lederlinjen i fakultetet. Når det gjelder tilgjengeliggjøring av personopplysninger fra Helsefaks helseregistre så har de ulike registrene i sine styringssystemer opprettet grupper som vurderer de aktuelle utleveringene. Det vil vanligvis være behov for juridisk kompetanse for å vurdere hvorvidt det

foreligger overføringsgrunnlag etter «Schrems II» avgjørelsen. Instituttene har ikke selv denne juridiske kompetansen.

## 4. Helsefaks ansvar og oppgaver

### 4.1 Ansvar

Ansvar for personvern og informasjonssikkerhet er et topplederansvar i en virksomhet. På UiT er det operative ansvaret og det praktiske arbeidet delegert til ulike enheter og roller gjennom ulike styringsdokumenter. I ISMS kapittel 3 fremgår det hvilket ansvar som er delegert til Helsefak og andre roller ved fakultetet.

#### 4.1.1 Enhetsleder

Med enhetsleder menes fakultetsledelsen (dekan og fakultetsdirektør).

Enhetsleder er delegert følgende ansvar og roller:

- er ansvarlige for å tilfredsstille krav til informasjonssikkerhet og personvern i egen enhet
- skal sørge for at risikovurderinger gjennomføres
- skal iverksette tiltak dersom det er nødvendig for å ivareta informasjonssikkerheten og personvernet i egen enhet
- har det overordnede ansvaret for at personvernkonsekvensvurderinger (DPIA) iverksettes der det er påkrevd etter personvernforordningen (GDPR) art. 35
- skal rapportere resultat fra risikovurderinger med handlingsplan og avvik til Faggruppe for informasjonssikkerhet og personvern
- skal følge opp avviksmeldinger i egen enhet og sørge for at disse blir lukket, i samarbeid med Faggruppe for informasjonssikkerhet og personvern
- skal informere ansatte i egen enhet om de rutiner og retningslinjer som gjelder til enhver tid og sørge for at kravene i ledelsessystemet til egen enhet blir fulgt

For Helsefak er det i hovedsak snakk om ansvar for praktiske oppgaver knyttet til personvern og informasjonssikkerhet og et mer overordnet ansvar for å sikre at enheten (fakultetet) tilfredsstiller krav til informasjonssikkerhet og personvern.

For å kunne følge opp ansvaret er det nødvendig med god kompetanse knyttet til personvern og informasjonssikkerhet, samt at man har et system for å følge opp at kravene følges, herunder gjennomfører ulike kontrollaktiviteter for å se at aktiviteten i Helsefak tilfredsstiller kravene til informasjonssikkerhet og personvern. Ansvaret krever god kompetanse i aktivitetene på fakultetet, instituttene og senterne.

#### 4.1.2 Leder av forskningsprosjekt

Leder av forskningsprosjekt er delegert følgende roller og ansvar:

- opptrer på vegne av UiT som behandlingsansvarlig for hva gjelder det konkrete forskningsprosjektet
- har det daglige ansvaret for at informasjonssikkerheten ivaretas i forskningsprosjektet
- har ansvaret for at det gjennomføres personvernkonsekvensvurderinger (DPIA) dersom det er påkrevd etter personvernforordningen (GDPR) art. 35.
- nærmere ansvar og forpliktelser følger av retningslinjer for personvern i forskings- og studentprosjekt

Oppgavene som er delegert til prosjektleder stiller store krav til kompetanse knyttet til informasjonssikkerhet og personvern. Det å opptre på vegne av UiT som behandlingsansvarlig i det konkrete forskningsprosjektet innebærer at leder av forskningsprosjektet må ha kunnskap om ulike roller som, behandlingsansvarlig, databehandler og felles behandlingsansvarlig. Prosjektleder må videre ha kjennskap til krav til behandlingsgrunnlag, regler knyttet til overføring av personopplysninger til land utenfor EU/EØS, når det skal inngås databehandleravtaler, klassifisering av data, hvilke systemer som kan benyttes til den aktuelle klassifiseringen og andre forhold knyttet til informasjonssikkerhet.

Forskningsprosjekter og studentprosjekter som behandler personopplysninger skal registrere sine prosjekt i meldingsarkivet til SIKT. I den forbindelse vil forskerne få støtte til personvernrelaterte spørsmål fra SIKT. På samme måte vil ledere av forskningsprosjekter kunne få bistand av personell med riktig kompetanse ved utarbeidelse av risikovurderinger. Prosjektleder må likefullt besitte nok kompetanse til å kunne identifisere utfordringer på egen hånd, og i mange tilfeller betyr det at også juristene på fakultetet gir veiledning til ledere av forskningsprosjekt. Eksempelvis til gjennomgang og utarbeidelse av databehandleravtaler.

#### 4.1.3 Systemeier

Systemeier er delegert følgende ansvar og roller:

- skal etablere og vedlikeholde rutiner for å ivareta sikkerhetsmålene
- skal stille krav til informasjonssikkerhet i anskaffelse, utvikling og vedlikehold av informasjon og informasjonssystemet, i samråd med Avdeling for IT
- skal ha fokus på ivaretagelse av innebygd personvern og personvern som standardinnstilling
- skal sørge for at tilganger blir gitt etter tjenstlig behov, avsluttet når behovet opphører, samt at nødvendig opplæring blir gitt
- skal sørge for at databehandleravtaler inngås
- skal utføre risikovurdering av systemet i henhold til kapittel 5, og dokumentere at risikovurderinger er utført
- skal iverksette eventuelle tiltak på bakgrunn av risikovurderinger

Helsefak har rollen som systemeier for flere ulike systemer. Dette kan være mindre og enkle systemer som inneholder informasjonsverdier som ikke har de høyeste behovene for sikkerhetstiltak, eller det kan være systemer hvor det behandles store mengder informasjonsverdier som krever høye sikkerhetstiltak. Noen eksempler på systemer hvor Helsefak har rollen og ansvaret som systemeier er:

Eutro	System for forskningsadministrasjon og oppbevaring av forskningsdata fra UiTs befolkningsundersøkelser.
Hunt Cloud	System hvor flere av befolkningsundersøkelsene oppbevarer forskningsdata fra eksempelvis genetiske analyser av humant biologisk materiale
Incission	System benyttet i utdanningen til studenter ved IHO.

I mange tilfeller tar institutter, forskningsgrupper etc. i bruk systemer uten at fakultetet involveres. Det gjør at fakultetet ikke har en komplett oversikt over systemer hvor instituttene har rollen som systemeier. Det bør legges til grunn at det benyttes andre systemer hvor ulike institutter har

systemansvar på Helsefak. For eksempel utvikles det systemer for digital oppfølging av studenter uten at fakultetet er involvert. Per i dag er det ikke noe krav om at Helsefak fører systemene inn i en systemkatalog. Den manglende oversikten gjør det vanskelig å utføre andre lovpålagte oppgaver som for eksempel å ha en oppdatert behandlingsprotokoll.

## 4.2 Oppgaver

I praksis innebærer delegeringen av ansvaret for de praktiske oppgavene at det utføres svært mange oppgaver knyttet til personvern og informasjonssikkerhet på Helsefak. De vanligste oppgavene er redegjort for i oversikten under.

Ulike juridiske vurderinger	I alle rollene som beskrevet i punkt 3.1 er det behov for ulike juridiske vurderinger. I mange tilfeller gjør for eksempel prosjektleder og andre ledere vurderingene selv, mens i andre tilfeller ber man om bistand til vurderingene fra en av fakultetets jurister. Det gis eksempelvis juridiske vurderinger knyttet til overføringsgrunnlag til land utenfor EU/EØS, muligheten for tilgang til forskningsdata under forskningstermin, vurderinger av rekkevidden av samtykker og informasjonsskriv, mulige rettslige grunnlag for å behandle data, vurderinger knyttet til anonymitet og pseudonymisering, muligheten for å tilgjengeliggjøre data, oppfølging av avvik og det skrives også ulike juridiske utredninger og høringsuttalelser.
Utarbeide ulike avtaler knyttet til personvern	Innføringen av personvernforordningen krever at det utarbeides databehandlingsavtaler, avtaler om felles behandlingsansvar, avtaler med underleverandører og ulike standardavtaler eller egenutviklede avtaler i forbindelse med overføringer til tredjeland. I utgangspunktet skal dette gjøres av den som er ansvarlig for behandlingen, men i realiteten blir en av fakultetets jurister bedt om å utarbeide eller gjennomgå avtalene. Disse er ofte tidkrevende å utarbeide ettersom den som utarbeider avtalen må skaffe seg en fullstendig oversikt over hva dataene skal brukes til, dataflyten som gjelder den aktuelle avtalen, kjennskap til andre lands regelverk med mer.
Opplæringsaktiviteter	Dette omfatter både å organisere og utvikle opplæringsaktiviteter rettet mot Helsefak. Helsefak har så langt ikke hatt kapasitet til å gjennomføre opplæring. Ansvaret for mer generelle opplæringsaktiviteter rettet mot hele UiT ligger til FPI. Helsefak jobber med å kjøpe

	inn et foredrag av SIKT rettet mot personvern i helseforskningen.
Oppgaver knyttet til behandlingsprotokollen	Helsefak har ansvar for å føre en komplett oversikt over fakultetets bruk av personopplysninger. Protokollen må tilfredsstillende kravene som stilles i personvernforordningen og UiTs lokale krav.
Ulike kontrollaktiviteter knyttet til informasjonssikkerhet og personvern	Fakultetet skal på oppdrag fra FPI utarbeide en årlig statusrapport for fakultetets arbeid med informasjonssikkerhet og personvern. I tillegg er det kommet nye krav til at det gjennomføres minimum en egeninitiert internkontroll på fakultetet årlig, og at det skal gjennomføres kontroller initiert av FPI. Det er anbefalt at det utarbeides en årsplan for kontrollaktiviteter. Dette kommer i tillegg til fakultetets øvrige kontroller knyttet til Helseforskningsloven og fakultetets internkontrollsystem for helseforskning. De ulike kontrollaktivitetene forutsetter at man har god oversikt over arbeidet med informasjonssikkerhet og personvern på fakultet og instituttene, lovkrav og retningslinjer. Helsefak har så langt ikke hatt kapasitet til å gjennomføre slike kontroller.
Utarbeide påkrevde vurderinger som for eksempel Risikovurderinger og DPIA	Gjennomføre risikovurderinger og DPIA der det er et krav om det.
Arbeid med personvern i Helseregistrene plassert på Helsefak	Juridiske problemstillinger knyttet til personvern og informasjonssikkerhet, herunder vurderinger knyttet til tilgjengeliggjøring, ny bruk, nye data etc.
Ulike eksterne grupper	Helsefak deltar i ulike grupper knyttet til arbeid med personvern og informasjonssikkerhet både internt på UiT og eksternt. Internt på UiT er Helsefak deltaker i informasjonssikkerhetsforum og i fakultetenes representant i personvernombudets DPIA gruppe. I tillegg deltar Helsefak i en lokal gruppe for personvernombud i Tromsø sammen med Sparebank1 Nord- Norge, Tromsø Kommune, UNN og UiTs PVO. Helsefak deltar også nasjonale nettverk sammen med eksempelvis FHI, NTNU, UiO og andre knyttet til personvern og helseforskning. HUNT har videre tatt initiativ til et juristnettverk mellom juristene som jobber med helseregistre og personvern.
Ulike prosjekter initiert fra UiT sentralt	Ulike oppgaver knyttet til personvern og informasjonssikkerhet. Eksempelvis prosjektet knyttet til datamigrering.



Listen over praktiske oppgaver er ikke uttømmende, men gir et bilde av nødvendigheten av at Helsefak har god kompetanse på personvern og informasjonssikkerhet, og at man holder seg løpende oppdatert på endringer og utviklingen av i lover, forordninger, forskrifter, nasjonal og europeisk praksis, lokale retningslinjer og rutiner.

## 5. Nærmere om oppgaver og utfordringer.

### 5.1 Risikostyring

UiT har i sin informasjonssikkerhetsstrategi en målsetning om at UiT skal løfte seg til en mer formalisert og systematisk sikkerhetspraksis. I dette ligger det at UiT skal ha en risikobasert tilnærming til informasjonssikkerhet. For å kunne ha en risikobasert tilnærming er det viktig at UiT og Helsefak har god oversikt over hvilke informasjonsverdier vi har og at det gjøres vurderinger av informasjonsverdiene for å avgjøre hvilke sikkerhetstiltak som er nødvendig. På UiT kategoriseres dette gjennom fargekodene grønn, gul, rød og sort.<sup>5</sup> hvor sort utgjør den kategorien som krever det høyeste nivået av sikkerhetstiltak. I tillegg er det avgjørende for en risikobasert tilnærming til informasjonssikkerhet at Helsefak har god kompetanse når og hvordan man skal gjennomføre risikovurderinger og følge opp disse, herunder hva som er akseptabel risiko for UiT.

#### 5.1.1 Informasjonsverdier

I ITAs årsrapport redegjøres det for UiTs arbeid med å kartlegge informasjonsverdier. Informasjonsverdier er et samlebegrep som inneholder både informasjon og tilhørende støtteverdier. HK Dir har i sin risiko og tilstandsvurdering for 2022 gitt følgende eksempler på hva begrepet informasjonsverdier omfatter.

- Data og opplysninger som virksomhetene behandler, blant annet personopplysninger, forskningsdata, og annen viktig informasjon, og
- Ulike typer digitale ressurser som benyttes i behandlingen av data og opplysninger: datamaskiner, programvare, nettverksutstyr, laboratoriemaskiner, osv.

Ansvaret for å kartlegge informasjonsverdier ligger i hovedsak på ITA, men fakultetene har på oppdrag fra ITA kartlagt sine informasjonsverdier. Helsefak har i sine statusrapporter for 2019, 2020 og 2021 levert oversikt over våre informasjonsverdier. Listen har blitt utarbeidet på grunnlag av Helsefaks kunnskap om aktiviteten på fakultetet og gjennom oppføringer i behandlingsprotokollen. For at Helsefak skal kunne videreutvikle oversikten over våre informasjonsverdier er det viktig at fakultetet har god oversikt over aktivitetene, for eksempel ved at behandlingsprotokollen holdes løpende oppdatert. Behandlingsprotokollen inneholder imidlertid kun en oversikt over informasjonsverdier knyttet til personopplysninger, noe som innebærer at det er vanskelig å ha en komplett oversikt over informasjonsverdier. For eksempel har ikke en systemkatalog over systemer vi er systemeier for.

Oversikt over kartlagte informasjonsverdier på Helsefak:

Kategori	Informasjon	Merknad	Støtteverdi	Klassifisering
Studentadministrasjon	Tilrettelagt undervisning/eksamen		Ephorte, Office 365	Rød
Studentadministrasjon	Skikkethetsvurderinger		Ephorte, Office 365	Rød
Studentadministrasjon	Fuskesaker		Ephorte, Office 365	Rød

<sup>5</sup> Se UiTs retningslinje for klassifisering av informasjon.

Studentadministrasjon	Studentprosjekter			Rød
Læring, vurdering og undervisning	Nettbaserte læringsressurser drevet av Helsefak	Incision		Gul
Forskning og utvikling	Helseregisteropplysninger	Tromsøundersøkelsen, Saminor, Kvinner og Kreft, Fit Future,	Eutro, TSD, krypterte enheter, HUNTCloud, Safe, lagring i instrumenter f.eks på UNN	Sort
Forskning og utvikling	Forskningsdata - Personopplysninger		TSD, Office 365, HUNTCloud	Rød

Arbeidet med å kartlegge informasjonsverdier er viktige for at UiT skal kunne treffe informerte valg knyttet til risiko, men det er også avgjørende for Helsefaks arbeid med informasjonssikkerhet og personvern at vi har en god oversikt over egne informasjonsverdier. For eksempel er det gjennom kartleggingen av informasjonsverdier blitt tydelig at enkelte data i en av befolkningsundersøkelsene lagres i instrumenter hos UNN. Dette er data UiT er behandlingsansvarlig for, men hvor vi ikke garantere for informasjonssikkerheten da utstyret er utenfor Helsefaks kontroll. Eksempelvis kan utstyret byttes ut av UNN med risiko for at dataene går tapt.

### 5.1.2 Risikovurderinger

#### 5.1.2.1 Gjennomføring av risikovurderinger

Gjennomføring av risikovurderinger er i tillegg til oversikt over informasjonsverdiene sentralt i risikobasert styring. Gjennom risikovurderinger vil man kunne avdekke potensielle trusler mot informasjonssikkerheten og personopplysningssikkerheten, man vil også kunne sette inn risikoreduserende tiltak for å redusere skadepotensialet innenfor akseptable rammer.

På UiT er det tatt inn krav til gjennomføring i risikovurderinger i ISMS kapittel 5, hvor det går frem at det skal gjennomføres risikovurderinger:

- Når trusselbildet endres
- Før oppstart av behandling av personopplysninger
- Ved oppstart av forskningsprosjekter
- Ved etablering eller endring av IKT- systemer
- Ved organisatoriske endringer som kan påvirke informasjonssikkerheten.

I ITAs årsrapport redegjøres det for at det har vært en markant bedring de senere år i gjennomføringen av risikovurderinger ved UiT, men at det er et stykke igjen. I tillegg vises det til at det knytter seg store utfordringer til å bygge opp tilstrekkelig kompetanse ute på enhetene til at slike vurderinger kan gjennomføres, samt at den største utfordringen er å få risikovurderinger til å bli en del av den naturlige arbeidsprosessen til ansatte ved UiT.

For Helsefak innebærer kravene til risikovurderinger at fakultetet hvert år skal gjennomføre svært mange risikovurderinger. Helsefak starter for eksempel hvert år opp mange nye forskningsprosjekter som skal risikovurderes, vi etablerer eller gjør endringer i mange IKT- systemer og vi starter årlig

mange nye behandlinger av personopplysninger. Helsefak har hatt utfordringer med å få gjennomført risikovurderinger i alle tilfeller hvor dette skal gjøres.

Helsefaks har ikke en komplett oversikt over alle tilfeller hvor det skulle vært gjennomført risikovurderinger, men kun en oversikt over forskningsprosjekter. Ettersom gjennomførte risikovurderinger også omfatter nye systemer etc og ikke bare nye forskningsprosjekter, gir ikke tabellen et riktig bilde, men den gir likevel et bilde på statusen ved Helsefak.

År	Antall risikovurderinger	Registrerte prosjekter	Andel risikovurderte prosjekter
2019	4	119	3,4 %
2020	7	87	8%
2021	23	88	26,1%
2022 (per 11.07)	7	44	15.9%

Utfra oversiktene over nye forskningsprosjekter er det tydelig at Helsefak ennå ikke har lyktes med å få risikovurderinger til å bli en del av den naturlige arbeidsprosessen for våre ansatte. Helsefak har etter 2020 hatt økt fokus på risikovurderinger ved at det eksempelvis gis veiledning knyttet til risikovurderinger, to av fakultetets ansatte har veiledning omkring risikovurderinger som en del av sine arbeidsoppgaver, kravet til risikovurderinger går frem av sjekklister og det jobbes med forenklede risikovurderinger for masterprosjekter. Fra 2020 til 2021 hadde fakultetet mer en enn tredobling av antallet risikovurderinger, og selv om tallet skulle vært høyere for å innfri kravene som stilles i ISMS så kan man si at dette var et stort steg i riktig retning. Tallene så langt for 2022 indikerer imidlertid at denne utviklingen ikke har fortsatt i 2022 og det er derfor fremdeles behov for at Helsefak har fokus på hvordan man kan følge opp kravet til gjennomført risikovurdering.

Hva som er grunnen til at det er vanskelig å få innført risikovurderinger som en naturlig del av arbeidsprosessen er vanskelig å identifisere, og bildet er nok sammensatt. En hovedutfordring kan knytte seg til kompetanse. Det kan dreie seg både om kompetanse om at det faktisk skal gjennomføres risikovurderinger, og det kan handle om at man opplever å ha manglende kompetanse til å gjennomføre en prosess med risikovurderinger. Når det gjelder utfordringen med kompetanse til selve gjennomføringen av risikovurderingen har Helsefak satt inn tiltak ved at to av våre ansatte har som en av sine oppgaver å bidra inn i risikovurderinger der det er behov for det. Det vil si at man kan veilede på hvordan man kommer i gang, gi råd knyttet til fagpersoner man bør involvere i vurderingen (eks, teknisk og juridisk kompetanse) og bistand til den faktiske gjennomføringen av prosessen og bistand til skrivingen av rapporten som følger av risikovurderingen.

Når det gjelder kompetanse knyttet til at risikovurderinger skal gjennomføres er dette en opplæring som bør gis til hele UiT og ikke bare lokalt på Helsefak, ettersom utfordringen med å bygge risikovurderinger som en naturlig del av arbeidsprosessen gjelder hele UiT og ikke bare Helsefak. Helsefak har foreslått at risikovurderinger kan tas inn som tema for sikkerhetsmåneden 2022.

Gjennomføringen av risikovurderinger er tidkrevende særlig for de to ansatte på fakultetet som gir bistand til risikovurderinger som en del av stillingen sin, og for fakultetets jurister som deltar i mange av risikovurderingene. Dette er tid som de ansatte må ta fra andre oppgaver de også skal løse.

#### *5.1.2.2 Oppfølging av risikovurderinger.*

For at risikovurderinger skal være effektive er det viktig at man følger opp at risikoreduserende tiltak iverksettes, at tiltakene har ønsket effekt og at man oppdaterer risikovurderingen fortløpende

dersom risikobildet skal endre seg. En risikovurdering er med andre ord ikke statisk dokument, men et arbeidsdokument som man må ta frem gjennom hele arbeidsprosessen.

Ettersom arbeidet med risikovurderinger enda er i startgropen, har fakultetet ikke oversikt om tiltakene i gjennomførte risikovurderinger følges opp, om de arkiveres eller om de justeres i tråd med endringer i risikobildet. Helsefak har per i dag ikke kapasitet til å følge opp gjennomførte risikovurderinger.

## 5.2 Avviksmeldinger

Uansett hvor gode systemer og retningslinjer en institusjon har, vil det alltid forekomme ulike avvik, for eksempel på grunnlag av menneskelig svikt eller systemsvikt. Avviksmeldinger er nødvendige for å kunne forbedre og videreutvikle rutineene. Noen eksempler på hendelser og avvik er:

- tyveri av datautstyr
- misbruk av IT-tjenester
- misbruk av passord
- fakturasvindel
- dataangrep
- datalekkasje
- løsepengevirus
- svakheter i IT-systemer
- brudd på eller manglende rutiner ved UiT
- fortrolig informasjon på avveie
- uautorisert tilgang til opplysninger
- bruk av databehandler uten tilstrekkelig avtale
- innsamling av personopplysninger utover det man hadde legitim bruk for (brudd på dataminimeringsprinsippet)
- behandling av personopplysninger uten lovlig grunnlag, herunder viderebehandling til nye formål uten at man har lovlig adgang til dette

Listen er ikke uttømmende.

### 5.2.1 Helsefaks avviksmeldinger

Årlig mottar ITA 15-25 avvik knyttet til personvern og informasjonssikkerhet. Helsefaks andel av dette er normalt 5-6 avvik. Fakultet blir imidlertid jevnlig koblet på andre saker som egentlig skulle vært meldt som avvik, eksempelvis:

- Personopplysninger sendes ut av EU/EØS i forskningsprosjekter uten at det er gjort vurderinger om det finnes overføringsgrunnlag
- Humant biologisk materiale sendes ut av EU/EØS for analysering som utleder personopplysninger uten at det er gjort vurderinger om det finnes overføringsgrunnlag
- Personopplysninger i forskningsprosjekt gjenbrukes til nye forskningsprosjekt uten at det er gjort vurderinger om det er adgang til dette
- Røde og sorte data behandles på utstyr som kun er godkjent for gule data
- Det inngås ikke databehandleravtaler
- Forskningsprosjekt starter opp uten at det er gjennomført risikovurderinger
- Pasientopplysninger oppbevares i studentskap

At det meldes få avvik på Helsefak kan ha flere årsaker. I enkelte tilfeller erfarer vi at det ikke er tilstrekkelig kompetanse knyttet til avvikssystemet for informasjonssikkerhet og personvern,

herunder hva som skal meldes og hvor det skal meldes. I noen tilfeller har man meldt avvik, men har en opplevelse av at de ikke blir fulgt opp videre. I andre tilfeller er man klar over avviket, men velger å begrense avviket selv fremfor å melde det inn. Dette kan for eksempel skyldes at det å melde avvik er så komplisert at man finner andre måter å håndtere det på.

Når avviket ikke meldes så mister UiT muligheten til å gjøre vurderinger knyttet til hvorvidt systemene og rutinene våre fungerer etter hensikten, man mister muligheten til å sette inn tiltak for å forhindre lignende hendelser på andre institutt eller fakultet og man mister muligheten til å vurdere de mulige skadene etter avviket. Ved å ikke melde avvik reduseres muligheten til å jobbe med en risikobasert tilnærming, og isteden jobber man fragmentert med skadebegrensning. Manglende avviksmeldinger kan også innebære at man ikke klarer å overholde meldeplikten til datatilsynet eller plikten til å orientere den opplysningene gjelder.

Det vurderes slik at utfordringene med meldekultur slik de belyses i PWCs internrevisjonsrapport og ITAs årsrapport også gjør seg gjeldende for Helsefak. Dette kan også illustreres av at avvikene som faktisk meldes 5 har en slik alvorlighetsgrad at man ikke kommer utenom at avvikene blir meldt, noe som er et uttrykk for mangler ved meldekulturen. Utfordringene med meldekulturen kommer også frem når det gjelder å melde avvik knyttet til helseforskning, der Helsefak til nå ikke har mottatt noen avviksmeldinger de siste 10 årene.

Det vurderes slik at man bør øke bevisstheten omkring avviksmeldinger for å bedre meldekulturen blant ansatte på Helsefak. I stor grad er dette en informasjonskampanje som bør gjelde hele UiT og ikke bare Helsefak, og Helsefak har foreslått at dette er tema for informasjonssikkerhetsmåned i 2022. I tillegg bør Helsefak også innenfor egnende forum på fakultetet orientere om avvik og avvikshåndtering både innenfor personvern og informasjonssikkerhet, men også helseforskning som i noen grad har overlappende problemstillinger.

### 5.2.2 Avvikssystemer

ITA har uttrykt at UiT har utfordringer knyttet til systemet for å melde avvik. Det vises her til at UiT har mange ulike systemer for å melde avvik og at dette gjør det vanskelig for ansatte og navigere i systemet. Eksempelvis er det ulike systemer for HMS avvik, Informasjonssikkerhet og personvern, Helseforskning og varslingssaker. Helsefak har gjennom statusrapporten uttrykt samme bekymring i rapportene for 2021 og 2020.

I tillegg til at det er vanskelig å navigere mellom avvikssystemene har Helsefak i statusrapportene meldt inn at avvikssystemet for personvern og informasjonssikkerhet ikke gir oss den tekniske støtten til å følge opp enhetsleders ansvar for å sørge for at Helsefak etterlever kravene til personvern og informasjonssikkerhet i det daglige arbeidet. Slik systemet nå er bygget opp, har ikke Helsefak oversikt over hvilke avvik som meldes og som knytter seg til Helsefak. Avvikene følges normalt opp med leder på instituttet og fakultetet har derfor ikke full oversikt. Uten den fullstendige oversikten vil ikke enhetsleder kunne treffe nødvendige tiltak for å sikre at kravene til informasjonssikkerhet og personvern etterleves. Helsefak har fått avklart at vi får tilgang til avvikene ved å kontakte FPI. I påvente av en teknisk løsning bør Helsefak lage et manuelt system hvor vi regelmessig innhenter oversikt over meldte avvik og gjør vurderinger knyttet til tiltak basert på en egen oversikt. En utfordring i denne sammenhengen er at Helsefak ikke har nødvendige ressurser til å følge opp avvik på et overordnet nivå.

Hvorfor det er viktig for fakultetet å ha denne oversikten kan illustreres med et eksempel fra Helsefak. I forbindelse med klipping av låser på studentskap fant Helsefak helseopplysninger om over 30 pasienter i forbindelse med studentpraksis. Dette var et brudd på Helsefaks rutiner. Dette ble

vurdert som et enkeltstående tilfelle ettersom man ikke hadde informasjon om tilsvarende avvik fra tidligere. Noen dager senere ble det imidlertid funnet samme typen helseopplysninger i ytterligere to studentskap. Dette gjaldt en annen enhet ved Helsefak og ettersom samme person avdekket avvikene og kontaktet samme person på fakultetet kunne man se at man her ikke lengre snakket om et enkeltstående avvik på ett institutt, men muligens en mer gjennomgående utfordring på tvers av institutter og enheter. I samtaler ble det klart at man også tidligere hadde gjort denne typen funn, men da hadde man håndtert dette ved å eksempelvis makulere dokumentene. De tidligere funnene har ikke vært meldt som avvik, og man er derfor usikker på i hvilket omfang dette har skjedd. Den samlede informasjonen gjorde det nødvendig å vurdere tiltak på tvers av institutter og enheter ved Helsefak slik at man kan redusere risikoen på samtlige institutt og enheter og ikke bare de involverte instituttene.

### 5.3 Kontrollaktiviteter

UiT stiller krav til at Helsefak utfører årlige kontrollaktiviteter knyttet til personvern og informasjonssikkerhet.<sup>6</sup> Enkelte kontrollaktiviteter skal utføres fast, mens andre kontrollaktiviteter kan initieres av fakultet eller FPI utfra behov. Ansvar på fakultetet er lagt til dekan, men oppgavene kan delegeres til andre eksempelvis fakultetsdirektør og instituttleder. Det anbefales at man lager rutiner på fakultet ved behov for det. Det er per i dag ikke gjort noen skriftlige eller sporbare delegasjonsvedtak fra dekan til andre.

Siden 2019 har Helsefak levert statusrapport for informasjonssikkerhet og personvern som en fast kontrollaktivitet. Rapporten er tidkrevende og krever god oversikt over all aktivitet på fakultetet, samt krav i lov, forskrift og sentrale og lokale retningslinjer.

Fra juni 2022 er det tatt inn et krav om at fakultetet skal gjennomføre minst en egeninitiert internkontroll knyttet til personvern og informasjonssikkerhet per år. Denne kontrollen skal utføres ved behov, men minimum en gang per år. For eksempel kan denne typen kontroller omfatte tema som:

- Gjennomføres det risikovurderinger i de tilfellene det skal gjøres.
- Behandles registerdata fra eksterne i samsvar med vedtaket, f.eks. slettes dataene i samsvar med kravene fra registreier.
- Tilgangsstyringen i systemer vi har systemansvar for. Eksempelvis Hunt Cloud, Eutro etc
- Er det tegnet databehandleravtaler
- Kontroll med data registrert i meldingsarkivet.
- Utleveres data fra Helsefaks Helseregistre i samsvar med gjeldende lovkrav.

I tillegg er det anbefalt at Helsefak utarbeider en plan for gjennomføring av kontrollaktiviteter. I informasjonssikkerhetsforum har det blitt orientert om at man ønsker en rolig innføring av fakultetenes kontrollaktiviteter, og at det for fremtiden vil komme ytterligere krav til gjennomføring og hyppighet. For eksempel er statusrapporten utvidet fra kun å omhandle informasjonssikkerhet til nå også å omfatte personvern.

Utover å utarbeide statusrapport for personvern og informasjonssikkerhet har ikke Helsefak tidligere utført kontroller knyttet til dette temaet. Dette er følgelig en ny oppgave som krever at man har

---

<sup>6</sup> [Retningslinje for UiTs kontrollaktiviteter innenfor informasjonssikkerhet og personvern - vedtatt 30-6-22.pdf](#)

klarer å identifisere temaer for kontroll, samt å gjennomføre kontrollaktiviteten og skrive rapport etter kontrollen.

For Helsefak gir dette flere utfordringer. For eksempel må man ta stilling til hvordan det skal jobbes med kontrollaktiviteter, og hvorvidt det skal utarbeides rutiner for dette arbeidet. I tillegg må man avklare hvilke ressurser som skal brukes i dette arbeidet. Per i dag har juristene på fakultetet utarbeidet statusrapporten og lagt denne frem for fakultetsstyret, men juristene har ikke hatt andre kontrolloppgaver innenfor informasjonssikkerhet og personvern. Dersom man kommer til at juristene skal gjennomføre kontrollaktivitetene generelt, må fakultetet ta stilling til hvilke andre arbeidsoppgaver man ikke lengre skal løse. For eksempel har ikke fakultetets jurister per i dag kapasitet til å følge opp internkontrollaktivitetene fakultetet er pålagt på helseforskningsområdet på grunn av den økte aktiviteten på området for personvern og informasjonssikkerhet.

#### 5.4 Opplæringsaktiviteter

FPI har etter ISMS ansvar for å drive med opplysningsarbeid, rådgivning og opplæring knyttet til personvern og informasjonssikkerhet. Faggruppen er også ansvarlig for å legge til rette for opplæring. Enhetslederne har på sin side ansvar for å informere egne ansatte om interne rutiner og retningslinjer som til enhver tid gjelder. På Helsefak har det vært lagt til grunn at FPI har hatt opplæringsansvaret og Helsefak har følgelig ikke en plan for opplæring innenfor informasjonssikkerhet og personvern. Av PWCs internrevisjonsrapport kommer det imidlertid frem at det er en forventning fra nivå 1, ved FPI, at den faktiske gjennomføringen av opplæringen skjer i linjen.

Helsefak har som nevnt ikke laget en plan for opplæring innenfor personvern og informasjonssikkerhet, men har drevet opplæringsvirksomhet sporadisk på forespørsel, normalt knyttet til enkeltsaker. Helsefak har fra høsten 2022 planlagt en 90 minutters opplæring innenfor Personvern og informasjonssikkerhet knyttet til vår forskningsaktivitet. Helsefak har leid inn SIKT til å holde opplæringen, blant annet grunnet manglende kapasitet til selv å utvikle og holde kurs. Per i dag har ikke Helsefak rutiner for opplæringsaktiviteter, eller plassert ansvaret for hvem som skal gjennomføre opplæring.

## 6. Organisering av arbeidet med personvern og informasjonssikkerhet på Helsefak.

### 6.1 Ressurser

Helsefak er UiTs største fakultet, og en stor andel av fakultetets oppgaver involverer informasjonssikkerhet og personvern. For eksempel håndterer fakultetet store mengder helseopplysninger i forbindelse med forskning og utdanningsaktivitet og de fire helseregistrene (Tromsøundersøkelsen, Kvinner og kreft, Saminor og Fit Futures).

Arbeidsoppgavene knyttet til personvern og informasjonssikkerhet har økt etter innføringen av personvernforordningen og i etterkant av at det operasjonelle ansvaret for området ble flyttet til FPI. I hovedsak er det prosjektledere som har et særskilt ansvar i forskningsprosjekter, og det legges til grunn at det for øvrige oppgaver følger en del ansvar gjennom lederlinjene i fakultetet. Økningen i oppgaver innebærer imidlertid økt behov for bistand fra fakultetet i forbindelse med ulike oppgaver i tillegg til at enkelte oppgaver løses på fakultetsnivå.

Følgende ressurser er avsatt i dag på fakultetsnivå til å jobbe med informasjonssikkerhet og personvern:

- To ansatte i Prosjektkontoret gir råd og veiledning knyttet til risikovurderinger. Dette er anslått til å utgjøre en liten del av disse stillingene, anslagsvis 25-30 % per stilling
- En juridiskressurs som gir råd og veiledning, samt utarbeider rapporter. Dette ble anslått til å utgjøre ca. 10 % av stillingen.

Kartlegging av faktisk ressursbruk viser at den juridiske ressursen benytter ca. 40-50 % av stillingen til veiledning og rådgivning innenfor personvern og informasjonssikkerhet til ansatte alene. I tillegg kommer andre oppgaver som deltakelse i informasjonssikkerhetsforum, DPIA gruppe, arbeid med behandlingsprotokoll, oppgaver fra FPI, samarbeidsmøter etc. Fakultetets andre jurist bruker også av sine ressurser på problemstillinger knyttet til personvern og informasjonssikkerhet, i tillegg til at majoriteten av dennes kapasitet benyttes til lederoppgaver og andre juridiske oppgaver. Manglende kapasitet til å følge opp tiltak i gjennomførte risikovurderinger, viser også at det er behov for mer ressurser.

Dette medfører at Helsefak per i dag må nedprioritere andre oppgaver slik som utviklingsarbeid innenfor helseforskningsrutinene og internkontrollaktiviteter innenfor helseforskning. Dette til tross for at Helsetilsynets tilsyn av Helsefak viser at fakultetet ikke følger opp helseforskningsprosjektene i tilstrekkelig grad og har flere avvik. Helsefaks jurister får heller ikke løst andre oppgaver som etterspørres innenfor personvern og informasjonssikkerhet, eksempelvis informasjons- og opplæringsaktivitet. Det må her bemerkes at juristene på Helsefak har en svært stor og variert oppgaveportefølje som blant annet omfatter avtaler og kontrakter, vitenskapelig uredelighet, samt at oppfølging av helseregistrene er en stor og tidkrevende oppgave.

Det vurderes slik at fakultetet har for liten juristkapasitet slik arbeidsmengden er i dag, og det er tydelige signaler på at disse oppgavene også vil øke i fremtiden. Eksempelvis økte kontrollaktiviteter, rutineutvikling, avviksoppfølging etc. Det kan også i denne sammenheng vises til internrevisjonsrapporten til PWC hvor det påpekes at det faktisk at enhetene har ulike behov og varierende kompleksitet med tanke på ivaretagelse av kravene til informasjonssikkerhet og personvern bør være førende for dimensjoneringen. Helsefak har ikke klart å fremskaffe en oversikt over de ulike fakultetenes ressursbruk knyttet til personvern og informasjonssikkerhet, men ettersom oppgavemengden og kompleksiteten av oppgavene varierer mellom fakultetene, vil heller ikke en slik oversikt kunne danne grunnlag for Helsefaks ressursbruk. For eksempel har Helsefak behov for å gi fortløpende komplekse juridiske utredninger, mens andre fakultet aldri eller sjelden har behov for å gi slike komplekse juridiske råd. Helsefaks ressursbruk bør ta utgangspunkt i oppgavene vi har ansvar for å løse. Sett i lys av Helsefaks størrelse, kompleksitet og oppgavemengde bør man se på hvorvidt det er tilstrekkelig at Helsefak har avsatt 10 % av den ene juriststillingen til å løse oppgavene knyttet til personvern og informasjonssikkerhet innenfor de rammene og kvaliteten som forventes. Dette bør særlig ses i lys av at den ene juristen alene bruker 40-50% av tiden sin på oppgaver innenfor personvern og informasjonssikkerhet, og at denne tidsbruken kun er tilstrekkelig for å løse fortløpende henvendelser fra forskere, studenter og instituttledere, men ikke faste oppgaver som arbeid med behandlingsprotokoll, opplæringsaktivitet, kontrollaktivitet etc.

Det er dermed i dag ikke avsatt tilstrekkelige ressurser til å arbeide med informasjonssikkerhet og personvern på fakultetet til å løse alle oppgavene som det stilles krav til at vi løser. Det må derfor tas i betraktning ved forslag til øvrige tiltak at det avsettes mer ressurser til dette arbeidet, enten ved nytilsetting eller omprioritering av eksisterende ressurser. Det er vanskelig å anslå hvor mye ressurser det er behov for, da det er mange av oppgavene som ikke løses i dag og fordi det er mye



mørketall i forhold til avvik. Det foreslås derfor at ressursbehovet løses ved å øke bemanningen med én stilling i første omgang, og at det videre ressursbehovet evalueres samtidig som neste års årsrapport legges frem for fakultetsstyret.

## 6.2 Organisering

Helsefak har per i dag ikke egne rutiner for behandling av saker knyttet til personvern og informasjonssikkerhet. Det innebærer at Helsefaks organisering av arbeidet følger ISMS, som er et overordnet styringssystem. Selv om man i ISMS har både styrende, gjennomførende og kontrollerende deler, har ikke ISMS tilstrekkelige gjennomgående rutiner til å regulere fakultetets arbeid med informasjonssikkerhet. ISMS stiller krav til at enhetene skal ha egne rutiner for den gjennomførende delen av arbeidet med personvern og informasjonssikkerhet dersom det er behov for det. Hvordan Helsefak velger å organisere og strukturere arbeidet med personvern og informasjonssikkerhet er viktig både for at arbeidet skal være tilstrekkelig formalisert, men også fordi det er avgjørende for hvorvidt oppgavene løses innenfor lovkrav, forskriftskrav og retningslinjer.

For eksempel oppstiller personvernforordningen en plikt for virksomheter å føre en behandlingsprotokoll, det vil si en komplett oversikt over all bruk av personopplysninger, inkludert hjemmel for å behandle opplysningene, hvordan man behandler opplysningene, hvem som har tilgang til opplysningene med mer. ISMS og øvrig dokumentasjon på UiT sier ikke noe om hvordan arbeidet med protokollen skal organiseres, utover at ansvaret for det praktiske arbeidet ligger til dekan. Man kan si at ansvaret for å avdekke og følge opp endringer i behandlingsaktiviteten på Helsefak følger linjeledelsen, men protokollen føres likefult ikke av linjeledelsen. For Helsefak er det viktig at behandlingsprotokollen er så komplett som mulig da den i tillegg til å svare på krav i personvernforordningen, gir et godt bilde av fakultetets informasjonsverdier. Ettersom arbeidsflyten omkring behandlingsprotokollen ikke er formalisert er det svært mange på Helsefak som ikke vet at protokollen eksisterer, hva den inneholder og at man må melde fra om nye, endrede eller avsluttede behandlinger som omfatter personopplysninger. Siden 2020 har ikke den ansatte som fører protokollen til fakultetet fått melding om endringer i behandlingsaktiviteten fra linjeledelsen. Hvorvidt Helsefaks behandlingsprotokoll er komplett avhenger derfor av hvorvidt personen som fører protokollen kjenner aktivitetene på fakultetet og instituttene godt nok og får dette ført i behandlingsprotokollen.

Det er heller ikke formalisert at fakultetet skal tilby støttetjenester til instituttledere, prosjektleder og andre ansatte. Dette gjør at støtten som tilbys avhenger av hvem som tilfeldigvis er kjent med eller kommer i kontakt med noen som kjenner til støttetjenestene som tilbys, som igjen kan bety at støttetjenestene ikke tilbys til alle som har behov for det.

## 7. anbefalinger

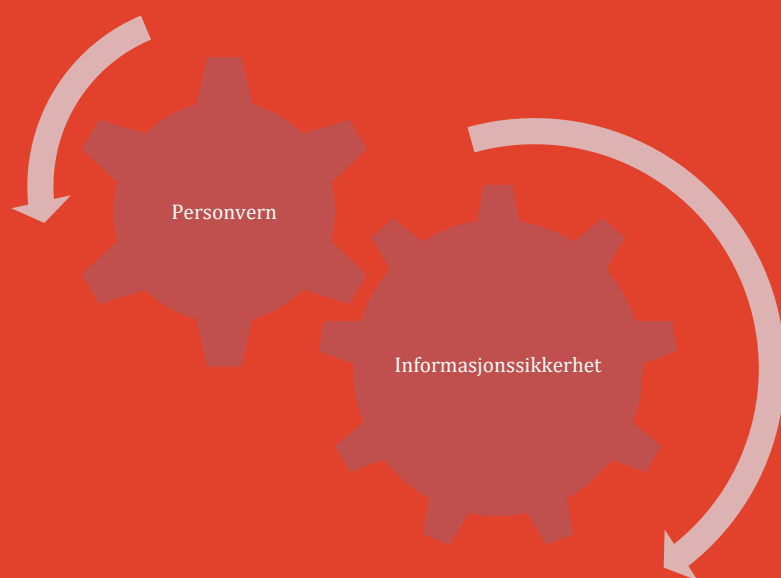
1. Helsefak skal tydeliggjøre hvilke konkrete oppgaver fakultetet har ansvar for innen personvern og informasjonssikkerhet og hvem som har delegert ansvar til å løse oppgavene.
2. Helsefak skal formalisere hvordan fakultetet skal jobbe med informasjonssikkerhet og personvern gjennom å blant annet utarbeide retningslinjer. Retningslinjene bør også omfatte hvordan det skal jobbes med opplæringsaktiviteter og hvem som har ansvaret for dette.
3. Fakultetsstyret ber dekanen styrke arbeidet med informasjonssikkerhet og personvern med prioritering av ressurser til å følge opp rapportens hovedkonklusjoner.

---

# Årsrapport informasjonssikkerhet og personvern 2021

Rektor, Avdeling for IT (ITA), 10.2.22

Ephorte 2021/5061



# Innholdsfortegnelse

1	Oppsummering.....	1
2	Bakgrunn.....	3
3	Risikobildet for UiT.....	4
3.1	Informasjonsinnhenting og påvirkning .....	5
3.2	Digital utpressing .....	7
3.3	Schrems II .....	9
4	Oppfølging av årsrapport 2020 .....	12
5	Hendelser og avvik .....	19
5.1	Oppsummering.....	19
5.1.1	Sikkerhetshendelsen høsten 2020 .....	20
5.2	Korona.....	29
6	Styring og kontroll.....	30
6.1	Risikostyring .....	30
6.1.1	Informasjonsverdier .....	31
6.1.2	Risikovurderinger .....	32
6.1.3	Håndtering og oppfølging av risikoer.....	33
6.2	IKT-sikkerhet .....	33
6.3	Statusrapport enhetene .....	35
6.4	Internrevisjon .....	36
6.5	Årsrapport personvernombudet.....	38
6.6	Behov for ytterligere kontrollaktiviteter .....	38
7	Ressurs- og kompetansebehov.....	39
7.1	IKT-sikkerhet .....	39
7.2	Enhetene .....	39
7.3	Opplæringsaktiviteter .....	39
8	Revisjon av ledelsessystemet.....	41
	Vedlegg.....	42

# 1 Oppsummering

*I Styringsdokument for arbeidet med sikkerhet og beredskap i Kunnskapsdepartementets sektor understreker departementet at de har økt oppmerksomhet til informasjonssikkerhet og personvern «som følge av et skjerpet digitalt risikobilde, og forventer at arbeidet med informasjonssikkerhet og personopplysningssikkerhet gis høy prioritet hos alle virksomheter i sektoren», og understreker at det er toppledelsens ansvar for at det er nok ressurser til at det arbeides tilfredsstillende med informasjonssikkerheten og personvernet.*

Universitetsstyret har ansvaret for at UiT ivaretar informasjonssikkerhet og personvern på en tilfredsstillende og forsvarlig måte. Gjennom årsrapporten for informasjonssikkerhet og personvern ved UiT får styret status på arbeidet innenfor disse områdene, og mulighet til å følge opp sitt ansvar.

Årsrapporten for 2021 beskriver blant annet sentrale deler av risikobildet for UiT, avvik og hendelser, oppfølging av kontrollaktiviteter samt en gjennomgang av ressursbehov.

UiT har arbeidet målrettet og strukturert med informasjonssikkerhet og personvern de senere år. Det har vært klare forbedringer i systematikk og helhet i arbeidet, og på flere felt har universitetet sterkt forbedret sin posisjon. Denne oppfatningen er understøttet både av tilbakemeldinger fra Unit (nå HK-dir), gjennom deres årlige kartleggingsmøter i forbindelse med sektorstyringen av informasjonssikkerhet og personvern i UH-sektoren, og av PwCs internrevisjonsrapport.

Selv om UiT var på svært god vei var ikke arbeidet kommet langt nok da UiT ble rammet av en alvorlig sikkerhetshendelse høsten 2020. I 2021 har arbeidet med informasjonssikkerheten vært preget av denne hendelsen, og det har blitt gjennomført en rekke tiltak for forbedring av IKT-sikkerheten.

I likhet med for de fleste andre virksomheter har risikobildet endret seg markant for UiT de siste årene. Dette skyldes ikke ensidig utviklingen på trusselaktørenes side, ved at de blir mer ressurssterke, målrettede og profesjonaliserte, men også endringer i måten vi arbeider og studerer på med flere og flere digitale tjenester, økt mobilitet mv.

Gjennom årene er det gjort fortløpende tiltak for å styrke sikkerheten og oppdatere infrastruktur og lignende. Imidlertid har flere grunnleggende forutsetninger og prinsipper om hvordan UiTs digitale infrastruktur og driftsmiljø skal bygges opp og driftes ligget fast i bunn.

Endringer i risikobildet gjør at disse forutsetningene og prinsippene må revurderes. I 2021 foretok UiT en grunnleggende endring i hvordan vi tillater at våre interne nett og tjenester kommuniserer med internett. Selv om ikke dette vises så tydelig i hverdagen for den enkelte ansatte og student var det en svært omfattende operasjon, og den største endringen i nettinfrastrukturen siden UiT koblet seg til internett på nittitallet.

Flere slike omfattende revurderinger må tas, og det er identifisert enkelte tyngre og ressurskrevende tiltak innenfor teknisk/IKT-sikkerhet som må gjennomføres i 2022.

Våren og høsten 2021 gjennomførte PwC internrevisjon av *ledelsessystem for informasjonssikkerhet og personvern*. Revisjonsrapporten inneholdt ingen større overraskelser, men en rekke nyttige anbefalinger som vil bli fulgt opp gjennom 2022. Den samlede vurderingen til PwC var at UiT har jobbet godt med informasjonssikkerhet og personvern over tid.

For å kunne vite hva man skal sikre samt hvordan og mot hvem, er det essensielt å vite hva man har. Siden 2019 har UiT strukturert kartlagt informasjonsverdiene gjennom en årlig statusrapport fra enhetene, hvor de også foretar en vurdering av egne sårbarheter, tiltak og en vurdering av egen tilstand og status. Denne har blitt levert årlig av alle fakultetene, UMAK og UB. Fra og med 2021 skulle også avdelingene i fellesadministrasjonen under universitetsledelsen levere. Alle enheter bortsett fra Avdeling for bygg og eiendom har levert, se kap. 6.3. Hovedformålet er at enhetene selv skal ha oversikt og et bevisst forhold til hvilke verdier som forvaltes og hvordan det skal gjøres. I tillegg får også UiT en samlet oversikt, og mulighet til å vurdere om informasjonsverdiene ivaretas godt nok. For å lykkes fullt ut med dette arbeidet er det sentralt at alle enhetene leverer årlig.

I likhet med 2020 har 2021 har vært preget av korona. De største omveltningene med betydning for informasjonssikkerhet og personvern fant sted i 2020, og for 2021 har det mer vært tale om en videreføring av de prosesser og systemer som ble etablert da. Problemstillinger og utfordringer som korona har skapt for informasjonssikkerhet og personvern vies derfor ikke like mye plass i denne årsrapporten som i 2020-rapporten.

I 2021 igangsatte UiT et arbeid for å ta en mer helhetlig og strukturert tilnærming til problemstillingene internasjonalisering kan skape for særlig informasjonssikkerheten. Dette har ikke blitt mindre aktuelt gjennom året som har gått, og blant annet kan de foreslåtte endringene i eksportkontrollregelverket få betydning for universitetene.

I løpet av 2022 må det utarbeides en ny strategi og der nåværende strategi kun dekker informasjonssikkerhet skal den nye også omfatte personvern. Dette blir første gang UiT får en samlet strategi for informasjonssikkerhet og personvern, og det vil være et viktig bidrag for å klare å ha en helhetlig tilnærming til disse temaene.

## 2 Bakgrunn

Det følger av *Ledelsessystemet for informasjonssikkerhet og personvern*, kapittel ni, at det skal utarbeides årsrapport som gjennomgår UiTs arbeid med informasjonssikkerhet og personvern og denne skal legges frem for Universitetsstyret. Personvernombudet utarbeider sin egen rapport som også fremmes styret.

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 i korte trekk å sikre at informasjon i alle former

- ikke blir kjent for uvedkommende (**konfidensialitet**)
- ikke blir endret utilsiktet eller av uvedkommende (**integritet**)
- er tilgjengelig ved legitimt behov (**tilgjengelighet**)

I utgangspunktet er disse tre aspektene ansett som like viktige, og det er ingen intern rangering blant dem. Hvilket aspekt som i hvert enkelt tilfelle skal veie tyngst i vurderinger av håndtering av risiko beror på informasjonens art, formålet med behandlingen av informasjonen og konsekvenser ved brudd. Det er sjelden til aldri mulighet for å ivareta alle tre aspekter like godt, da de ofte vil gå på bekostning av hverandre. Mange kan ha en tendens til å alltid likestille informasjonssikkerhet med ivaretagelse av konfidensialitet, og kun det. Det er viktig at denne tilbøyeligheten endres.

Informasjonssikkerhet er en viktig del av ivaretagelse av personvernet, og følgerlig sentrale forpliktelser etter personopplysningsloven og personvernforordningen (GDPR). Imidlertid skal sikkerheten også ivaretas for informasjon som *ikke* inneholder personopplysninger, slik som eksempelvis 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 av opplysninger og enkeltpersoners rettigheter skal ivaretas (slik som informasjonssplikt, rett til innsyn, sletting etc). Dette er ikke en direkte del av *informasjonssikkerheten*, men blant de øvrige, sentrale forpliktelser UiT er underlagt etter lovverket 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 håndteringen av disse fagområdene, og UiTs daværende ledelsessystem for informasjonssikkerhet ble derfor utvidet til å også omfatte personvern. Det er en pågående prosess å få revidert hele ledelsessystemet slik at alle deler gjenspeiler denne utvidelsen.

### 3 Risikobildet for UiT

Det er avgjørende å ha forståelse av hvilket risikobilde UiT står overfor når man vurderer om organiseringen, ressursbruken og fokus innenfor arbeidet med informasjonssikkerhet og personvern er hensiktsmessig og tilstrekkelig.

Ofte vil vurdering og presentasjon av risikobildet i stor grad omhandle interne og eksterne trusler som kan lede til brudd på informasjonssikkerheten. Denne rapporten skal imidlertid også omhandle personvern utover sikkerhetsaspektet alene, og det vil dermed være aktuelt å ta med også andre typer risikoer. Eksempelvis risikoen ved at regulatoriske krav er høyere enn hva UiT klarer oppfylle. Og at blir aktiviteten ved universitetet følgelig blir skadelidende ved at prosesser og prosjekter ikke kan gjennomføres som planlagt. Eller at UiT løper en høy risiko for lovbrudd ved at aktiviteter gjennomføres selv om kravene ikke overholdes. Eksempelvis grunnet manglende kunnskap om, eller forståelse for, kravene. Et slikt forhold er «Schrems II», en avgjørelse fra EU-domstolen som har fått store konsekvenser for overføring av personopplysninger ut av EU/EØS, se kap. 3.3.

Årlig utgis det nasjonalt flere ulike trussel- og risikovurderinger, og blant disse kan særlig Politiets sikkerhetstjenestes (PST) trusselvurdering og Nasjonal sikkerhetsmyndighets (NSM) risikovurdering trekkes frem. Disse omtaler trusler og risikoer som er svært relevante for UiT, og sikkerhetshendelsen høsten 2020 aktualiserte noen av de risikoene PST og NSM har pekt på. Kunnskapsdepartementet understreker i tildelingsbrevet for UiT at de forutsetter at *«institusjonene holder seg oppdatert om risiko- og trusselvurderinger fra de nasjonale etterretnings- og sikkerhetstjenestene»*<sup>1</sup> grunnet det skjerpede digitale risikobildet.

Da denne årsrapporten er et offentlig dokument presenteres risikobildet for UiT på et noe overordnet nivå hvor enkelte, sentrale risikoer og trusler trekkes frem.

Også fysiske trusler er relevante, slik som informasjonstap grunnet brann, oversvømmelser, tyveri eller eksplosjoner. UiT gjennomfører en overordnet risikovurdering på krisehendelser som kan ramme verdiområdene og utløse konsekvenser for UiTs kjernevirksomhet, og denne revideres årlig eller ved hendelser og følges opp med tiltak i beredskapsplanverket etter ansvarsområde. Grunnet dette samt bakteppet med sikkerhetshendelsen høsten 2020 er den digitale sikkerheten hovedfokus for årsrapporten for 2021.

---

<sup>1</sup> Tildelingsbrev for 2022 – UiT, pkt. 4.2.2.



### 3.1 Informasjonsinnhenting og påvirkning

PST har trukket frem at mål «*relatert til Nord-Norge, Svalbard og forsvars- og nordområdepolitikken vil være særlig utsatt*» for påvirkningsoperasjoner, både av geografiske og tematiske årsaker.

UiT har både en geografisk plassering og en forskningsprofil som gjør PSTs vurdering høyst relevant. Også utdanninger, både med tanke på samarbeidspartnere og fagprofil, kan av samme grunn være utsatt. Gjennom sikkerhetshendelsen i 2020 ble dette aktualisert da målet etter alt å dømme var informasjonsinnhenting, hvor det særlig var vist interesse for informasjon relatert til nordområdene og forskning, herunder forskningsadministrasjon. Videre var det vist interesse for studieadministrasjonen, og da særlig knyttet til internasjonalisering.

Både i 2020 og 2021 pekte NSM på et økt fokus mot forsknings- og utdanningssektoren.

I rapporten «Nasjonalt digital risikobilde 2021» trekker NSM frem nettopp angrepet mot UiT høsten 2020.

*«Som i fjorårets rapport peker NSM også i 2021 på et økt fokus mot forsknings- og utdanningssektoren. NCSC har i 2020-2021 håndtert flere hendelser tilknyttet denne sektoren i Norge.*

*Operasjonen omfatter en rekke virksomheter tilhørende forsknings- og utdanningssektoren, blant annet Norges arktiske universitet UiT (UiT) som i desember 2020 informerte om at de var rammet av et datainnbrudd. NCSC og Uninett CERT har siden desember bistått UiT med hendelseshåndtering.*

*Analyse har avdekket både kompromitterte servere og brukerkontoer, hvor veien inn har vært sårbare systemer og manglende multifaktorautentisering. UiT har fortløpende iverksatt en rekke risikoreduserende og skadebegrensende tiltak.*

*Det har vært observert kartleggingsaktivitet mot en rekke virksomheter i saken, samt enkelte påloggingsforsøk hvor formålet ser ut til å være knyttet til informasjonsinnhenting. NCSC og de sektorvise responsmiljøene i andre sektorer har fortløpende varslet og vært i dialog med berørte virksomheter.»*

Videre kan UiT bli utsatt for angrep fordi fremmede stater søker informasjon om konkrete personer blant våre ansatte eller studenter. PST trekker frem at «*Kina, Iran og andre autoritære stater bruker sine etterretningstjenester til å kartlegge og overvåke flyktninger og dissidenter som oppholder seg i Norge. Denne aktiviteten vil de videreføre i 2021. Formålet vil være å undergrave, nøytralisere eller eliminere politisk opposisjon.*». UiT må ta høyde for at vi kan ha ansatte og studenter som er i en utsatt situasjon i denne sammenheng, og det er essensielt at både disse og andre tilknyttet UiT kan føle seg trygge på at deres informasjon forvaltes på en forsvarlig måte.

Målrattede angrep fra fremmede stater er særs vanskelig og komplisert å håndtere, da de er tålmodige, ressurssterke og svært kompetente. Metoder for å gjennomføre digitale operasjoner er mangefasettert, og kan eksempelvis omfatte angrep hvor de forsøker bryte seg inn i UiTs

systemer «hjemmefra». Dette er en tilnærmet risikofri og forholdsvis rimelig fremgangsmåte, spesielt sammenlignet med mer tradisjonelle etterretningsoperasjoner. En annen fremgangsmåte er at de søker å kompromittere datautstyr tilhørende ansatte og studenter som er på reise<sup>2</sup> i et utsatt land. Enten fordi personen og informasjon denne har tilgang til er interessant i seg selv, eller for å bruke tilgangen som et springbrett videre. Det vil også være en gråsoner mellom statlige aktører og aktører som bedriver økonomisk kriminalitet. Fremfor å angripe direkte selv kan statlige aktører ta i bruk andre som gjør jobben for dem. Disse kan i tillegg ha egne motiver som eksempelvis kan medføre at de i etterkant av operasjonen selger kompromittert informasjon videre på det mørke nettet.

Det er videre viktig å være oppmerksom på at det ikke utelukkende er risiko for rene digitale etterretningsoperasjoner, men også mer «tradisjonelle» metoder. Eksempelvis ved å rekruttere eller sende en forsker eller student til UiT, herunder på gjestepopphold, og deretter benytte den tilgangen og tilliten de får til å f.eks. innhente informasjon, bedrive påvirkning eller benytte teknologi og utstyr staten ellers ikke ville hatt tilgang til. Dette peker også PST på, og nevner at *«noen stater [vil] utnytte norske utdannings- og forskningsinstitusjoner gjennom ulovlig kunnskapsoverføring. Russland, Kina, Iran og Pakistan vil utgjøre den største trusselen»*.

UiT må ha en helhetlig og planmessig tilnærming til disse problemstillingene, for å kunne håndtere dem på en god og forsvarlig måte. Utenriksdepartementet (UD) har foreslått endringer i eksportkontrollregelverket<sup>3</sup>, og dette vil også inkludere kontroll av teknologi- og kunnskapsoverføring. Det legges blant annet opp til en lisensieringspraksis, men UD vil gjennomføre en prosess hvor bl.a. berørte utdannings- og forskningsinstitusjoner høres<sup>4</sup>. Dette vil etter alt å dømme bli en sentral problemstilling å håndtere gjennom 2022 og videre.

Gjennom den årlige statusrapporten<sup>5</sup> fra enhetene meldes det at UiT har utstrakt samarbeid med land der Norge ikke har fullverdig sikkerhetssamarbeid rapporteres som en utfordring for informasjonssikkerheten. Dette er en problemstilling som gjenspeiles både gjennom at UiT har ansatte og studenter fra såkalte høyrisikoland<sup>6</sup>, samt reisevirksomhet til ovennevnte land. De som har samarbeid om fellesgrader rapporterer om et økt behov for innsyn fra samarbeidsinstitusjonene i eksempelvis Russland, og det oppleves utfordrende å ivareta informasjonssikkerheten i denne sammenheng. UiT har ansvaret for informasjonssikkerheten rundt forskningsprosesser, forskningsdata og ivaretagelsen av samarbeidspartnere – som gjennom sitt samarbeid med UiT kan bli mål for ulike trusselaktører.

---

<sup>2</sup> UiT har en retningslinje for utlån av PC mv ved reise til høyrisikoland, slik at den ansattes ordinære utstyr ikke medbringes.

<sup>3</sup> Gjennom Meld. St. 35 (2020-2021), se også fotnote 4.

<sup>4</sup> Stortingets utenriks- og forsvarskomite avgir sin innstilling til Stortinget den 21.12.2021, se Innst. 93 S (2021-2022), hvor flertallet ga sin tilslutning til Meld. St. 35 (2020-2021). Stortinget voterte over dette den 6.1.22 hvor vedtaket ble i samsvar med innstillingen.

<sup>5</sup> Se kap. 6.3 for nærmere informasjon som den årlige statusrapporten fra enhetene ved UiT.

<sup>6</sup> Russland, Kina, Iran m.fl.

Andre nasjoners fokus og intensjoner i nordområdene må være på agendaen når UiT vurderer samarbeid og håndterer informasjonssikkerheten for prosjekter og arbeid med strategisk betydning.

Dette var også fremhevet i årsrapport for informasjonssikkerhet og personvern 2020, og styret vedtok at det skulle igangsettes et arbeid med å kartlegge og håndtere de sikkerhetsrisikoene som knytter seg til internasjonalt arbeid, se kap. 4 for redegjørelse for oppfølgingen av dette.

## 3.2 Digital utpressing

Forsøk på digitale angrep er konstant og det er utallige måter å angripe på, med ulike metoder og målsetting. Den typen angrepsforsøk det er klart mest sannsynlig at UiT kan bli utsatt for i forholdsvis stor skala i fremtiden er knyttet til digital utpressing<sup>7</sup>. Uavhengig av sektor peker NSM særlig på denne trusselen. Det er også denne typen angrep som potensielt vil kunne føre til størst skade for UiT.

Blant disse aktørene er det særlig utbredt å benytte «løsepengevirus» («ransomware») som metode. Europol rapporterer at løsepengevirus er en konstant trussel, og aktiviteten har økt det siste året. I Norge er det 23 virksomheter og kommuner som ble utsatt for løsepengevirus-angrep i 2021, og det er kun de angrepene som er offentlig kjent<sup>8</sup>.

Etter Europols syn<sup>9</sup> virker det som at trusselaktørene beveger seg vekk fra den mer tradisjonelle angrepsmetoder med massedistribuerte automatiserte «breddeangrep» med løsepengevirus, og heller fokuserer på angrepsmål av høy verdi, blant annet i utdanningssektoren. Disse utsettes også for mer sofistikerte angrep.

Dersom UiT treffes av et vellykket løsepengevirus-angrep kan konsekvensene bli alvorlige og omfattende for hele virksomheten, eksempelvis grunnet omfattende stopp i aktivitet, langvarig eller permanent datatap samt lekkasje av fortrolige data.

I forsvaret mot slike angripere må UiT ivareta to aspekter:

- Klare å motstå slike angrep så godt som mulig, og
- Kunne gjenopprette normaltilstand så raskt som mulig dersom et vellykket angrep finner sted

Dette er særs kompliserte og ressurskrevende øvelser.

---

<sup>7</sup> <https://nsm.no/fagomrader/digital-sikkerhet/rad-og-anbefalinger-innenfor-digital-sikkerhet/skadevare/digital-utpressing-for-ledere>

<sup>8</sup> Ifølge oversikt utarbeidet av NRK i artikkel publisert 11.1.2022, <https://nrkbeta.no/2022/01/11/losepengevirus-koster-norske-virksomheter-dyrt/>. Blant disse er Østre Toten kommune, Nortura, Amedia, Nordic Choice og Akva Group. Nærmere detaljer om flere av angrepene i 2021 kan leses her:

<sup>9</sup> *Internet organised crime threat assessment 2021* fra Europol, pkt 2.1. [internet\\_organised\\_crime\\_threat\\_assessment\\_iocta\\_2021.pdf \(europa.eu\)](https://www.europol.europa.eu/publications-and-communications/internet-organised-crime-threat-assessment-iocta-2021)

Det er et enormt antall potensielle angripere og svært mange er så profesjonaliserte og ressurssterke at UiT må påregne at vellykkede angrep av denne art *vil* finne sted. Videre er aktiviteten «kommersialisert» slik at det er mulig å kjøpe denne typen angrep som en tjeneste, og dermed utføre mot en gitt virksomhet uten at de som står bak behøver å inneha mye ressurser eller kompetanse selv.

Det er heller ikke nødvendigvis slik at selv om man klarer å gjenopprette normaltilstand så er angrepet håndtert uten konsekvenser. Ved større angrep, slik som f.eks mot Hydro i 2019 eller Østre Toten kommune<sup>10</sup> i 2021, tok det månedsvis før alle systemene var oppe igjen og ikke all data lot seg gjenskape. For UiTs vedkommende kan det innebære at forsknings- og/eller undervisningsaktivitet må pauses eller avbrytes, samt at sentrale administrative- og ledelsesfunksjoner ikke kan ivaretas. Dette kan vedvare over tid hvis angrepet er stort nok. I noen tilfeller må man også kassere større mengder IT-utstyr og infrastruktur da man ikke lenger kan stole på disse, dvs vite med sikkerhet at de er helt frie for skadevare og angriperen ikke lenger har tilgang.

Det er også svært dyrt å håndtere slike angrep. Eksempelvis anslår Østre Toten at angrepet hittil har kostet kommunen ca 33 millioner kroner i direkte utgifter<sup>11</sup>. Det varslede overtredelsesgebyret fra Datatilsynet, som ser ut til å bli 4 millioner kroner, kommer i tillegg.

Videre har det blitt vanligere for angripere å hente ut data før de krypterer denne, og de benytter dette som ekstra pressmiddel for å få den berørte virksomheten til å betale løsepengene, f.eks ved å true med å selge informasjonen på det mørke nettet, slippe den offentlig, bedrive utpressing av enkeltpersoner mv. Europol ser<sup>12</sup> at nye utpressingsmetoder

---

<sup>10</sup> NSM trakk Østre Toten kommune frem i sin rapport «nasjonalt digitalt risikobilde 2021» (s. 21) som et eksempel på skadeomfanget ved et større løsepengevirusangrep:

*«Kommune-CSIRT rapporterer om at de lørdag 9. januar ble kontaktet av Østre Toten kommune som var rammet av et løsepengevirus med skadevaren PYSA. Hele den virtuelle serverparken til kommunen ble kryptert og låst ned. Også de internetbaserte sikkerhetskopiene ble kryptert og utilgjengeliggjort. Aktøren hadde også stjålet betydelige mengder data, og dobbel utpressing fremstod som et mulig scenario. Kommunens operative evne ble sterkt redusert da de aller fleste av kommunens digitale tjenester var nede. Situasjonen ble ytterligere forverret den 29. mars, da PYSA publiserte deler av dataene som var stjålet fra kommunen på det mørke nettet. Kommunen måtte håndtere sensitive personopplysninger på avveie, og informere og støtte personer som ble rammet.*

*På NSMs sikkerhetskonsferanse 11. mars fortalte Østre Totens ordfører Bror Helgestad at hendelsen i praksis medførte at de eldres alarm-system på sykehjem ble erstattet med bjeller, låse-systemet på kommunens bygninger ikke fungerte, og at helsestasjonen for barn og unges journaler var utilgjengelige. Kommunen måtte operere manuelt i flere måneder uten fungerende IT-systemer.»*

<sup>11</sup> <https://nrkbeta.no/2022/01/11/losepengevirus-koster-norske-virksomheter-dyrt/>. Blant norske virksomheter er det hittil dataangrepet mot Hydro som har medført de største kostnadene, de anslår at angrepet har kostet dem ca 800 millioner kroner. Som oftest vil kostnadene være en del lavere enn for Hydros tilfelle, men likevel betydelige. F.eks Akva Group som ble utsatt for løsepengevirus 10.1.2021 rapporterer at angrepet kostet dem nesten 50 millioner kroner, se <https://www.tu.no/artikler/cyberangrep-kostet-akva-group-naer-50-millioner-kroner/509982?key=7Tbq0VY8>.

<sup>12</sup> *Internet organised crime threat assessment 2021* fra Europol, pkt 2.1, avsnitt “extra layers of extortion added”.

også inkluderer å ringe journalister, klienter og samarbeidspartnere for å øke presset på den angrepne virksomheten.

I rapporten «nasjonalt digitalt risikobilde 2021» (s. 20) påpeker NSM at «*Det er en svært høy risiko for at flere norske virksomheter vil utsettes for løsepengevirus i løpet av 2022. Det er også mulig at norske virksomheter vil utsettes for løsepengevirus med omfattende konsekvenser.*».

Internasjonalt ser man tendensen til at aktører i større grad benytter merkedager til å gjennomføre angrep, og årsaken kan ifølge NSM være at de håper å forbli uoppdaget så lenge om mulig, eller ramme på verst tenkelig tidspunkt<sup>13</sup>.

Denne trusselen må UiT ha tilstrekkelig med fokus og ressurser til å håndtere. Dette vil bli nærmere berørt i kap. 6.2 og 7.1.

### 3.3 Schrems II

Den 16. juli 2020 avsa EU-domstolen dom i den såkalte «Schrems II»-saken, som omhandlet overføring av personopplysninger til USA. All overføring av personopplysninger til land utenfor EU/EØS (såkalte «tredjeland») krever et gyldig overføringsgrunnlag etter personvernforordningen (GDPR) kap. 5.

I Schrems II underkjente domstolen ett av de mest brukte grunnlagene for overføring av personopplysninger mellom EU og USA; «Privacy Shield»<sup>14</sup>. Og det andre<sup>15</sup> av de to mest anvendte grunnlagene ble i praksis svært vanskelig å benytte. Årsaken er at deler av amerikansk etterretningslovgivning er såpass problematisk at EUs pakt om grunnleggende rettigheter<sup>16</sup> ikke kan ivaretas godt nok når man overfører personopplysninger dit, og Privacy Shield var utilstrekkelig med hensyn til å motvirke dette. Dermed risikerer man at enkeltpersoners rettigheter og friheter blir forringet ved overføring av deres personopplysninger til USA, med mindre man identifiserer og iverksetter tilstrekkelige tiltak<sup>17</sup> som kan sikre et tilsvarende beskyttelsesnivå som innad i EU/EØS.

---

<sup>13</sup> Nasjonalt digitalt risikobilde 2021, s. 26. Av nyere eksempler på dette kan det her nevnes at i perioden 21.12.21 – 28.12.21 ble blant annet Nortura, Nordland fylkeskommune og Amedia rammet av alvorlige dataangrep.

<sup>14</sup> Privacy Shield var et rammeverk mellom EU og USA for å sikre beskyttelsesnivået av personopplysninger overført fra EU/EØS til USA. Dersom den mottagende virksomhet i USA var sertifisert under Privacy Shield kunne man overføre personopplysninger dit.

<sup>15</sup> EU Standard Contractual Clauses; «SCC». En standardkontrakt som kan benyttes som lovlig grunnlag ved overføring av personopplysninger til tredjeland, men etter Schrems II kreves det ofte tiltak i tillegg til de som følger av kontrakten. Det er krevende å identifisere og gjennomføre aktuelle tiltak, og ikke alltid mulig.

<sup>16</sup> Nærmere bestemt artikkel 7 (respekt for privatliv og familieliv), artikkel 8 (vern av personopplysninger) og artikkel 47 (adgang til effektiv klageadgang og rettfærdig rettergang).

<sup>17</sup> Disse kan være juridiske, organisatoriske og/eller tekniske.

En «overføring» er ikke definert i GDPR, men uttalelser fra tilsynsmyndighetene legger terskelen lavt. Også fjerntilgang fra et tredjeland regnes som en overføring, så det er ikke begrenset til de tilfeller hvor dataene faktisk hentes og lagres i det aktuelle landet. Det er heller ikke begrenset til fortrolige personopplysninger eller store mengder, all overføring av alle typer personopplysning omfattes, inkludert tilsynelatende trivielle opplysninger.

Dette får stor betydning for virksomheter i hele EU/EØS, og UiT er intet unntak. Alle deler av UiTs virksomhet kan være berørt av dette, men den mest omfattende og direkte påvirkningen er bruken av IT-tjenester og systemer som involverer leverandører utenfor EU/EØS. Det er også den problemstillingen som er vanskeligst å løse. UiT har en strategi om «sky først», og amerikanske leverandører har en svært sterk posisjon i IT-markedet. Om ikke som direkte leverandør, så i en eller annen kapasitet som underleverandør, f.eks ved å drifte datasentre. Det er ikke nødvendigvis problematisk at leverandøren i seg selv er fra et tredjeland, men svært ofte involverer slike tjenester tredjeland aktivt, og da især USA. Eksempelvis for utvidet brukerstøtte, at enkelte deler av tjenesten kjøres derfra mv.

Videre vil påvirkningen på internasjonal forskningsaktivitet potensielt kunne være betraktelig, ved at samarbeid i prosjekter som involverer personopplysninger kan bli problematiske å få til.

Oppfølging og håndteringen av utfallet av Schrems II har blitt ytterligere komplisert ved at det i lengre tid hersket en betydelig usikkerhet om rekkevidden av dommen, primært hva som er tilstrekkelige tiltak for å sikre et tilsvarende beskyttelsesnivå som i EU/EØS. Det europeiske personvernrådet (EDPB) kom med endelig utgave av sine anbefalinger og tolkninger i juni 2021, og Datatilsynet lagde sin veileder sommeren/høsten 2021. Det har dermed kommet noen avklaringer som gjør premissene noe klarere. Imidlertid er håndteringen fremdeles særs kompleks, og det er i dag ingen gode og effektive løsninger på problematikken. For enkelte typer IT-tjenester finnes det i praksis ikke fullgode alternativer, og det kan være vanskelig for berørte forskningsprosjekt å foreta nødvendige endringer uten at det får betydning for forskningen.

Datatilsynet har signalisert at de ser betraktelig strengere på avtaler som ikke er i henhold til kravene om overføringsgrunnlag dersom de er inngått *etter* dommen enn hva tilfellet er for eksisterende avtaler og samarbeid. Dette fordi avtaler inngått i etterkant anses å være inngått mot bedre vitende, mens de som ble inngått tidligere tross alt var i henhold til de daværende krav. Etter hvert som tiden går vil imidlertid gjenværende avtaler av slik art bli sett strengere på, og det forventes at dette ryddes opp i. Dette er en krevende øvelse.

Resultatet er at videreutvikling og anskaffelser av nye IT-tjenester og systemer ved UiT i stor grad har stoppet opp det siste året. Det er noe bevegelse nå, men i meget begrenset omfang. For enkelte av eksisterende IT-tjenestene som antagelig ikke er i henhold til kravene finnes det foreløpig ingen gode alternativer. For flere av disse tjenestene vil en avvikling uten noen erstatning i praksis lamme deler av UiTs virksomhet. Her er vi i samme situasjon som store

delar av det offentlige Norge, samt øvrige sektorer innenlands og utenlands, uten at det reduserer det ansvaret universitetet sitter med. Det bidrar imidlertid til at det settes press på leverandører og relevante myndigheter fra mange hold for å få løst problemstillingene slik at tjenestene opererer innenfor de aktuelle lovkravene. Det vil imidlertid ikke lykkes i alle situasjoner, og omstillinger må derfor påregnes. Hvor omfattende disse blir beror mest på om EU og USA klarer enes om et nytt rammeverk som løser de problemstillingene som felte Privacy Shield. Det er ikke gitt at så vil skje.

For forskningsprosjekter er en mulig løsning å lene seg på bruk av pseudonymisering av personopplysningene før de overføres. Det er nokså vanlig å benytte pseudonymisering, men i denne sammenheng er det satt opp strenge krav for at slik pseudonymisering skal anses som «sterk nok» til at det aksepteres som et tilleggstiltak som sikrer at forskningsdeltakernes rettigheter og friheter ivaretas når opplysningene overføres til tredjeland. Her må det bygges kompetanse på fakultetene slik at de kan identifisere hvilke prosjekter dette gjelder, og om disse håndteres i henhold til kravene.

Videre er det viktig å understreke at kravet om «tilsvarende beskyttelsesnivå» gjelder alle tredjeland og ikke kun USA selv om fokus ofte trekkes dit da de er en stor aktør, spesielt på IT-siden. For USA foretok EU-domstolen en vurdering av landets etterretnings- og sikkerhetslovgivning, som virksomhetene i stor grad kan bygge på når man vurderer om en overføring omfattes av den aktuelle lovgivningen. Tilsvarende vurdering<sup>18</sup> må tas for alle tredjeland man skal overføre personopplysninger til, og det er lagt til hver enkelt virksomhet å foreta denne vurderingen. Dette er en ekstremt krevende oppgave. Ikke minst for en virksomhet som UiT som har aktivitet, forskningsprosjekter og studentutveksling over hele verden.

I dialog med HK-dir<sup>19</sup> og Sikt<sup>20</sup> har UiT gitt tilbakemelding om at det må iverksettes et sterkere sektorsamarbeid om disse problemstillingene, fremfor at hver enkelt institusjon skal foreta de samme omfattende og kompliserte vurderingene hver for seg.

Dette er en problemstilling som vil prege virksomheten ved UiT over lang tid, og som ikke har en klar løsning. I sum medfører det både en risiko for at UiT bryter GDPR, med de følger det kan ha for både institusjonen og enkeltpersoner hvis opplysninger behandles, og at ønsket aktivitet ved UiT blir forsinket eller ikke lar seg gjennomføre. Det kan være fordi man ikke finner de nødvendige tiltak for å gjøre overføringen lovlig, enten grunnet manglende kompetanse, tid, ressurser eller at det rett og slett ikke finnes tiltak som er gode nok.

---

<sup>18</sup> Vurderingene vil gå på om landets lovgivning og inngrep er proporsjonal og om enkeltpersoners rettigheter og friheter ivaretas godt nok. Her kan det være forskjeller på lovgivning som gjelder personer som er i det aktuelle landet, og personer som befinner seg utenlands og/eller utenlandske borgere.

<sup>19</sup> Direktoratet for høyere utdanning og kompetanse.

<sup>20</sup> Kunnskapssektorens tjenesteleverandør. Opprettet 1.1.22 gjennom sammenslåing av NSD, Uninett og Unit.

## 4 Oppfølging av årsrapport 2020

Årsrapport for informasjonssikkerhet og personvern 2020 ble behandlet av Universitetsstyret i møte 4. mars 2021 (sak S 11/21), og styret fattet følgende vedtak:

1. *Universitetsstyret tar årsrapporten for informasjonssikkerhet og personvern 2020 til etterretning, og ber om at arbeidet med informasjonssikkerhet og personvern ved UiT styrkes ytterligere.*
2. *Styret ber om at årsrapporten tas opp i styret for alle fakulteter, UB og UMAK med særlig henblikk på forbedringsområder for egen enhet.*
3. *UiT skal opprettholde deltakelsen i Varslingssystem for digital infrastruktur («VDI»).*
4. *Universitetsdirektøren igangsetter arbeidet med å kartlegge og håndtere de sikkerhetsrisikoene som knytter seg til internasjonalt samarbeid.*
5. *Universitetsdirektøren iverksetter prosess for å anskaffe eksterne tjenester for kontinuerlig overvåkning av UiTs systemer og tjenester.*
6. *Universitetsdirektøren (v/Avdeling for IT) skal kartlegge og foreslå nødvendige endringer i UiTs IKT-infrastruktur slik at universitetet er bedre rustet til å motstå, oppdage og håndtere dataangrep.*

Vedtaket er fulgt opp gjennom 2021 og nedenfor gis en kort redegjørelse for denne oppfølgingen. Enkelte av oppfølgingstiltakene svarer ut flere deler av vedtaket.

1. ***Universitetsstyret tar årsrapporten for informasjonssikkerhet og personvern 2020 til etterretning, og ber om at arbeidet med informasjonssikkerhet og personvern ved UiT styrkes ytterligere.***

Det har vært en rekke tiltak for å styrke arbeidet med informasjonssikkerhet og personvern gjennom 2021, og de mest sentrale gjennomgås nedenfor.

### *- Utvidet bruk av multifaktor*

Multifaktor, ofte omtalt som «tofaktor», er et svært effektivt tiltak for å bedre informasjonssikkerheten. Det innebærer at i tillegg til å kjenne passordet til en brukerkonto så må man også ha tilgang til en ekstra faktor, eksempelvis en engangskode som genereres via en mobilapp, sendes vis sms e.l. Bruk av BankID er praktisk eksempel på multifaktor, hvor man både må skrive inn passordet til nettbanken samt engangskoden BankID-brikken genererer. Det er en kjensgjerning av enkeltbrukeres passord ofte er på avveie, og det kan være flere grunner til dette. UiT må ta høyde for at det til enhver tid vil være brukere hvis passord er kjent for uvedkommende som ønsker utnytte det. Bruken av multifaktor er et svært effektivt tiltak for å redusere konsekvensene av dette siden det ikke vil være nok for en angriper å kun vite passordet, de må også ha tilgang til denne ekstra faktoren.

Over flere år har multifaktor vært i bruk for ansatte for enkelte av UiTs tjenester. I 2021 ble imidlertid bruken betydelig utvidet, både ved at multifaktor ble påslått for en rekke nye tjenester samt for studentenes brukerkontoer.



For Office 365 har UiT hatt multifaktorpålogging for ansatte siden juni 2018. I desember 2020 ble dette også innført for ansattes bruk av UiTs VPN-tjeneste, som et akuttiltak under sikkerhetshendelsen.

For studenter ble multifaktorpålogging innført høsten 2021. Siden dette medførte en stor endring i studentenes brukeropplevelse måtte det gjøres en grundig teknisk analyse for å sikre at UiT ikke påførte sine studenter ekstra kostnader ved denne endringen.

Svært mange av UiTs tjenester bruker Feide<sup>21</sup> til innlogging, og det har lenge vært et ønske om å aktivisere multifaktor også for disse. Her måtte vi avvente til Feide var klargjort for å kunne benytte UiTs løsning for multifaktor, men da det var avklart og iverksatt høsten 2021 innebar det at alle tjenestene UiT hvor benytter Feide for innlogging nå hadde dette sikkerhetstiltaket. De mest sentrale er Canvas (UiTs digitale læringsplattform), WiseFlow (eksamenssystem) og PAGA (personal og økonomi). Den 1.1.22 innførte UiT nytt økonomi- og lønssystem levert av DFØ, men i og med at Feide benyttes for pålogging er også tilgang til disse tjenestene lagt bak multifaktorpålogging.

Denne omfattende utvidelsen av bruk av multifaktor er den viktigste sikkerhetsforbedringen som er gjennomført på brukersiden i 2021, og har gjort det betydelig vanskeligere å kompromittere og utnytte brukerkontoer hos UiT.

Ansatte og studenter har blitt anbefalt å benytte mobilapp for multifaktorpålogging, men Avdeling for IT (ITA) har tilbudt ansatte å hente en fysisk «nøkkel» (et såkalt «hardwaretoken», av typen YubiKey) hos brukerstøtteskrankene. De aller fleste foretrekker å bruke mobilapp så i praksis har dette vist seg å være en meget begrenset kostnad for UiT<sup>22</sup>. ITA vurderer om samme tilbud skal gis til studenter.

- *Styrking av budsjettrammer for informasjonssikkerhet for 2022 flg.*

Den 14.6.21 behandlet Universitetsstyret sak S 26/21 om «intern hovedfordeling av budsjett 2022». Fordelingen av budsjettrammene for 2022 inkluderte finansering av tiltak for å følge opp styrets tidligere vedtak om å styrke arbeidet med informasjonssikkerhet og personvern.

Nærmere bestemt gjaldt det følgende tiltak:

- *«Det inngås avtale med ekstern leverandør for SoC (24/7 sikkerhetsovervåkning) i 2021 og dette må inn som en fast post i budsjettet*
- *Nye tjenester for mottak av logger og overvåkning, MS Defender Azure Sentinel er etablert. Nye systemer for nettverksovervåkning er under vurdering.*
- *Stillingsbehov for å kunne drifte proaktivt sikkerhetsarbeid estimeres til 1 stilling til hver av områdene nettverk, sentral infrastruktur og klientsystemer»*

---

<sup>21</sup> Feide er en nasjonal løsning for sikker innlogging og datadeling i utdanning og forskning, se <https://www.feide.no/om-feide>.

<sup>22</sup> Mindre enn 50 enheter har blitt utlevert. Skulle et større antall ønske seg en slik vil det imidlertid kunne bli en betydelig kostnad da hver slik «nøkkel» koster flere hundre kroner.

I styresaken var årlig kostnad for disse tiltakene vurdert til 7,5 millioner kroner, fordelt på driftskostnader samt lønns- og personalkostnader.

Midlene gjelder fra og med 2022, men i og med at ansettelsesprosesser tar tid og det er et sterkt behov for å få styrket det proaktive sikkerhetsarbeidet ble prosessen for ansettelse av personer i disse tre stillingene igangsatt høsten 2021. De vil tiltre i løpet av våren 2022.

- *Utvidelse av årlig statusrapport for informasjonssikkerhet*

Videre har den årlige statusrapporten blitt utvidet til at også avdelingene i fellesadministrasjonen leverte. Dette var egentlig planlagt til 2020, men ble utsatt grunnet koronapandemien. Gjennom denne rapporteringen kartlegger og vurderer enhetene sine informasjonsverdier samt foretar en egenvurdering av sårbarheter og organisering av arbeidet med informasjonssikkerhet og personvern. Utvidelsen innebærer at fra og med 2021 skal samtlige enheter ved UiT foreta denne strukturerte vurderingen og rapporteringen, og dette vil gi både enhetene separat og UiT samlet en helt annen oversikt og forståelse for hvilken informasjon som forvaltes, og hvordan dette arbeidet må og kan foregå. Se nærmere redegjørelse i kap. 6.3.

- *Datamigreringsprosjekt*

I 2021 ble det påstartet et prosjekt for å få flyttet data ut fra gamle lagringsløsninger som hjemme- og fellesområdene til Office 365. Dette med mål om å avslutte disse løsningene, da Office 365 gir både mer funksjonalitet og bedre sikkerhet. I statusrapporteringen fra enhetene har flere rapportert om at økt informasjonssikkerhet etter datamigreringsprosjekt, da dette har medført at ansatte har gjort en digital opprydding og kunne ta i bruk arkivtjenester og skytjenester med tilhørende klassifisering.

For øvrig vil oppfølgingen av vedtakets pkt. 2 – 5 alle innebære en generell styrking av arbeidet med informasjonssikkerhet og personvern, i tillegg til den pågående økningen i bevissthet rundt disse problemstillingene – en forbedring som har pågått over flere år.

**2. *Styret ber om at årsrapporten tas opp i styret for alle fakulteter, UB og UMAK med særlig henblikk på forbedringsområder for egen enhet.***

Dette ble gjennomført som planlagt, og i forkant av styremøtene har *faggruppe for informasjonssikkerhet og personvern* hatt møte med ledelsen på de ulike enhetene for gjennomgang av årsrapport og forberedelse til styremøtet. Selve saken for styrene er det imidlertid enhetene selv som utarbeidet. Faggruppen har deltatt i styremøtene når saken ble behandlet, og ga samtlige styrer en nærmere orientering om sikkerhetshendelsen UiT hadde høsten 2020. Dette fordi det gir styrene en nærmere forståelse av det aktuelle trussel- og risikobildet som finnes, og ga mulighet for direkte dialog om hvordan enhetene burde handle for å bidra til å forhindre tilsvarende hendelser.

I etterkant av internrevisjonen utført av PwC<sup>23</sup> ble kontrollerende del (kap. 7-9) av *ledelsessystemet for informasjonssikkerhet og personvern* ved UiT revidert, både for å følge opp anbefalingene fra PwC samt foreta øvrige endringer UiT har sett behov for. Den etterfølgende behandlingen av årsrapportene i styret for alle fakulteter, UB og UMAK er nå regulert direkte i kapittel 9 («ledelsens gjennomgang») som en fast ordning. I enhetenes sak for eget styre skal både årsrapporten samt særskilte problemstillinger og forbedringsområder for egen enhet tas opp. Videre innføres det fra 2022 at også avdelingene i fellesadministrasjonen under universitetsledelsen skal behandle årsrapporten i sine ledermøter, på tilsvarende måte som enhetene med eget styre.

Det er derfor ikke lenger behov for at Universitetsstyret årlig vedtar at enhetsstyrene skal gjennomføre en slik oppfølging av årsrapporten m.m.

### ***3. UiT skal opprettholde deltakelsen i Varslingssystem for digital infrastruktur («VDI»)***

I forbindelse med håndteringen av sikkerhetshendelsen høsten 2020 ble UiT medlem av *Varslingssystem for digital infrastruktur («VDI»)*<sup>24</sup> som er et sensornettverk driftet av Nasjonalt cybersikkerhetssenter (NCSC) hos Nasjonal sikkerhetsmyndighet (NSM). Målsetningen med VDI er å detektere og varsle om cyberoperasjoner som treffer kritisk infrastruktur eller kritiske funksjoner i Norge. Annet enn en engangskostnad knyttet til anskaffelse av VDI-boksen som er utplassert i UiTs nettinfrastruktur medfører ikke dette økonomiske kostnader for UiT, da deltakelse for offentlige virksomheter dekkes over statsbudsjettet.

UiT utsettes for kontinuerlige angrepsforsøk. Dette er den nye normalen og universitetet må agere deretter. Gjennom 2021 har UiT blitt varslet av NCSC om flere angrepsforsøk, som universitetet dermed har kunnet raskt håndtere eller avverge før skade oppsto.

Flere av disse forsøkene ble kun oppdaget og varslet gjennom VDI-samarbeidet, og ikke via øvrige samarbeidspartnere og tjenester innenfor sikkerhet, herunder UH-sektorens sikkerhetsovervåkning. VDI har derfor hatt klar nytteverdi for UiT, og det er ønskelig at deltakelsen opprettholdes.

Det må imidlertid presiseres at det også er tilfeller hvor vi ble varslet av de øvrige sikkerhetstjenestene vi har anskaffet, og hvor vi ikke fikk varsel via VDI. Det understreker behovet for et bredt sammensatt spekter av tjenester innenfor sikkerhetsovervåkning og -analyser, da vi ikke kan støtte oss på kun én type tjeneste eller leverandør. Til det er risikobildet for komplekst og skiftende, og tjenestene til en viss grad for spesialiserte.

---

<sup>23</sup> Se kap. 6.4.

<sup>24</sup> <https://nsm.no/tjenester/varslingssystem-vdi/>

#### ***4. Universitetsdirektøren igangsetter arbeidet med å kartlegge og håndtere de sikkerhetsrisikoene som knytter seg til internasjonalt samarbeid.***

I møte i universitetsledelsen den 8.3.21 ble oppfølging av dette vedtaket behandlet, og følgende tiltak fastsatt:

*«Det foreslås å opprette et team med gitte roller og funksjoner for å koble og følge opp det helhetlige trusselbilde, koordinering og integrering internt, samarbeid med eksterne aktører, være et kontaktpunkt for interne og eksterne i virksomheten.*

*UiT skal sikre et varig systematisk samfunnssikkerhetsarbeid med kontinuerlig oppfølging av risikoer på ulike nivå i virksomheten.*

*Det settes ned en gruppe som arbeider videre med mandat for en slik gruppe.*

*Tilbakemelding fra ledermøtet at det må stå mer om arbeid ut mot enhetene under tiltak, som å dele informasjon, gi opplæring, rådgivning.*

*Aktuelt:*

- *Sjekkliste/tiltakort til bruk ved prosjektplanlegging og ansettelser (som punkter NSM)*
- *Instruks: Vurdering av engasjement av eksterne gjesteforskere, doktorgradsstipendiater og andre (eksempel fra andre i UH sektoren)*
- *Håndtering av objektive holdepunkter (som treffpunkter radikaliserings)*
- *Informasjon, opplæring og rådgivning»*

Denne arbeidsgruppen ble ledet av Avdeling for økonomi og organisasjon, og hadde medlemmer fra Avdeling for IT, Avdeling for bygg- og eiendom, Avdeling for forskning, utdanning og formidling samt stab for rektor og direktør.

Arbeidsgruppen leverte sitt notat i juni 2021 med forslag om at det gjøres endringer i ledelsessystem for informasjonssikkerhet og personvern slik at det også inkluderer et tilstrekkelig styringssystem for samfunnssikkerhet og sikkerhetsloven. Videre at det etableres et tverrfaglig team som arbeider bredt med sikkerhet innenfor samfunnssikkerhet og beredskap, og består av få personer med kompetanse innen samfunnssikkerhet, informasjonssikkerhet, internasjonalt arbeid, utdanning og forskning. Det vil være ønskelig og nødvendig også med deltakelse fra fakultetsnivå. Teamet skal være strategisk og operativt, og arbeide systematisk med samfunnssikkerhet og beredskap på området. Deltakelse i teamet vil kunne bidra til at de eksisterende miljøene som arbeider med informasjons- og samfunnssikkerhet på UiT i større grad får et samhandlingspunkt, og sikre en mer enhetlig tilnærming til tematikken på tvers av enhetene.

**5. *Universitetsdirektøren iverksetter prosess for å anskaffe eksterne tjenester for kontinuerlig overvåkning av UiTs systemer og tjenester.***

Dette er ikke en engangsprosess, og behovet må kontinuerlig vurderes da endringer i risikobildet også kan medføre endringer i hvilken overvåkning som er påkrevd. Dette punktet ble blant annet fulgt opp gjennom budsjettinnspill til Universitetsstyrets sak S 26/21 som ble behandlet i møte 14.6.21. Især budsjettinnspillene knyttet til SoC (døgnkontinuerlig sikkerhetsovervåkning) og nye tjenester for mottak av logger og overvåkning m.m. var en oppfølging av dette vedtakspunktet, se nærmere redegjørelse under vedtakspunkt 1 ovenfor.

Arbeidet med å styrke disse tjenestene pågikk gjennom hele 2021, og vil fremdeles pågå i 2022. En viss forsinkelse har det blitt grunnet markant usikkerhet rundt UH-sektorens nye cybersikkerhetssenter (EduCSC), da det fremdeles er uklart akkurat hva EduCSC vil kunne levere og til hvilken kostnad. Det vil imidlertid uansett ikke være tilstrekkelig for UiT å kunne lene oss på EduCSC som ekstern partner, av samme grunn som at det ikke er tilstrekkelig med f.eks kun VDI som sikkerhetsovervåkingstjeneste, se ovenfor under redegjørelse for oppfølging av vedtakspunkt 3.

**6. *Universitetsdirektøren (v/Avdeling for IT) skal kartlegge og foreslå nødvendige endringer i UiTs IKT-infrastruktur slik at universitetet er bedre rustet til å motstå, oppdage og håndtere dataangrep.***

Dette er i stor grad endringer som går på den tekniske infrastrukturen og hvordan denne skal håndteres, og det vil være et kontinuerlig arbeid uten sluttdato. En rekke tiltak er foreslått og implementert, og høsten 2021 ble ytterligere tiltak identifisert gjennom risikovurderinger, se kap. 6.2 *IKT-sikkerhet* for nærmere redegjørelse.

Noen endringer var besluttet i forkant av styrets vedtak, men er av såpass markant betydning at de tas med. Dette for å gi et innblikk i helheten av styrkingen av sikkerheten i UiTs IKT-infrastruktur gjennom 2021.

**- *Omlegging av UiTs nettverk fra standard «åpen» til standard «lukket»***

UiT og andre akademiske institusjoner har siden «internetts barndom» ansett åpne nettverk som en god standard for å oppfordre til utstrakt bruk av nettet, bl.a. for å stimulere til videreutvikling, og det har dermed i stor grad vært mulig for ansatte og studenter å sette opp tjenester på nettet uten sentral godkjenning og kontroll.

De siste års utvikling av risiko- og trusselbildet har vist at dette prinsippet ikke lenger kunne opprettholdes, og tilnærmingen måtte dermed endres. Tidlig i 2021 ble det derfor besluttet at UiTs nettverkregler skulle endres slik at alle tjenester som skal være tilgjengelig fra internett må kontrolleres og godkjennes av Avdeling for IT. Dette er den største nettverksendringen som er gjennomført i UiTs 30 år på internett, og ble iverksatt den 30. januar 2021.

- *Ny infrastruktur for brannmur*

Den eksisterende brannmurinfrastrukturen var planlagt byttet i 2021 som en del av normal utskifting. Ny løsning forventes å være operativ januar 2022 og vil gi langt bedre mulighet for kontroll og deteksjon av uønsket aktivitet i UiTs nettverk.

## 5 Hendelser og avvik

### 5.1 Oppsummering

I tidligere årsrapporter har det være pekt på en mistanke om til dels betydelig underrapportering av avvik innenfor informasjonssikkerhet og personvern. Dette grunnet det forholdsvis lave antallet avvik som meldes. *Faggruppe for informasjonssikkerhet og personvern* («faggruppa») og forløperen til faggruppa har årlig fått melding om ca 15-25 hendelser og avvik. For 2021 ligger nivået rimelig likt som tidligere. Selv om man tar høyde for at avvik også håndteres via andre kanaler, slik som f.eks brukerstøtte, IT-tekniske fora mv., er det fremdeles god grunn til å tro at ikke alle avvik meldes. At avvik håndteres via ulike kanaler er en utfordring i seg selv, da det gjør det vanskelig å se helheten, sikre at alt faktisk håndteres samt å avdekke de tilfeller hvor årsaken til avvik skyldes systemsvikt og det ikke er tilstrekkelig å håndtere det enkelte tilfellet isolert.

Dette berøres også av enhetene i deres årlige statusrapport<sup>25</sup> om informasjonssikkerhet. Her er det flere som trekker frem større utfordringer knyttet til avvikssystemet. Det pekes på manglende oversikt over egne avvik, samt manglende kunnskap om hva som skal meldes og hvordan avvik håndteres. Mistanken om underrapportering av avvik bygger på usikkerhet blant ansatte, samt deres bevissthet rundt informasjonssikkerhet. Dette er sammenfallende med funn i internrevisjonsrapporten fra PwC<sup>26</sup> som anbefaler retningslinjer og kulturendring knyttet til avvikshåndtering.

Av statusrapporteringen fremkommer det også dokumentasjon tilhørende informasjonssikkerhet og avvik oppleves som vanskelig eller ukjent. Arbeidet med å gjøre ressursiden [uit.no/sikkerhet](https://uit.no/sikkerhet) bredt kjent må derfor fortsette. Årsaken til avvikene er ofte menneskelig feil eller brudd på rutiner, og det er sentralt å vurdere om UiT har enkelte systemer og prosesser hvor det er for lett å gjøre feil.

Videre er det slik at de avvikene som meldes primært er innenfor informasjonssikkerhet, og i liten grad knyttet til personvern utover sikkerhetsaspektet<sup>27</sup>. Det må derfor fokuseres på kompetanseheving og kulturbygging slik at også slike meldes fra om.

Etter hva faggruppa forstår er det også tilsvarende utfordringer ved avvikshåndtering på andre felt enn informasjonssikkerhet og personvern. En tilbakemelding som er gitt i møter med flere enheter er at det er vanskelig for ansatte og studenter å vite hvordan ulike avvik skal kategoriseres, samt hvor og hvordan de skal meldes. UiT har mange forskjellige måter å melde avvik på, avhengig av tematikk (HMS, informasjonssikkerhet, varsling mv.). Det fremstår derfor som et sterkt behov for en harmonisering slik at ansatte og studenter har kun et fåtall

---

<sup>25</sup> Se kap. 6.3.

<sup>26</sup> Se kap. 6.4.

<sup>27</sup> Eksempler på slike avvik kan være behandling av personopplysninger uten lovlig grunnlag, innsamling av for mange personopplysninger, bruk av databehandler uten tilstrekkelig avtale mv.

steder å forholde seg til med tanke på selve innmeldingen av avvik, og aller helst kun et samlet sted. Dette kan være komplekst å få til, da det er ulike tekniske systemer, enheter og fagfelt involvert i avvikshåndteringen.

Et nærliggende tiltak er at UiT kjører en forbedringsprosess på universitetets avvikssystem, slik at det gis mulighet for å se de ulike områdene i sammenheng på en strukturert måte og komme frem til løsninger på kort og lang sikt.

### ***Datatilsynet***

I 2021 hadde UiT to avvik som måtte meldes til Datatilsynet. Det ene omhandlet en situasjon hvor en underviser glemte å skru av mikrofonen i en pause, og studentene kunne overheøre samtalen vedkommende hadde med en annen underviser.

Det andre avviket oppsto i forbindelse med sensurering hvor vurderingsresultat og tilhørende begrunnelse ble synlig for feil kandidat. Dette gjaldt noen få studenter.

Datatilsynet har avsluttet saksbehandlingen av begge disse avvikene, og UiT er ikke ilagt noen formell reaksjon på disse.

I 2021 ble det videre levert sluttrapport til Datatilsynet knyttet til sikkerhetshendelsen høsten 2020. På tidspunktet denne årsrapporten ble skrevet hadde ikke UiT mottatt endelig vedtak fra Datatilsynet.

### **5.1.1 Sikkerhetshendelsen høsten 2020**

Som kjent ble UiT utsatt for et omfattende og alvorlig datainnbrudd («sikkerhetshendelsen») høsten 2020. Hendelseshåndteringen fortsatte utover 2021, og oppfølging har pågått hele 2021. En redegjørelse for denne hendelsen tas derfor med i årsrapporten.

Hendelsen var særs alvorlig, og del av et større angrep som også omfattet andre virksomheter enn UiT.

Dette er den mest alvorlige sikkerhetshendelsen UiT har vært utsatt for, og konsekvensene kunne blitt betraktelig verre enn hva de ble. Det er essensielt å forhindre at en trusselaktør klarer å oppnå samme fotfeste og posisjon i fremtiden. Det vil være ressurskrevende å oppnå, både med tanke på personellressurser og investeringer, men kostnadene ved opprydning etter en trusselaktør som i større grad utnytter en tilsvarende posisjon vil være betraktelig større.

I tillegg løper UiT en betraktelig risiko for omdømmetap hvis en tilsvarende sak skulle oppstå igjen, samt at skadepotensialet for enkeltpersoner<sup>28</sup> kan være betydelig, avhengig av hvilken informasjon som kompromitteres.

---

<sup>28</sup> Eksempelvis studenter, ansatte eller forskningsdeltakere.



Det ble gitt orientering til Universitetsstyre i egen orienteringssak i januar 2021, og denne orienteringen ble også inntatt som vedlegg til årsrapport for informasjonssikkerhet og personvern 2020 (sak S 11/21, behandlet i styremøte 4. mars 2020). Saken ble også meldt til Datatilsynet.

Arbeid med håndtering og oppfølging av sikkerhetshendelsen har pågått gjennom hele 2021, og gjennom våren 2021 har det også blitt gjennomført nærmere vurderinger og analyser av skadeomfang og -potensiale. Det ble utarbeidet en evalueringsrapport om sikkerhetshendelsen, som var ferdigstilt tidlig høst 2021. Denne omhandler hendelsesforløpet, årsaker, skadeomfang og UiTs håndtering, og er inntatt som vedlegg tre til årsrapporten.

I selve årsrapporten inntas en oppsummering av hendelsesforløpet samt informasjon om skadeomfanget og -potensialet.

#### **5.1.1.1 Hendelsesforløpet oppsummert**

Fredag 4. desember 2020 ble UiT v/assisterende IT-direktør oppsøkt av PST, da de hadde informasjon om at en maskin<sup>29</sup> kunne være kompromittert. Dato for kompromittering var antatt å være 11. november 2020.

Samme dag ble det etablert kontakt mellom UiT<sup>30</sup>, NSM og Uninett CERT<sup>31</sup>. På dette tidspunktet fremsto sikkerhetshendelsen som forholdsvis begrenset, men det var mye usikkerhet knyttet til situasjonen med tanke på omfang og alvorlighetsgrad. Sentral beredskap ble derfor satt tidlig påfølgende uke.

NSM og Uninett CERT ga en klar og sterk oppfordring om at UiT skulle forholde seg i ro; i den forstand at vi ikke skulle foreta noen aktive oppslag eller tiltak mot den kompromitterte maskinen, ei heller opptrå «unormalt»<sup>32</sup> i andre systemer da dette kunne gjøre trusselaktøren<sup>33</sup> klar over at denne var oppdaget. NSM understreket at det kunne innebære en til dels betydelig risiko dersom aktøren skjønte at den var oppdaget før vi hadde tilegnet oss nok informasjon gjennom kartlegging og analyser, og var klare til å iverksette tilstrekkelige, samtidige tiltak.

Det ble foretatt forberedelser for å kunne gjennomføre undersøkelser uten å alarmere trusselaktøren, og gjennom disse undersøkelsene ble det klart at det var et forholdsvis stort

---

<sup>29</sup> Dette er en maskin som ble brukt til utvikling og håndtering av kildekode, og var åpen også for brukere utenfor UiT.

<sup>30</sup> Ved leder for UiTs Computer Security Incident Response Team (CSIRT), som også er tilknyttet Faggruppe for informasjonssikkerhet og personvern ved UiT.

<sup>31</sup> Uninett CERT er universitets- og høyskolesektorens responsmiljø («SRM») ved digitale sikkerhetshendelser, se <https://www.uninett.no/en/node/743>.

<sup>32</sup> I denne sammenheng menes å ikke foreta pålogginger, søk, oppslag eller handlinger som ikke ville blitt foretatt som del av normal drift, dvs. enhver handling som skilte seg ut fra «hverdagsarbeid».

<sup>33</sup> Dvs. angriperen, som omtales som «trusselaktøren», «TA» eller «aktøren».

antall lokale brukerkontoer på maskinen. Selv om passordene var hashet<sup>34</sup> så var dette etter såpass gammel standard at det ville ikke medføre særlig vanskeligheter å knekke passordene. Siden gjenbruk av passord dessverre er utbredt anså vi det som en potensiell risiko at trusselaktøren kunne forsøke å kompromittere enkeltbrukers kontoer i andre tjenester (utenfor UiT), ved hjelp av «credential stuffing»<sup>35</sup>. Ut fra dette vurderte UiT at sikkerhetshendelsen hadde fått en slik karakter at meldeplikten til Datatilsynet inntrådte, jf. personvernforordningen (GDPR)<sup>36</sup> art 33 nr. 1. Melding ble oversendt 12.12.2020, og fulgt opp med ny melding den 21.12.2020 om videre utvikling i saken. Personvernombudet ved UiT<sup>37</sup> ble orientert om hendelsen i forbindelse med utarbeidelse av den første avviksmeldingen til Datatilsynet.

Gjennom videre analyser ble det klart at ytterligere maskiner var kompromittert, og sikkerhetshendelsen endret karakter og alvorlighetsgrad.

Den 15.12.2020 ble de første skadebegrensende tiltakene iverksatt. På formiddagen den 16.12.2020 ble alle ansatte ved UiT informert og bedt om å endre sitt passord. Videre var saken av en slik art at pressemelding ble sendt ut samtidig, slik at det ble orientert bredt om at det var en pågående sikkerhetshendelse ved UiT. Den 18.12.2020 fikk alle øvrige brukere<sup>38</sup> beskjed om å endre sitt passord. Frist for passordbyte for samtlige brukere på UiT ble da satt til 23.12.2020 kl. 08:00.

Frem til 23.12.2020 pågikk det intenst arbeid med tiltak og analyser, inkludert rigging av økt monitorering av sentrale systemer og infrastruktur. I denne perioden ble det klart at sikkerhetshendelsen innebar en omfattende kompromittering, og en rekke maskiner, tjenester og kontoer var kompromittert. Angrepet var svært alvorlig, og en målrettet, ressurssterk og profesjonell aktør sto bak.

---

<sup>34</sup> «Hashing» av passord er et sikkerhetstiltak for å gjøre det vanskeligere for en angriper å bli kjent med hva passordet faktisk er (i «klartekst»), og er en prosedyre/teknikk for å beskytte passord når de lagres. Dvs at passordene lagres ikke i klartekst (f.eks «detteermittdarligepassord»), men «omsettes» via en enveis algoritme til en tekststreng (f.eks «64acf9a61e4be21e6aa642abf01462c8») som ikke har noen tilsynelatende sammenheng med det faktiske passordet, og det er ingen algoritme som kan brukes til å reversere fra et hash til et passord. Når man logger på en brukerkonto omsetter algoritmen passordet til en slik tekststreng, og sammenlignes med det som er laget i databasen. Stemmer disse overens vet systemet at det er rett passord som er skrevet inn og man får logget på. For en forenklet forklaring av dette, se artikkel i [tek.no](https://tek.no) (fra 2015, men konseptet er fremdeles nokså likt).

<sup>35</sup> Dette er en fremgangsmåte angripere benytter for å forsøke å bryte seg inn i kontoer (f.eks epostkontoer, Facebook-kontoer osv). Dersom de blir kjent med hvilket brukernavn (ofte en epostadresse) og passord en person har brukt for en tjeneste (f.eks etter en datalekkasje, et angrep e.l.) så forsøker de denne kombinasjonen av brukernavn/passord i alle tenkelige andre tjenester. De utnytter altså at personer ofte gjenbraker passord på tvers av tjenestene.

<sup>36</sup> EU 2016/679 av 27. april 2016.

<sup>37</sup> [Personvernombud ved UiT Norges arktiske universitet | UiT](https://www.personvernombudet.no/)

<sup>38</sup> Studenter og andre med UiT-brukerkonto, eksempelvis eksterne sensorer.

Blant det mest alvorlige var at trusselaktøren hadde klart å kompromittere UiTs eposttjeneste (Exchange Online i Office 365), og hadde tilegnet seg tilgang til 16 postbokser. Videre hadde trusselaktøren opparbeidet seg full kontroll over UiTs Active Directory («AD»), noe som utgjorde en særs alvorlig kompromittering som var kompleks å håndtere.

Den 17.12.2020 anså vi at trusselaktøren var stengt ute fra UiTs sentrale driftsmiljø, herunder Office 365 og Azure-infrastrukturen, og analyser viste ingen aktivitet fra trusselaktøren etter denne datoen bortsett fra noen enkelttilfeller med nye angrepsforsøk i januar og videre utover våren. Disse var riktignok del av samme sakskompleks, men svært begrenset i omfang<sup>39</sup>. Imidlertid forelå det fremdeles en risiko for at aktøren hadde klart å etablere hittil ukjente bakdører, spesielt på klientsiden<sup>40</sup>. I så fall ville de kunne klare å komme seg på innsiden igjen, og dette var bakgrunnen for mye av det påfølgende arbeidet utover januar.

Monitoreringen som ble satt opp i denne perioden besto primært av installasjon av Varslingstjeneste for digital infrastruktur (VDI)<sup>41</sup> fra NSM (v/NCSC) og en separat overvåkningstjeneste fra mnemonic<sup>42</sup> som alarmerte ved ukjente eller mistenkelige pålogginger og aktivitet i UiTs Office 365. Dette var nødvendig både for å oppnå kontroll samt sørge for at ansatte på IT-avdelingen kunne ta fri i julen etter en periode med særs høyt arbeidspress og -omfang, uten at det innebar økt risiko for fornyet eller ytterligere kompromittering fra trusselaktørens side.

Trusselaktøren forholdt seg rolig i juleperioden, og foruten enkelte automatiske/maskinelle skanninger av nettverket vårt så vi ingen ny aktivitet fra aktøren før tidlig januar 2021.

Analysene og arbeidet som pågikk i håndteringen av hendelsen resulterte også i at tidspunkt for første kompromittering måtte oppdateres. Først ble datoen flyttet tilbake til 1.11.2020, deretter til 1.9.2020 og i januar 2021 ble det klart at dato for første kompromittering var 31.8.2020. Analyser viste også at trusselaktøren hadde rekognosert UiTs infrastruktur siden juli 2020, dog ikke kompromittert den. Fra 2. september, gjennom oktober og deler av november ser vi ingen spor av aktivitet fra trusselaktøren, så det var en lengre periode hvor aktøren ikke hadde noen aktive utfall mot UiT.

---

<sup>39</sup> Det gjaldt kompromitteringen av en maskin tilhørende Universitetsbiblioteket og utnyttelsen av en kompromittert brukerkonto hvor aktøren hadde klart å fange opp det nye passordet.

<sup>40</sup> Alle kompromitteringer til da hadde vært på servere og ikke via klienter, så bakdører på klientsiden ville representert et markant skifte av fremgangsmåte. Det fremsto som mindre sannsynlig at klientene var akutt utsatt, og de ble derfor ikke prioritert for tiltak i desember.

<sup>41</sup> Se <https://nsm.no/tjenester/varslingssystem-vdi/>

<sup>42</sup> mnemonic er en leverandør av IT-sikkerhetstjenester, og blant de største i Europa innenfor dette feltet. Se <https://www.mnemonic.no>. De ble også hyret inn for rådgivning for håndtering av sikkerhetshendelsen. De er blant de selskap som tilfredsstiller NSMs krav i deres godkjenningsordning for leverandører som tilbyr tjenester for håndtering av dataangrep. For nærmere informasjon, se [Kvalitetsordning for leverandører som håndterer IKT-hendelser - Nasjonal sikkerhetsmyndighet \(nsm.no\)](#).

Vi antar at i hvert fall deler av forklaringen er at de bearbeidet data de hadde hentet ut fra AD, for å kunne klare å sikre seg kontrollen over denne da de startet hovedangrepet i november/desember. Dette kan endre seg dersom f.eks NSM skulle komme frem til nye vurderinger.

Arbeidet med gjennomføringen av ytterligere skadebegrensende tiltak, og forberedelse til en større omlegging av UiTs infrastruktur, pågikk gjennom hele januar. Denne omleggingen ble gjennomført helgen 30. – 31.1.2021, og var nødvendig for å berede grunnen for tiltakene som var påkrevd for å gjenvinne full kontroll over Active Directory (AD), og sikre at trusselaktøren ikke hadde noe gjenstående fotfeste i AD. Dette arbeidet var vellykket, og etter begynnelsen av februar var ikke UiT lenger i en aktiv beredskapssituasjon.

Gjennomføring av ytterligere tiltak og oppfølging av sikkerhetshendelsen pågikk gjennom hele 2021.

Ut fra hva vi kan se er det primært i postkassene til enkeltansatte at trusselaktøren har vært interessert i *innholdet*<sup>43</sup>. Øvrige kompromitteringer bærer preg av å enten være som et direkte steg videre inn eller rundt i UiTs driftsmiljø, eller grep for få tak i brukerkontoer, påloggingsinformasjon o.l. for å kunne tilegne seg tilgang til ytterligere maskiner, tjenester mv. Øvrig innhold (dokumenter etc.) på disse maskinene/tjenestene virker ikke å ha vært i fokus, dog kan ikke dette fullstendig utelukkes grunnet manglende loggnivå samt tidsperspektivet.

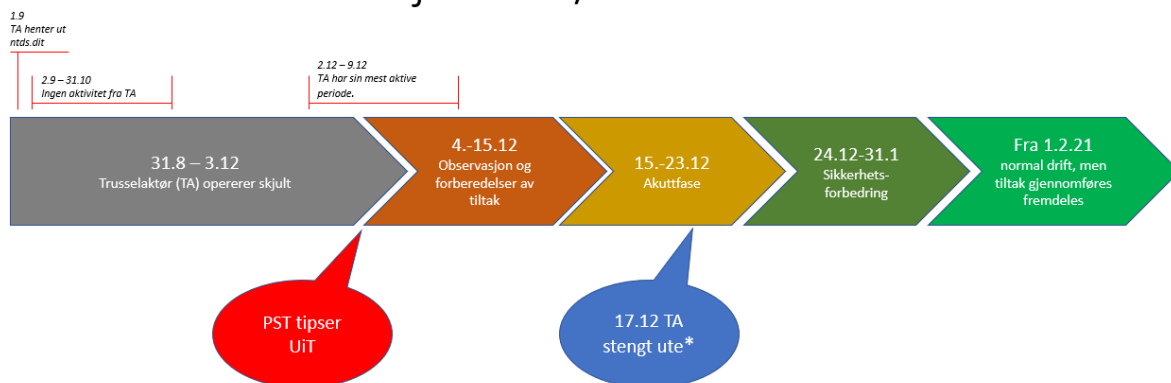
For postkassene kan vi si noe om hvilke personer trusselaktøren har valgt ut, og dette er primært administrativ ansatte, men også fra toppledelse samt flere vitenskapelig ansatte. Gjengangeren i tematikk for arbeids-/ansvarsområdene til de ansatte er internasjonalt samarbeid, forsknings- og studieadministrasjon, øverste ledelse samt forskning innenfor nordområdene, politikk og samfunn.

Aktøren fremstår profesjonell, målrettet, ressurssterk og politisk motivert.

---

<sup>43</sup> I denne sammenheng menes «innholdet» dokumenter, eposter, personlige filer, bilder, video etc.

# Overordnet tidslinje 2020/2021



\*) to vellykkede enkeltinnbrudd siste uke januar

Figur 1 – Overordnet tidslinje for sikkerhetshendelsen

## 5.1.1.2 Skadeomfang

### - Postbokser

En rekke tjenester og kontoer ble kompromittert. Etter UiTs vurdering er det de kompromitterte postboksene som innebærer det største og mest alvorlige bruddet på personopplysningssikkerheten.

I postboksene befant det seg er en omfattende informasjonsmengde som berører tema relatert til UiTs ledelse, forskning innenfor politikk, nordområdene mv., samt administrasjon innenfor primært forskning og internasjonalisering.

Totalt sett er det derfor vanskelig å vurdere skadepotensialet. Både for de 16 som postboksene tilhører, samt alle som enten har kommunisert med dem via e-post eller er omtalt i e-poster som befinner seg i postboksene.

Imidlertid kunne trusselaktøren gitt seg selv rettigheter til postboksene til samtlige av UiTs brukere, og dermed gått inn på langt flere enn de 16 postboksene som ble kompromittert. Det er derfor interessant og relevant å si noe om deres stilling/arbeidsfelt, i vurderingen av både motivasjon og skadeomfang/-potensiale.

Det var fire vitenskapelig ansatte, to fra universitetets toppledelse og 10 fra sentraladministrasjonen som alle arbeider innenfor forskningsadministrasjon og/eller internasjonalt samarbeid.

### - Brukerkontoer

Trusselaktøren tilegnet seg flere brukerkontoer tilhørende ansatte og studenter. Aktørens handlinger samt den informasjon vi kan se ut fra aktivitetslogger tyder på at disse brukerkontoene var interessante for å tilegne seg videre adgang til UiTs driftsmiljø.

De var altså ikke interessante grunnet *innholdet* som befant seg tilknyttet kontoene (filer, eposter mv), men ble brukt som verktøy av aktøren for å bevege seg rundt internt i UiTs driftsmiljø. Det fremstår derfor som forholdsvis lite sannsynlig at det er hentet ut informasjon som kan benyttes for å skade personene disse kontoene tilhører, eller tredjepersoner som måtte vært omtalt i dokumenter, korrespondanse m.v. som var lagret i tilknytning til disse kontoene.

De eleverte kontoene (administratorkontoer o.l.) trusselaktøren tilegnet seg er separat fra de IT-ansattes ordinære kontoer. Også her ligger skadepotensialet i at disse ble benyttet til å komme seg videre inn i driftsmiljøet og dermed tilegne seg tilgang til *andre* kontoer, systemer mv, fremfor personlig informasjon som eventuelt er tilknyttet selve kontoen.

### **5.1.1.3 Påvirkning på aktivitet ved UiT**

De aller fleste ved UiT ble ikke direkte påvirket av sikkerhetshendelsen, annet enn passordbyttet, og forsknings- og utdanningsaktivitetene forløp som planlagt. Men noe påvirkning vil det være i en slik omfattende situasjon og enkelte miljø ble rammet hardere enn andre. Blant annet var det en samarbeidspartner som for å være på den sikre siden så seg nødt til å blokkere all kommunikasjon med UiT (innkommende eposter samt tilgang til deres nettverk), og dette påvirket det aktuelle forskningsprosjektet negativt bl.a. ved at de ikke fikk tilgang til sensorene de benyttet til måling.

Nedenfor vil vi trekke frem noen miljøer og prosesser som ble negativt påvirket. Dette er imidlertid ikke en uttømmende liste.

#### **- *Site.uit.no***

Site.uit.no var blant de tjenestene som ble tatt ned og her lå blant annet tjenesten for digital mappe (pedagogisk mappe). Søknadsfristen for professoropptrykk var 31.12.2020, og tilbakemeldingene fra fagmiljøene var at mange hadde satt av juleperioden for å arbeide med sin pedagogiske mappe og dette utgjorde et stort problem. Det var heller ikke gitt god informasjon utad om dette så de vitenskapelige ansatte visste ikke om dette var en forbigående situasjon eller om tjenesten ville forbli nede over lengre tid. Teknikere på Avdeling for IT ble aktivisert i jula, og tjenesten ble åpnet igjen den 26.12.2020.

Videre lå også romværsidene fra *Fakultet for naturvitenskap og teknologi* her og dette er en tjeneste som benyttes av mange offentlige etater.

- **Det helsevitenskapelige fakultet**

Som et «føre-var»-tiltak frem til situasjonen var under kontroll tok UiT ned Eutro<sup>44</sup>, og denne tjenesten ble holdt avslått i perioden 22.12.2020 – 16.2.2021. I denne perioden ble det riktignok gjennomført en rekke forbedringer av Eutro, også av sikkerhetsmessig art, som ellers ville måtte blitt tatt over lengre tid, så det var ikke utelukkende negativt.

Imidlertid er det klart at manglende tilgang til Eutro, både prosjektadministrasjonsdelen og forskningsdataene, hadde en negativ påvirkning på forskningsaktiviteten på det Helsevitenskapelige fakultet.

*Konsekvenser for administrasjonen ved Helsefak og SSHF/SAMINOR*

Seksjon for forskning, utdanning og formidling på Det helsevitenskapelige fakultet ble bedt om å gi tilbakemelding på de konsekvensene nedstengningen av Eutro fikk for administrasjonen og SSHF<sup>45</sup>/SAMINOR<sup>46</sup>:

*«Helsefaks administrasjon fikk beskjed om at EUTRO ble stengt ned som følge av datainnbrudd før jul 2020. For fakultetets del fungerer EUTRO først og fremst som 1) en oversikt hvilke prosjekter som ikke har datasett fra våre registre, og 2) som et varsel for forskerne om å forlenge eller jobbe med å avslutte et prosjekt der REK-godkjenninga løper ut. Superbruker hadde i tida med nedstenging fokus på å avslutte prosjekter, og forhøre seg om prosjekter eventuelt hadde blitt forlenget av REK. En del av svarene fra forskerne ble derfor liggende uten å loggføres. I tillegg ble ikke prosjektlederne varslet i tida fram til at EUTRO kunne brukes igjen. Det ble også et etterslep på innføring av nye prosjekter med REK-godkjenning.*

*Senter for samisk helseforskning og SAMINOR hadde forholdsvis lite endringer i prosjektporteføljen sin eller behov for uttak av data i perioden. Forlengelse og avslutning av en håndfull prosjekter ble berørt, men det var overkommelig å håndtere, men SSH/SAMINOR fikk erfart viktigheten av å ha dokumenter relatert til søknader og datautlevering lagret andre steder i tillegg til i EUTRO.»*

---

<sup>44</sup> «Eutro» er en IT-løsning som gir en komplett oversikt over en rekke studiers samlede forskningsmateriale, både biologisk materiale, helsedata og prosjektadministrasjon. Eutro benyttes i store regionale, nasjonale og internasjonale studier, herunder til håndtering og arkivering av all forskningsdata innsamlet gjennom Tromsundersøkelsen (består av totalt syv befolkningsundersøkelser og utgjør alene over 40 år med forskningsdata). Eutro driftes og utvikles av UiT gjennom et eget miljø tilknyttet Institutt for samfunnsmedisin ved Det helsevitenskapelige fakultet

<sup>45</sup> SSHF er Senter for samisk helseforskning ved Institutt for samfunnsmedisin, UiT. Se [Senter for samisk helseforskning | UiT](#).

<sup>46</sup> SAMINOR er en stor befolkningsbasert undersøkelse og en av de viktigste kildene til kunnskap om helse og levekår i den samiske og nordnorske distriktsbefolkningen. Se [SAMINOR | UiT](#).

### *Konsekvenser for forskningsaktivitet/befolkningsundersøkelsene*

Tromsøundersøkelsen<sup>47</sup> representerer den største brukeren av Eutro, og de ble bedt om å gi tilbakemelding om konsekvensene nedstengingen fikk for deres aktivitet:

- «Etablering/utlevering av data til 24 nye prosjekter kunne ikke effektueres og vi kunne heller ikke fakturere eller lage avtaler med forskere.
  - o Flere av disse var studentprosjekter og studentene kom i tidsskvis ift mastergradsoppgaver som skulle leveres. Vi har ikke informasjon om det resulterte i forsinket innlevering/eksamen – men da hadde vi nok hørt det.
- Oppfølging/oppdatering i om lag 50 prosjekter kunne ikke iverksettes
  - o 18 av disse måtte vente på prosjektutvidelse/endring, evt utlevering av nye variabler
- Mellom 3-5 dataimporter kunne ikke effektueres
  - o Dette medførte forsinkelser og tapt arbeidstid bl a. for en postdoc som var ansatt for å gjøre analysene.

*Det er vanskelig å anslå eksakt hvor mye arbeidstid som har gått tapt, men det er nok noen mndverk.»*

#### **- Øvrige**

Det at en rekke tjenester ble tatt ned fikk nødvendigvis noe negativ påvirkning på virksomheten. For de fleste aktive tjenestene så var det imidlertid tale om kortere tidsrom, og store deler av nedstengingen skjedde over juleperioden hvor det uansett var lavdrift pga ferieavvikling. For andre var påvirkningen større, eksempelvis for Universitetsbiblioteket da en av maskinene som ble tatt ned blant annet styrte alarmportalene deres.

#### **5.1.1.4 Skadepotensiale**

UiT ble påført stor skade gjennom at en trusselaktør tilegnet seg et sterkt fotfeste dypt inne i vårt driftsmiljø, og tilegnet seg informasjon. I og med at målsetningen til trusselaktøren er ukjent er det vanskelig å vurdere det mer langsiktige skadepotensialet for UiT.

Det som imidlertid er særskilt viktig å trekke frem er at den posisjon og fotfeste trusselaktøren hadde skaffet seg i UiTs driftsmiljø kunne påført langt større skade. Hadde aktøren vært interessert i bred informasjonsuthenting kunne den klart å hente ut langt mer enn hva den har gjort, f.eks. ved å gi seg tilgang til langt flere postbokser enn de 16. Hadde aktøren gått målrettet etter systemer og tjenester med fortrolig innhold fremstår det som sannsynlig at gitt nok tid ville de klart å tilegne seg adgang til disse. Det ville imidlertid ikke vært en triviell oppgave – selv med den posisjonen de hadde opparbeidet seg i UiTs driftsmiljø.

Videre kunne trusselaktøren ha iverksatt et omfattende angrep med løsepengevirus som ville satt UiT mer eller mindre ute av spill over lengre tid. Det fremstår også som sannsynlig at de

---

<sup>47</sup> [Tromsøundersøkelsen | UiT.](#)



var i en posisjon til å kompromittere backupløsningene. Dermed var det en reell risiko for at data kunne gått permanent tapt som følge av en slik handling.

Det er umulig å gardere seg helt mot dataangrep, men UiT må gjøre det så vanskelig som mulig for en angriper å lykkes. Videre er det essensielt å ha gode nok tjenester og planer for å oppdage sikkerhetshendelser, håndtere disse og være i stand til å oppnå normaltilstand så raskt som mulig.

## 5.2 Korona

Som for 2020 var 2021 preget av koronapandemien.

Det ga mye fysisk fravær fra campus som igjen skapte utfordringer knyttet til informasjonssikkerheten. Bruken av hjemmekontor for administrativt ansatte, vitenskapelige ansatte og studenter har ulike problemstillinger, men noen fellesnevner er det. Møter og undervisning som gjennomføres digitalt ved hjelp av ulike videoverktøy har satt informasjonssikkerheten på prøve. Det ble derfor tidlig i pandemien utarbeidet informasjon og «kjøreregler» for ivaretagelse av informasjonssikkerheten og personvern på hjemmekontor; knyttet til beskyttelse av papirutskrifter, bevissthet rundt at andre i husstanden ikke skal kunne overhøre møter, bruk av VPN osv.

I denne perioden har blitt innført flere digitale verktøy, og feil bruk av disse kan medføre utfordringer for informasjonssikkerheten. Her er det en stor utfordring i å løfte kompetansen blant ansatte og studenter raskt nok, inkludert at det kun skal benyttes tjenester som UiT har avtale med. I perioder har det vært veksling mellom undervisning på campus og fulldigital undervisning, og spesielt i de tilfeller hvor omstillingen har måttet skje raskt har risikoen for informasjonssikkerhets- og personvernbrudd økt. For en del digitale tjenester må man velge «riktig» påloggingsmetode<sup>48</sup> for å benytte tjenesten innenfor de vilkår UiT har avtalt med leverandøren. Siden flere og flere tjenester også har mulighet for privat bruk øker dette muligheten for at en ansatt i praksis bruker sin private konto på den aktuelle tjenesten fremfor UiT-kontoen, og dette må det gis tilstrekkelig informasjon og bevisstgjøring rundt.

Imidlertid må det tilføyes at de endringene som har skjedd med arbeidsmetoder og den økte digitaliseringen som hurtig har tvunget seg frem de siste to årene, også har bidratt til å øke informasjonssikkerheten. Blant annet har brukerkompetansen økt, og enkelte manuelle prosesser har blitt digitalisert.

---

<sup>48</sup> Eksempelvis at man skal logge på ved hjelp av Feide.

## 6 Styling og kontroll

Det gjennomføres flere kontrollaktiviteter opp mot informasjonssikkerhet og personvern gjennom året, noen er faste og andre ved behov. Formålet med kontrollaktivitetene er å kunne vurdere i hvilken grad de etablerte tiltakene er tilstrekkelige og effektive for å sikre etterlevelse av relevant regelverk og overordnede føringer. Gjennom kontrollerende aktiviteter vil det kunne avdekkes forbedringsområder knyttet til eksisterende tiltak og identifiseres eventuelle ytterligere tiltak som bør iverksettes.

Blant de faste, årlige kontrolltiltakene er en statusrapport hver enkelt enhet skal levere med egenvurdering av tilstanden på enheten samt en oversikt og vurdering av egne informasjonsverdier, se kap. 6.3.

### 6.1 Risikostyring

UiTs nåværende informasjonssikkerhetsstrategi har i korte trekk som hovedmålsetning at UiT skal løfte seg til en mer formalisert og systematisk sikkerhetspraksis. Strategien har en risikobasert tilnærming til informasjonssikkerhet, og gjennom arbeidet med strategien ble det klart at generelt sett har UiT en relativt høy risikotoleranse.

Imidlertid betyr ikke det at hver enhet, forsker mv. står «fritt» til å akseptere den risiko man anser som hensiktsmessig. For det første finnes det lovkrav om ivaretagelse av tilstrekkelig sikkerhetsnivå, eksempelvis gjennom personvernforordningen (GDPR). Videre har Universitetsstyret vedtatt enkelte, ytre rammer for hvor høy risiko UiT kan ta («akseptabel risiko»).

Det innebærer ikke at all risiko «innenfor» disse grensene er greit, men gir uttrykk for noen klare yttergrenser som ikke skal passeres uansett hvor høy den potensielle gevinsten er.

Vi kan ikke påvirke hvilke trusselaktører som er interessert i UiTs informasjonsverdier, men gjennom tiltak kan vi redusere de sårbarhetene vi har og dermed bedre beskytte verdiene fra disse aktørene. Slike tiltak vil være nødvendige for å redusere risikoen fra et uakseptabelt nivå til et akseptabelt.

Imidlertid er iverksettelse av sikkerhetstiltak et spørsmål om ressurser og prioritering. For svake eller mangelfulle sikkerhetstiltak medfører fort sikkerhetsbrudd som kan ha alvorlige konsekvenser, men det er heller ikke ønskelig å ilegge strengere sikkerhetstiltak enn nødvendig, både ut fra et ressurs- og bruksperspektiv. For strenge sikkerhetstiltak som man ikke er i stand til å forklare eller rettferdiggjøre ut fra risikobildet oppleves ofte som begrensende og unødvendig tungvint av brukerne. Da inviterer man til en viss grad til direkte omgåelser av tiltakene, og sikkerheten kan i verste fall bli svakere enn hvis disse aldri var innført.

Til tider kan det også være slik at man ikke har, eller ønsker prioritere, ressurser til å iverksette nødvendige tiltak for å dra ned en høy risiko, og vanskelige avgjørelser må tas.

Eksempelvis at et ønsket IT-system ikke kan tas i bruk eller et forskningsprosjekt ikke kan gjennomføres som planlagt, for det er ikke mulig å ivareta et tilstrekkelig sikkerhetsnivå ved hjelp av de ressurser som UiT generelt og/eller fakultetet spesielt er villig til å avsette. Slike avgjørelser kan ha stor påvirkning for ansatte og studenter ved UiT, og må være velbegrunnet og velforankret.

Disse vurderingene og beslutningene skal derfor bygge på risikovurderinger.

Før en kan vurdere risiko må man imidlertid vite *hva* man har og hvor viktig disse informasjonsverdiene er for UiT. Først da har vi mulighet til å iverksette presise og passende tiltak, samt ha en fungerende internkontroll.

### 6.1.1 Informasjonsverdier

For at det skal være mulig å ta informerte valg om risiko må UiT som nevnt ha oversikt over hvilke informasjonsverdier universitetet har, hvor viktige og/eller kritiske disse er samt hvilke trusler disse reelt sett er utsatt for.

I 2019 iverksatte UiT tiltak for å få en etablert en strukturert tilnærming til disse spørsmålene, ved at enhetene årlig skal kartlegge og rapportere hvilke informasjonsverdier de har mv., se kap. 6.3.

Det har vært en gradvis innføring og fra og med 2021 er samtlige enheter omfattet.

Dette var et til dels nytt og omfattende arbeid i akkurat den formen, og det vil måtte gå noen runder med rapportering før man har nådd et hensiktsmessig detaljnivå. Imidlertid er det førstegangsrapporteringen som er mest krevende, og det er fortsatt slik at kartleggingen utført i 2019 utgjør hovedgrunnlaget for rapporteringen. Endringene går primært på detaljnivået i rapporteringen, hvor det nå er bedre presisjon. Etterfølgende års rapportering visere også at tilbakemeldingene fra *faggruppe for informasjonssikkerhet og personvern* i stor grad benyttes i arbeidet.

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

Enkelte fakultet var fremdeles for overordnet i sin rapportering i 2020, og detaljnivået har nå blitt bedre. Arbeidet med vurdering av trusselaktører mot enkelte informasjonsverdier er spisset og der det tidligere ofte kun var registrert én aktuell trusselaktør mot en gitt verdi klarere enhetene i større grad å se at det er omstendigheter hvor verdien kan være interessant for flere<sup>49</sup>.

---

<sup>49</sup> De bes oppgi maksimalt to trusselaktører som anses som de største truslene mot de enkelte informasjonsverdiene. UiT har utarbeidet en liste over aktuelle trusselaktører (statlig, konkurrent, utro tjener, aktivist m.fl.) som enhetene vurderer ut fra.

Det har i større grad blitt fokus på informasjonsverdier UiT erverver gjennom avtaler med eksterne partnere både nasjonalt og internasjonalt. For ivaretagelse av informasjonssikkerheten er det svært viktig med økt fokus på denne type informasjonsverdier, der UiT kan bli misbrukt som portal til informasjon som igjen kan skade samarbeidspartnere.

Enkelte informasjonsverdier kan være komplekse å håndtere da de endrer klassifisering over tid, eksempelvis eksamensoppgaver som er fortrolig/rød informasjon før eksamen er avholdt og åpen/grønn etterpå. Flere fakultet har tatt med dette aspektet for aktuelle informasjonsverdier i årets rapportering.

I og med at årets rapportering nå involverer samtlige enheter ved UiT er det mulig å se informasjonsverdiene fullt ut i sammenheng, og ett av momentene som er nytt i år er en større grad av fokus på informasjonsverdier som eies av en enhet, men forvaltes av en annen enhet. Det er viktig at UiT har avklarte skiller for eierskap og forvalteroppgaver til informasjonsverdiene.

Tilsvarende problemstilling vil også kunne eksistere mellom UiT og eksterne samarbeidspartnere, hvor UiT forvalter informasjon som eies av andre. Det vil her være viktig at krav til informasjonssikkerhet og tiltak fra UiTs side reguleres i aktuelle avtaler med samarbeidspartnerne.

Øvrige deler av UH-sektoren har vist interesse for det arbeidet UiT gjennomfører rundt kartlegging og vurdering av informasjonsverdier.

### **6.1.2 Risikovurderinger**

Det følger av *ledelsessystemet for informasjonssikkerhet og personvern* kap. 5 at risikovurderinger skal foretas

- når trusselbildet endres
- før oppstart av behandling av personopplysninger
- ved oppstart av forskningsprosjekter
- ved etablering eller endring av IKT-systemer
- ved organisatoriske endringer som kan påvirke informasjonssikkerheten

Det har vært en markant bedring de senere år i gjennomføringen av risikovurderinger ved UiT, men det er enda et stykke igjen. Det knytter seg store utfordringer til å bygge opp tilstrekkelig kompetanse ute på enhetene til at slike vurderinger kan gjennomføres. Det er også et sterkt behov for at UiT klarer å forenkle prosessen for i hvert fall risikovurderinger av lettere og mer oversiktlige prosesser og prosjekter.

Det kan her også nevnes at deler av utfordringen er å få dokumentert risikovurderingene og sikre at disse skjer på en systematisk måte som ivaretar kvaliteten og helheten, fremfor at det ikke skjer noen form for risikovurdering. De aller fleste tenker over og diskuterer «hva kan gå galt», og hvordan skal man unngå det. Imidlertid er det mangler knyttet til systematikken og

dokumentasjonen, og det kan medføre at man overser risikoer som man ellers kunne sett, ikke identifiserer de mest hensiktsmessige og/eller presserende tiltakene samt at dersom et sikkerhetsbrudd skulle finne sted er man heller ikke i stand til å påvise hvilke vurderinger som er gjort.

Videre er det et sterkt behov for bedre systemstøtte, da dagens gjennomføring av risikovurderinger skjer ved hjelp av malverk i Excel. Det oppleves som vanskelig tilgjengelig og det er en betraktelig terskel for å komme i gang. Her er det imidlertid på gang en anskaffelsesprosess i sektoren, og forhåpentligvis vil en bedre løsning være på plass i løpet av 2021.

Den største utfordringen virker imidlertid å være å klare å bygge risikovurderinger inn som en naturlig del av arbeidsprosessene på alle nivå, hvor metodikken benyttes som et effektivt verktøy for å identifisere nødvendige og hensiktsmessige tiltak. Her er det en viss bedring, og gjennom statusrapporten for 2021 melder enkelte enheter at de i økende grad baserer seg på risikovurderinger som del av beslutningsgrunnlaget når de utarbeider nye rutiner og prosesser.

### **6.1.3 Håndtering og oppfølging av risikoer**

UiT ser en klar økning i gjennomføringen av risikovurderinger, men det er fremdeles knyttet utfordringer til at alle gjennomførte risikovurderinger faktisk blir fulgt opp og tiltak gjennomført. Videre skal det skje en evaluering av gjennomførte tiltak etter en viss tid eller dersom risikobildet endrer seg, for å sikre at tiltaket fungerer etter hensikten. Dette gjennomføres fremdeles i for liten grad, i alle fall i dokumentert utgave.

## **6.2 IKT-sikkerhet**

IKT-sikkerhet<sup>50</sup> trenger et større løft slik at UiT er rigget for å møte det gjeldende risikobildet, både slik det er i dag og slik det måtte utvikle seg videre. Målsetningen for IKT-sikkerheten er i korte trekk firedelt<sup>51</sup>, og innebærer å kunne

- identifisere og kartlegge universitetets behov, strategi, ressurser, prioriteringer mv.
- beskytte og opprettholde sikker tilstand,
- oppdage og fjerne sårbarheter og trusler,
- håndtere og gjenopprette normaltilstand ved sikkerhetshendelser.

I 2021 ble det gjennomført en intern kartlegging og vurdering av hvordan UiT oppfyller NSMs grunnprinsipper for IKT-sikkerhet, som anbefales gjennom *Policy for*

---

<sup>50</sup> Ofte omtalt som «operativ sikkerhet» og omfatter primært det tekniske aspektet ved sikkerhet slik som logging/overvåkning, analyser, backup, hendelseshåndtering mv.

<sup>51</sup> <https://nsm.no/regelverk-og-hjelp/rad-og-anbefalinger/grunnprinsipper-for-ikt-sikkerhet-2-0/introduksjon-1/de-fire-kategoriene/>

*informasjonssikkerhet og personvern i høyere utdanning og forskning*<sup>52</sup> pkt. 1 e). Gjennom blant annet dette arbeidet identifiseres hva som må utvikles og styrkes videre.

Avdeling for IT (ITA) ved UiT har i 2021 gjennomført en rekke tiltak for å forbedre IKT-sikkerheten i institusjonens systemer og tjenester. Det er imidlertid tydelig at risikobildet utvikler seg så raskt at det behov for ytterligere styrking av ITAs kapasitet på IKT-sikkerhet.

*Følgende tiltak anses som de viktigste for 2022:*

- Ytterligere sikring av UiTs data og systemer mot utpressingsangrep samt katastrofegjenoppretting. Dette er tiltak som både vil kreve investering i 2022 samt medføre en fast økning i løpende kostnader for videre drift, både for vedlikehold av den tekniske infrastrukturen samt økning i personellressurser (tilsvarende én stilling).
- Tre nye stillinger for operativ sikkerhet. Universitetsstyret ga tilsagn til midler til disse stillingene i styresak S26/21 (14.6.21), og ansettelsesprosess ble iverksatt høsten 2021.
- Etablering av samarbeid med UH-sektorens cybersikkerhetssenter (EduCSC) samt kontrakt med godkjente sikkerhetsselskaper for bistand ved akutte hendelser, oppdateringer og revisjoner av UiTs sikkerhetstiltak.

De nærmere detaljer om behov for investeringer og styrking av IKT-sikkerhet er inntatt i vedlegg 2, som er unntatt offentlighet da de peker på konkrete sårbarheter ved UiTs IKT-sikkerhet som kan utnyttes av ondsinnede aktører dersom de har de nødvendige detaljene.

*Særlig om kvalitetssystemet for Avdeling for IT (ITA)*

I dag har UiT et *kvalitetssystem for Avdeling for IT*, som omfatter all drift av IT-systemer og tjenester i regi av ITA. Imidlertid er det flere systemer og tjenester som driftes av miljøer på enhetene selv. Det innebærer blant annet at prosedyrer for endringer eller oppdateringer av systemer ikke er like på tvers av UiT, selv om det kan gjelde tjenester som er bredt i bruk. Det er heller ingen automatikk i at tjenester og systemer som driftes av enhetene føres opp i UiTs systemkatalog, og det finnes dermed ingen fullstendig og oppdatert oversikt.

Det at kvalitetssystemet kun gjelder for ITA og ikke for all drift av IKT ved UiT er også en utfordring med tanke på universitetets evne til å ivareta informasjonssikkerheten og personvernet. Det fremstår derfor som naturlig at kvalitetssystemet bør utvides til å bli et *kvalitetssystem for IKT ved UiT* fremfor å gjelde kun for ITA. Dette vil være en krevende overgang for ITA som må utvide sine interne prosesser til å også omfatte øvrige enheter, men vil også kunne være krevende for miljøene på de ulike enhetene som vil oppleve det som mer detaljert styring fra ITAs side.

---

<sup>52</sup> Fastsett av Kunnskapsdepartementet i rundskriv F-04-20 den 1.10.2020.

## 6.3 Statusrapport enhetene

I 2019 ble det innført en årlig statusrapport for informasjonssikkerhet. I begynnelsen omfattet denne fakultetene, UMAK og UB. Det er ikke gjort endringer i strukturen av utsendt materiale for 2021 og gjennom statusrapporten skal informasjonsverdier identifiseres, samt trusler og tiltak vurderes.

Gjennom rapporten foretar enhetene en egenvurdering av organiseringen av informasjonssikkerhetsarbeidet og orienterer om status på risikovurderinger. Sentralt for bakgrunnen for rapporteringen er at enhetslederne har ansvaret for informasjonssikkerheten på egen enhet, og for at disse skal være i stand til å oppfylle sitt ansvar er de nødt til å ha oversikt over egne informasjonsverdier og hvilket trusselbilde disse utsettes for. Den totale oversikten som dannes gjennom rapporteringen fra enhetene gir videre UiT et helhetlig bilde av hvilke informasjonsverdier universitetet forvalter, hvilke trusler disse kan utsettes for og sårbarheter som må håndteres.

Behovet for denne typen oversikt og kontroll trekkes også frem i «*Styringsdokument for arbeidet med sikkerhet og beredskap i Kunnskapsdepartementets sektor*» (desember 2021)<sup>53</sup>.

Fra 2021 er også avdelingene i fellesadministrasjon omfattet av rapporteringen. Førstegangsrapporteringen er en omfattende prosess, men gir et grunnlag som gjør senere rapportering enklere da det i stor grad vil dreie seg om oppdateringer på hva som har endret seg siste året. For 2021 har fakultetene, UB og UMAK i all hovedsak oppdatert deres tidligere rapport, samt svart på tilbakemeldinger og tatt inn noen nye momenter som følge av pågående arbeid og utvikling i sin forståelse av informasjonssikkerhet.

Årets statusrapportering viser en modning i arbeidet med informasjonssikkerhet ved UiT. Dette gjenspeiles gjennom en økt forståelse for viktigheten for forankring av ansvaret hos enhetslederne. Det er kontinuitet i arbeidet med karlegging av informasjonsverdier, samt at flere erkjenner mangler på kompetanse og hensiktsmessig organisering. I denne sammenheng ser vi at enkelte fakultet har økt resursene som arbeider med informasjonssikkerhet og at andre har dannet arbeidsgrupper. Dette gir et fokus der informasjonssikkerhet får en større oppmerksomhet i det daglige arbeidet. Som en følge av koronapandemien gjenspeiler også årets rapportering utfordringer som oppstår når ansatte og studenter ikke kan være fysisk på campus.

Gjennom arbeidet med årlig statusrapport og tilhørende tilbakemeldinger har fakultetene fått en bedre oversikt som igjen har resultert i konkrete prioriteringer. Disse prioriteringene varierer fra målrettet kompetansesøkende tiltak i egen organisasjon til spesifikke fokusområder hvor trusselvurderingen ligger til grunn.

---

<sup>53</sup> <https://www.regjeringen.no/no/dokumenter/styringsdokument-for-arbeidet-med-samfunns-sikkerhet-og-beredskap-i-kunnskapssektoren/id2512037/>, pkt. 6.1.

For avdelingene i fellesadministrasjonen har arbeidet med førstegangsinnlevering av statusrapporten vist et bevisst forhold til arbeid med informasjonssikkerhet og personvern. Rapporteringen vitner jevnt over om god forståelse for informasjonsverdiene og trusler de utsettes for. Tiltak som er iverksatt eller under arbeid baserer seg på risikonivå der resultater fra risikovurderinger utgjør en stor del av beslutningsgrunnlaget.

Avdeling for bygg og eiendom (BEA) har ikke levert sin statusrapport for informasjonssikkerhet, uten at grunnen til dette er kjent. UiT mangler derfor innsikt i hvilke informasjonsverdier som forvaltes av BEA, og hvordan de vurderer egen tilstand herunder sårbarheter, organisering, risikohåndtering samt det relevante trusselbildet. Dette er en utfordring med tanke på UiTs mulighet til å identifisere sårbarheter, se helheten og kontrollere etterlevelsen av UiTs *ledelsessystem for informasjonssikkerhet og personvern*.

### ***Oppsummering***

For 2021 har UiT fått en mer komplett rapportering av status innen informasjonssikkerhet gjennom at avdelingene i fellesadministrasjonen også rapporterer. Oversikten vil imidlertid ikke bli komplett før samtlige enheter faktisk rapporterer.

Oversikten over informasjonsverdiene har for hver rapportering gradvis blitt justert fra overordnet til mer detaljert. Dette gir en konkret mulighet til å drive målrettet sikkerhetsstyring for å unngå avvik og uønskede hendelser, samt få en hensiktsmessig prioritering av ressursbruken.

Gjennom årets rapportering vises modning i arbeidet med informasjonssikkerhet. En økt ressursbruk og kontinuitet i prosesser har gjort kartleggingen av informasjonsverdiene mer spisset. Samtidig erkjennes mangel på kompetanse og manglende kultur for avviksrapporing. I sum gir dette en bedre mulighet for UiT til å identifisere og iverksette sikkerhetstiltak mer treffsikkert. Det vises større forståelse for styring av risiko i arbeidsoppgavene, forskingen og undervisningen, mens den daglige informasjonshåndteringen fremdeles bærer mer preg av en fragmentert tilnærming enn et kontinuerlig fokus på informasjonssikkerhet.

For rapporteringen for 2022 er det ønskelig å utvide den til å også omfatte personvern.

## **6.4 Internrevisjon**

I 2021 ble gjennomførte PwC internrevisjon av *ledelsessystemet for informasjonssikkerhet og personvern ved UiT*. Rapporten ble overlevert UiT i oktober 2021, og forelagt Universitetsstyret i møte 24. november 2021 sammen med rapportene fra de øvrige internrevisjonene som var gjennomført av PwC i samme tidsrom.



For denne årsrapporten gjengis sammendraget av internrevisjonsrapporten:

*«UiT er en kompleks organisasjon med et høyt antall ansatte og studenter, en stor faglig bredde og en rekke ulike utdanninger. Både de ytre føringene UiT er underlagt samt omfanget av oppgaver og organisasjonens størrelse og kompleksitet, tilsier at det er et stort spenn fra den overordnede styringen av universitetet til implementeringen av konkrete krav på laveste operative nivå. Dette gjør seg gjeldende både på personvern- og informasjonssikkerhetsområdet, og det er derfor nødvendig å etablere et relativt komplekst maskineri for å ivareta helhetlig etterlevelse.*

*Det er vår samlede vurdering at UiT har jobbet godt med personvern og informasjonssikkerhet over tid. Dette kommer særlig til uttrykk gjennom (i) etablering av faggruppe for informasjonssikkerhet og personvern (ii) etablert ledelsessystem for informasjonssikkerhet og personvern og (iii) etablert ledelsens årlige gjennomgang, med årlig rapportering fra fakulteter/enheter til faggruppen. Disse tiltakene underbygger vår oppfatning om at UiT både har tydelig fokus på og ønske om god styring og kontroll av områdene. Internrevisjonen ønsker i denne forbindelse også å trekke frem at det i gjennomførte intervjuer gjennomgående er blitt fremhevet en opplevelse av en positiv utvikling på informasjonssikkerhet og personvernområdet.*

*Koronapandemien har skapt utfordringer for UiT, som for de fleste øvrige virksomheter. Dette har tidvis medført nødvendig utsettelse av enkelte planlagte aktiviteter og at det har vært mindre kapasitet til å ha kontinuerlig fokus på det løpende arbeidet med informasjonssikkerhet og personvern. Ut fra dette, finner PwC det naturlig å fremheve de mer systemiske utfordringene som har fremkommet gjennom revisjonen, da den mer akutte situasjonen antas å ville normaliseres over tid.*

*UiT har vært gjennom en større omorganisering de siste årene, med en økt grad av sentral styring der administrative ressurser fra nivå 2 er samlet i større administrative enheter på nivå 1. Sentralisering av kompetanse, med en sentral faggruppe, vurderes å være et godt tiltak for å styrke arbeidet med personvern og informasjonssikkerhet. Det fremstår imidlertid å være en for stor forventning til at nivå 2 har tilstrekkelig ressurser med kapasitet og relevant kompetanse til å utføre oppgavene som er lagt til nivå 2. Gjennomgående er det uttrykt et behov for større kapasitet på nivå 2, både for å være et støtteapparat tilgjengelig på fakultetene og også som et kontaktpunkt mellom nivå 1 og nivå 2. Enkelte fakulteter er i prosess med etablere slike roller*

*Etter vår vurdering kan UiTs hovedutfordringer med å lykkes med god implementering og etterlevelse over tid, relateres til virksomhetens komplekse organisering og behovet for styrking av kapasitet for å sikre en tilstrekkelig kraft ved implementeringen. Det er et omfattende arbeid som skal til for at man på en styrt og kontrollert måte får trygghet for samlet ivaretagelse av kravene, og for å lykkes er det nødvendig med et helhetlig apparat som samlet sett får den nødvendige kraften til både å utvikle styrende og kontrollerende føringer*

og til å implementere disse føringene i den daglige informasjonshåndteringen. Denne kompleksiteten bør det jobbes videre med, slik at alle komponentene i maskineriet går i takt. For å komme videre med innføringen av kontrollregimet for personvern- og informasjonssikkerhetsområdet, og for å kunne etterleve gjeldende krav på disse områdene over tid, har internrevisjonen tre hovedanbefalinger:

1. Rolleavklaring: Det bør arbeides videre med å definere og kommunisere hvilket ansvar og hvilke oppgaver som ligger til styrende nivå (nivå 1), og hva som forventes av implementeringen i linjen (nivå 2). Dette vil redusere risikoen for at man på operativt nivå oppfatter at noe ivaretas sentralt, og motsatt.
2. Gjennomføringsevne: Med tydeligere definerte og implementerte roller og oppgaver vil det bli lettere å styre ressursinnsatsen slik at de ulike aktørene kapasitets- og kompetansemessig settes i stand til å ta det ansvaret de er tildelt. Eksempelvis kan en prinsipielt lik rolle være mer eller mindre krevende avhengig av et fakultets eller institutts størrelse og kompleksitet. Eventuelle utfordringer bør fanges opp gjennom etablerte rapporteringslinjer, møter/utvalg og internkontroll-/risikostyringsmekanismer, slik at eventuelle vurderinger av ressursdisponering kan tas ut fra et helhetsperspektiv.
3. Helhetlig styringssystem: Styringssystemet for informasjonssikkerhet og personvern omhandler personopplysningssikkerhet, men dekker ikke personvernområdet i sin helhet. Dette er styringsverktøyet for behandlingsansvarlig ved UiT, og det er behov for justeringer slik at styringssystemet også definerer styrende krav og føringar for behandling av personopplysninger ved UiT, på linje med informasjonssikkerhet.»

Det var flere mer detaljerte anbefalinger fra PwC og gjennom 2022 vil disse bli fulgt opp. De funn som gjaldt den kontrollerende del av ledelsessystemet (revisjon/internkontroll, avvikshåndtering samt ledelsens gjennomgang) er fulgt opp, og endringer i de aktuelle kapitlene i ledelsessystemet er gjennomført.

## 6.5 Årsrapport personvernombudet

UiT har eget personvernombud, og dette skal blant annet kontrollere UiTs overholdelse av personvernforordningen (GDPR), relevant nasjonalt regelverk og UiTs interne regelverk på feltet. Personvernombudet leverer sin egen årsrapport, og den fremmes Universitetsstyret i egen orienteringssak.

## 6.6 Behov for ytterligere kontrollaktiviteter

UiT har enkelte faste kontrollaktiviteter, slik som egenvurderingen og informasjonsverdikartleggingen som skjer via statusrapporten enhetene leverer hver høst. Det er også fastsatt at internrevisjon av ledelsessystemet skal foretas ved behov og som hovedregel ikke sjeldnere enn hvert femte år. Videre blir andre kontrollaktiviteter gjennomført ved behov, men det er nødvendig å konkretisere flere av disse, eksempelvis faste kriterier for når og hvordan. Dette vil bli fulgt opp og fastsatt i egen retningslinje i løpet av våren 2022.

## **7 Ressurs- og kompetansebehov**

### **7.1 IKT-sikkerhet**

Det er behov for økt satsning på IKT-sikkerhet. Dette omfatter både investeringer i teknisk utstyr, men også personellsiden må styrkes. Detaljer fremkommer i vedlegg to.

### **7.2 Enhetene**

I internrevisjonsrapporten peker PwC på at det er utfordrende for fakultetene å håndtere det ansvaret de er tillagt for informasjonssikkerhet og personvern.

Gjennom den årlige statusrapporten melder enhetene om noe økt ressursbruk på informasjonssikkerhet i 2021. Dette er løst på ulike måter på de enkelte enhetene som har foretatt grep for å styrke dette arbeidet, alt etter hvilket behov de har og hvordan arbeidet internt er organisert. Noen enheter har opprettet administrative team med formelt ansvar for rapportering og arbeidsoppgaver knyttet til informasjonssikkerhet. Interne ressurser benyttes mer systematisk i arbeidet med risikovurderinger og rådgivning tett på de deler av organisasjonen som har primærbehovet. Det er økning i antall fakultet som inkluderer arbeid med informasjonssikkerhet i stillingsbeskrivelsen til enkeltansatte, og dermed skaper rom for at dette arbeidet ivaretas på enheten.

Imidlertid er det fortsatt enkelte enheter som beskriver en hverdag der ansvaret for arbeid med informasjonssikkerhet ikke er tydelig formalisert. Det innebærer ikke nødvendigvis at ingen arbeider med det, men det er ikke del av stillingsbeskrivelsen eller gir utslag i organiseringen internt. De som her tildeles et særskilt ansvar for oppfølging av informasjonssikkerhet gis det gjerne på bakgrunn av at de allerede innehar relevant kompetanse eller fordi de har en gitt plassering i organisasjonen. Gjennom statusrapporten skal enhetene rapportere på hvilke områder som krever nærmere fokus og tiltak, og enkelte enheter har meddelt at de vil ta en gjennomgang av ressursdisponeringen og organiseringen innen informasjonssikkerhet. For disse har kontinuitet og sikkerhetskultur blitt viktige fokusområder, samt at det fremgår at informasjonssikkerhet har blitt en fast post på ledermøter og i årshjul. For Avdeling for bygg og eiendom er ressursbruken ukjent grunnet manglende innlevering av statusrapporten. Det at enhetene har ulikt behov og varierende kompleksitet med tanke på ivaretagelse av kravene til informasjonssikkerhet og personvern vil være førende for dimensjonering, men som internrevisjonsrapporten fra PwC også påpeker må ansvar og oppgaver konkretiseres nærmere. De bør også knyttes til en rolle fremfor et individ.

### **7.3 Opplæringsaktiviteter**

Det er utfordrende å få til god opplæring for alle ansatte og studenter innenfor informasjonssikkerhet og personvern. Noe vil være felles grunnopplæring, men i stor grad har de fleste behov for tilpasset opplæring. Enhetene har rapportert om planlagte tiltak for 2022, og for flere inkluderer det opplæring.

Enhetene har rapportert om behovet for opplæring innen informasjonssikkerhet siden statusrapporten ble innført i 2019. I rapporten for 2020 pekte enkelte enheter på opplæringsaktiviteter som de planla, og det meldes i årets rapportering at disse er iverksatt. Det vises til opplæringspakke og seminar for nyansatte, workshop for vitenskapelige og saksbehandlerkurs med fokus på informasjonssikkerhet.

Som i 2020 har flere rapportert at selve arbeidet med statusrapporten gir kompetanseløft i deler av organisasjonen. Kartlagte informasjonsverdier brukes internt til kompetanseheving i sammenheng med behandling, tilgang og klassifisering. Flere satser også på digital informasjon til nytilsatte før tiltredelse som et hjelpemiddel innen informasjonssikkerhet, og dette gjør at ansatte kan tilegne seg kompetanse før behandling av informasjon starter.

Selv om statusrapporteringen viser at det gjennomføres enkeltvis, gode opplæringsaktiviteter er det sammenfallende med internrevisjonsrapport at det mangler en helhetlig plan for opplæring og kompetansebygging, samt hva opplæringen skal inneholde og kontinuitet i opplæringen. Herunder også de krav det stilles til opplæring på personvernområdet.

Av særlige tema kan det trekkes frem at UiT er pålagt å ha en protokoll over samtlige behandlingsaktiviteter som involverer personopplysninger. Det ble gjort et større arbeid i 2018 med å få denne på plass i forbindelse med ikrafttredelsen av GDPR. Det er imidlertid svært lett at slike oversikter blir utdaterte, og enhetenes kompetanse rundt protokollen og hva som skal føres der må økes.

Selv om noe opplæring kan og bør lages som egne kurs innenfor informasjonssikkerhet og personvern vil nøkkelen for å lykkes være å klare å integrere disse temaene i eksisterende opplæring. Det må bli en selvsagt del av de vanlige arbeidsprosessene, og en helt separat opplæring i denne tematikken vil kun bidra til å underbygge at det er noe særskilt og noe som tenker på litt løsrevet fra øvrige prosesser.

Det fremstår derfor som hensiktsmessig og fornuftig at UiT arbeider for at informasjonssikkerhet og personvern skal bygges inn i all internopplæring av ansatte og studenter, i det omfang som er relevant. Denne tilnærmingen er diskutert med personvernombudet som har gitt sin tilslutning til idéen.

## **8 Revisjon av ledelsessystemet**

Som nevnt ovenfor er det besluttet at ledelsessystemet skal omfatte personvern i tillegg til informasjonssikkerhet. Dette krever en gjennomgang og revisjon slik at de nødvendige endringene identifiseres og gjennomføres. Dette arbeidet ble satt noe på hold i 2021 i påvente av internrevisjonsrapporten, slik at arbeidet kunne ta med seg funnene fra internrevisjonen. Denne er nå mottatt og gjennom 2022 vil det bli foretatt en helhetlig gjennomgang og revisjon av de gjenstående delene av ledelsessystemet.

Spesielt vil det bli foretatt en gjennomgang av kapittelet om roller, ansvar og oppgaver. Til dels fordi internrevisjonen peker på at enkelte rolle- og oppgavefordelinger oppfattes som uklare, men også fordi UiT fra 1.8.21 gikk over til enhetlig ledelse og det må tas stilling til hvilken betydning denne endringen skal få for arbeidet med informasjonssikkerhet og personvern.

Videre må det utarbeides en ny strategi for informasjonssikkerhet og personvern. Dagens strategi omfattet kun informasjonssikkerhet, og gjaldt i utgangspunktet for perioden 2019 – 2021. Flere av tiltakene i strategien er forsinket, primært grunnet korona og håndtering av sikkerhetshendelsen ved UiT. På grunn av dette samt at det krever et større arbeid å få utvidet strategiens tema til å omfatte personvern er gjeldende strategi forlenget ut 2022.

## Vedlegg

*Vedleggsnumrene er fastsatt etter hvilken nummerering det enkelte vedlegg fikk i saksfremlegget hvor årsrapporten ble fremlagt Universitetsstyret 10.2.22. Her er selve årsrapporten vedlegg nr én, og følgelig starter nedenstående liste på nr to.*

- 2) Nærmere om IKT-sikkerhet ved UiT; status og behov (unntatt offentlighet)
- 3) Evalueringsrapport sikkerhetshendelsen høsten 2020 (unntatt offentlighet)

