UiO : Universitetet i Oslo
Universitetsdirektøren

Til **Universitetsstyret**
Fra **Universitetsdirektøren**

Sakstype:	**Informasjonssak**
Møtesaksnr.:	**I-sak 8**
Møtenr.:	**3/2021**
Møtedato:	**4. mai 2021**
Notatdato:	**16. april 2021**
Arkivsaksnr.:	
Saksansvarlig	**IT-direktør Lars Oftedal**
Saksbehandler:	**Espen Grøndahl, Martin Bore, Are Evju**

Status på arbeidet med informasjonssikkerhet og personvern ved Universitetet i Oslo

Kunnskapsdepartementets styringsmodell for informasjonssikkerhet i høyere utdanning og forskning spesifiserer styrets ansvar for informasjonssikkerhet og personvern. I denne saken orienteres det om UiOs arbeid på områdene.

Det vises også til tidligere orienteringer i styret 5. mai 2020 O-SAK 2 «Status på arbeidet med informasjonssikkerhet og personvern ved Universitetet i Oslo».

Hovedproblemstillinger i saken

Fokuset på informasjonssikkerhet og personvern har økt de siste årene. Informasjonssikkerhet er utfordrende på et universitet hvor man ønsker åpenhet og samarbeid med andre forskere i inn- og utlandet, samtidig som man skal benytte IT-løsninger som beskytter UiOs verdier, men som også eksponeres mot et økende antall trusselaktører. Det siste års saker med angrep mot blant annet Universitetet i Tromsø, Stortinget og Østre Toten kommune viser at trusselbildet er i stadig endring, og vi må skjerpe innsatsen innen informasjonssikkerhet.

Det er nye og tydeligere krav til informasjonssikkerhetsarbeidet i lov- og regelverk, i tildelingsbrev, digitaliseringsstrategi mv. Det er også et sterkt økende internasjonalt trusselbilde. Svikt i informasjonssikkerhetsarbeidet kan medføre store konsekvenser for UiO, både økonomisk og omdømmemessig.

I denne saken orienteres styret om følgende:

- Trusselbildet og informasjonssikkerhetsløft
- Digitalisering
- Policy for informasjonssikkerhet
- Eksportkontroll
- Hendelseshåndtering og uønskede hendelser

- Ledelsessystem for informasjonssikkerhet
- Internkontroll
- Personvern
- Teknisk gjeld
- Videre arbeid

Arne Benjaminsen
universitetsdirektør

Lars Oftedal
IT-direktør

Vedlegg:

- Fremleggsnotat med tilhørende vedlegg

UiO : Universitetet i Oslo

FRA
UNIVERSITETSDIREKTØREN

FREMLEGGSNOTAT
Møtesaksnr.: I-sak 8
Møtedato: 4. mai 2021
Notatdato: 16. april 2020
Arkivsaksnr.:
Saksbehandler: Bore, Evju, Grøndahl

TIL
UNIVERSITETSSTYRET

Status på arbeidet med informasjonssikkerhet og personvern ved Universitetet i Oslo

> *«Digitalisering er en viktig driver i samfunnsutviklingen og bidrar til vår velferd, trygghet og verdiskaping. Den teknologiske utviklingen fører imidlertid til at sårbarhetsflaten øker. Et dynamisk og komplekst sårbarhetsbilde gjør det utfordrende å tilpasse sikkerhetstiltakene raskt nok.» Jf. NSM risiko 2021. S. 7*

Det siste året har vært et år preget av pandemien vi er inne i, og av at digitaliseringen av UiO og Norge har gått på høygir. På ett år har det på UiO vært holdt mer enn 523 000 møter i Zoom fordelt på over 3,6 millioner unike møtedeltakere. Digitaliseringen har også satt UiOs infrastruktur på prøve, UiO har opplevd en økning av ondsinnede aktører som prøver å komme seg inn i UiOs digitale tjenester, og vi opplever daglig forsøk på dataangrep med forskjellig alvorlighetsgrad.

I det følgende legger vi beskrivelsene i statusen fra 5. mai 2020 til grunn[1], og kommenterer endringer som er skjedd siden da. Som beskrevet i forrige status har UiO siden innføringen av EUs personvernforordning (GDPR) i 2018 hatt et særlig fokus på informasjonsarbeid og rutiner knyttet til etterlevelse av dette regelverket.

Trusselbildet og informasjonssikkerhetsløft

Trusselbildet er i endring, aktørene blir mer målrettet og bruker mer ressurser. Politiets sikkerhetstjeneste sin nasjonale trusselvurdering 2021[2] tar opp problematikken med økende interesse fra utenlandske aktører inn mot vår sektor.

> *«Flere stater vil i 2021 forsøke å anskaffe teknologi i Norge som de ikke har lov til å kjøpe, på grunn av eksportkontrollregelverket og vestlige sanksjoner. I tillegg vil noen stater utnytte norske utdannings- og forskningsinstitusjoner gjennom ulovlig kunnskapsoverføring. Russland, Kina, Iran og Pakistan vil utgjøre den største trusselen.»*

[1] O-SAK 2 Orientering om status for arbeidet med informasjonssikkerhet og personvern ved universitetet i Oslo

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

Internkontrollen utført for 2020 viser behovet for å arbeide mer med eksportkontroll i tiden framover. Vi kommer tilbake til internkontrollen under.

Det siste året har Norge vært rammet av flere store informasjonssikkerhetshendelser. Av de større kan vi nevne dataangrep mot Stortinget sommeren 2020 samt et større angrep mot Universitetet i Tromsø som ble avdekket i desember 2020. Angrepet i Tromsø medførte at UiT satte ned krisestab i over 2 måneder, og store deler av IT-virksomheten ble lammet. En alvorlig sårbarhet i Microsoft Exchange våren 2021 traff bredt globalt, og Stortinget var blant mange norske virksomheter som opplevde vellykkede angrep. Med disse og andre tilsvarende saker i bakhodet ser USIT at det er nødvendig å gjøre et informasjonssikkerhetsløft i 2021 for på en hensiktsmessig måteå kunne beskytte UiO sine informasjonsverdier i tråd med økte digitale trusler.

UiO har alltid hatt god informasjonssikkerhet og arbeid med informasjonssikkerhet innebærer tiltak som skal sikre følgende:

- *Tilgjengelighet:* Sikrer mot tap av eller avbrudd i tilgangen til informasjon og data
- *Konfidensialitet:* Sikrer mot ikke-autorisert innsyn i, endring av eller offentliggjøring av informasjon og data
- *Integritet:* Sikrer informasjonens og dataenes nøyaktighet, fullstendighet og opprinnelighet

UiO har en stor og kompleks IT-infrastruktur med over 20.000 datamaskiner, fordelt på klienter og servere. For å kunne håndtere en IT-sikkerhetshendelse, og få full oversikt over hva som har skjedd, må store mengder data fra flere forskjellige kilder analyseres. Historisk har dette vært en svært omfattende manuell jobb. Logger måtte samles inn fra mange forskjellige kilder og formater, og store datamengder måtte tolkes. UiO hadde mye data, men ingen god måte å bruke informasjonen effektivt på i det operative arbeidet.

USIT har en moderne plattform for håndtering av loggdata. Løsningen skalerer godt og oppslag som før kunne ta timer er nå gjort på sekunder. Plattformen er ett av de viktigste verktøyene i det operative IT-sikkerhetsarbeidet.

God drift av IT-systemer er en avgjørende del av godt informasjonssikkerhetsarbeid. UiO var tidlig ute med å standardisere og sentralisere drift av våre IT-systemer. Vi har i mange år sikret systemene våre etter flere grunnprinsipper. Et av prinsippene er sikkerhet i dybden, hvor vi, så langt det lar seg gjøre, forsøker å sikre systemene og tjenestene med sikringstiltak på flere nivåer slik at vi ikke er avhengig av ett enkelt sikringstiltak for å være trygge. Et annet sentralt prinsipp er god grunnsikring. Vår grunnsikring er basert på beste praksis fra leverandørene på alle systemer vi setter opp, samt at vi har ytterligere sikring basert på egne risikovurderinger.

God grunnsikring og flere barrierer har en rekke ganger reddet UiO fra større sikkerhetshendelser som har rammet bredt ellers i verden, eksempelvis har dette beskyttet oss i større saker som angrepene som traff Stortinget i fjor og tidligere i år.

Utviklingen i samfunnet viser at målrettede aktører setter inn stadig flere ressurser for å finne og utnytte svakheter i oppsett, programvare og oss som enkeltpersoner og hvordan vi bruker de forskjellige IT-systemene. E-tjenesten, PST og nasjonal sikkerhetsmyndighet peker alle på vår sektor som en spesielt utsatt sektor i sine årlige åpne trusselvurderinger. USIT arbeider med et notat til Universitetsdirektøren med beskrivelser av nødvendige tiltak i informasjonssikkerhetsløftet. Vi kommer tilbake til noen av disse tiltakene senere i dette dokumentet.

Rett før påske åpnet forsknings- og høyere utdanningsminister Henrik Asheim Cybersikkerhets-senter for forskning og utdanning. Senteret samler kunnskapssektorens fremste ekspertise innenfor cybersikkerhet, og blir en sentral brikke i kampen mot trusselaktørene. UiO bidrar som partner i senteret.

Digitalisering

Digitalisering i høyere utdanning og forskning er et kjerneområde i føringer fra Kunnskapsdepartementet (KD) og andre offentlige myndigheter. Digitalisering medfører at universitetets oppgaver kan effektiviseres og, som vi virkelig har sett det siste året, opprettholdes og videreutvikles selv om tilgang til fysiske lokaler har vært begrenset. Vi ser at arbeidsprosesser, undervisning og formidling utføres på effektive, nyskapende og kreative måter. Samtidig medfører digitalisering at stadig mer av universitetets verdier og beskyttelsesverdige informasjon behandles i komplekse tekniske løsninger, ofte hos tredjeparter og på ulike enheter. KDs digitaliseringsstrategi slår fast at det er behov for en målrettet styrking av arbeidet med informasjonssikkerhet og personvern.

Da universitetet ble stengt ned i mars i 2020 på grunn av Covid-19, startet en massiv digitalisering på universitetet. På svært kort tid flyttet universitetet undervisningen og møtevirksomhet fra fysiske rom til digitale flater. Universitetet hadde allerede før nedstengingen gode rutiner for vurderingen av IT-sikkerhet og personvern i sine tjenester. Dette har bidratt til at det ikke har vært nødvendig med store endringer i tjenester som ble hasteinnført i forbindelse med den første nedstengingen i 2020.

Selv om UiO har gjort veldig mye riktig det siste året innenfor digitalisering, er dette ikke en jobb som er ferdig i det en tjeneste er innført. Alle tjenester krever forvaltning i forskjellig grad etter hvert som bruken utvikler seg, nye behov oppstår, det skjer teknologiske endringer, eller endringer i rettstilstanden.

Digitaliseringen som har skjedd på UiO det siste året hadde ikke vært mulig uten kompetansen USIT og IT-virksomheten sitter på. Ved å klare å holde på et godt fagmiljø på tvers av informasjonsteknologien har organisasjonen vært i stand til å sammen snu seg rundt og virkelig levere. Dette hadde ikke vært mulig hvis UiO istedenfor å satse på USIT hadde satt ut leveranser til tredjepart.

Policy for informasjonssikkerhet

Som ledd i at KD i 2019 innførte en ny styringsmodell for informasjonssikkerhet, har Unit utarbeidet en policy for informasjonssikkerhet og personvern i høyere utdanning og forskning. Denne ble vedtatt av KD, og ble gjeldende fra 01.10.2020. Policyen oppsummerer nasjonale føringer og lovkrav til informasjonssikkerhet og personvern og brukes av Unit i den årlige kartleggingen av arbeidet med informasjonssikkerhet og personvern.

I policyen pekes det på viktigheten av at institusjonene har oversikt over eksportkontrollregelverket. Den siste tiden har også media hatt fokus på universitets- og høyskolesektorens etterlevelse av dette regelverket. Eksportkontroll innebærer at visse varer, teknologi og tjenester ikke kan eksporteres fra Norge uten lisens utstedt av Utenriksdepartementet. Særlig relevant for UiO er at immateriell teknologi og kunnskapsoverføring er dekket av regelverket. Internkontrollen for 2020 viser at det fortsatt er et strukturelt problem at mange enheter mener at regelverket ikke er relevant. Regelverket er ikke nytt, men det har tidligere hatt noe begrenset fokus innad i sektoren. Det gjøres allerede arbeid på feltet, det er viktig at dette arbeidet fortsetter og at det sikres god kommunikasjon med Unit og KD. Utfordringene er felles for

alle i sektoren, og det må komme felles retningslinjer. Utenriksdepartementet utarbeider nå oppdaterte retningslinjer om eksportkontrollregelverket som er bedre tilpasset UH-sektoren, det er viktig at dette arbeidet følges opp på UiO, så vi sikrer at ansatte ved UiO ikke står i fare for å bryte regelverket.

Hendelseshåndtering og uønskede hendelser

Vi ser en betydelig nedgang i innmeldinger av personsikkerhetsbrudd ved UiO, fra 38 i 2019 til 24 i 2020. Internkontrollen for 2020 viser at det er en nedgang i kjennskap til avviksrutiner både blant ledere og ansatte. Vi har grunn til å tro at noe av nedgang skyldes utstrakt bruk av hjemmekontor som resulterer i at noe av «institusjonshukommelsen» forsvinner når ansatte ikke møtes ansikt til ansikt i like stor grad som tidligere. Avvikene som går igjen er primært manglende tilgangsstyring og feilsendt informasjon, og vi ser fremdeles et behov for grunnleggende opplæring i informasjonssikkerhet. Siden forrige gjennomgang har UiO meldt fem avvik til Datatilsynet. I alle tilfellene har Datatilsynet vært fornøyd med hendelseshåndteringen til UiO, og har ikke sett behov for å følge opp sakene.

I februar 2021 ble UiO utsatt for et dataangrep, en sårbarhet i programkode ble utnyttet og ukjente gjerningspersoner misbrukte sårbarheten til å utvinne kryptovaluta. Angrepet ble raskt avdekket og stoppet, saken er politianmeldt.

I juli 2020 oversendte Unit «Rammeverk for håndtering av IKT-sikkerhetshendelser i UH-sektoren» som ble gjeldende fra mottaksdato. Rammeverket er en sektortilpassing av nasjonal sikkerhetsmyndighet sitt rammeverk for håndtering av sikkerhetshendelser og beskriver aktører og varslingslinje ved større IKT-sikkerhetshendelser. USIT følger opp implementering av rammeverket, som i stor grad understøtter eksisterende rutiner og prosesser. Kunnskapsdepartementet har besluttet at alle virksomheter omfattet av rammeverket må oppfylle forventningene som er spesifisert, dette inkluderer blant annet en plikt til å ha nødvendig kompetanse og kapasitet til å kunne følge opp hendelser i det digitale rom på en tilfredsstillende måte.

UiO-CERT har sett eksempler på hendelser hvor én del av UiO sin IT-infrastruktur har blitt benyttet, ved hjelp av brukernavn og passord på avveie, for å angripe eller misbruke andre deler av infrastrukturen. Vi er ikke kjent med saker hvor dette har fått alvorlige konsekvenser, eller hvor det er tydelig at trusselaktør har arbeidet målrettet og «forstått» hvilken bredde av IT-tjenester de har hatt mulighet til å utnytte. Vi kan se for oss tap eller endring av data som brukes i forskning som områder hvor en målrettet aktør kan gjøre uopprettelig skade.

UiO-CERT håndterte i underkant av 3000 innkommende saker i 2020. Håndtering av saker i et slikt omfang er mulig på grunn av veletablerte rutiner og høy kompetanse, på tross av få dedikerte personellressurser. Saksmengden er økende, og det er svært viktig at UiO klarer å opprettholde og videreutvikle kompetansen som er bygget opp gjennom mange år.

I snitt håndterer UiO-CERT i overkant av 100 saker i året der brukernavn og passord til UiO-brukerkontoer har kommet på avveie og blitt misbrukt. Til nå i 2021 (per 15. april) er vi kjent med 78 slike saker, en svært uheldig utvikling. Såkalt flerfaktor-autentisering/multifaktorautentisering/to-faktor-autentisering er det viktigste tekniske tiltaket som vi ser kan hjelpe til med å begrense dette antallet. USIT ser behovet for å innføre dette alle steder det er teknisk mulig, og følger opp dette i sikkerhetsløftet beskrevet over. Arbeidet er igangsatt.

Ledelsessystemet for informasjonssikkerhet

Ledelsessystem for informasjonssikkerhet (LSIS) skal gjennom en årlig ledelsens gjennomgang. Det har i løpet av 2020 ikke vært meldt inn eller avdekket behov for større endringer.

Den delen av LSIS som er mest relevant for brukere flest er klassifiseringen av informasjonsressurser og lagringsguiden. Dette er veiledere om hvordan informasjonsressurser skal klassifiseres i en av de fire klassene - grønn, gul, rød eller svart. Lagringsguiden veileder brukerne om hvilke tekniske løsninger som er godkjent for hvilken klasse. Vi ser at dette klassifiseringssystemet har satt seg, og er godt implementert i organisasjonen, men det er et sterkt og økende behov for rådgiving og veiledning. Det jobbes kontinuerlig med å forbedre dokumentasjon og fagspesifikke veiledere for å sikre at informasjonsressurser klassifiseres likt og riktig på tvers av organisasjonen.

Det har i løpet av 2020 blitt utarbeidet nye tillegg til LSIS, som veileder hvordan videoverktøy kan brukes på en sikker og personvernvennlig måte for å gjennomføre intervjuer og møter. Det har også blitt laget en veiledning for hvordan Zoom kan brukes til å gjennomføre intervjuer og undervisning med rød data.

Internkontroll

Universitetet er pålagt å gjennomføre organisatoriske tiltak for å sikre overholdelse av personvernregelverket. Internkontrollen er et ledd i oppfyllelsen av denne forpliktelsen, og er inntatt i LSIS kapittel 14. Den årlige internkontrollen av behandlinger av personopplysninger ble gjennomført ved at ledelsen ved hver grunnenhet besvarte et nettskjema.

Internkontrollen viser at UiO har generelt sett har ganske god kontroll på personvern, men internkontrollen viser også at ett år med hjemmekontor har satt sine spor, og at kunnskapen om personvern har på de fleste områdene som kontrollen dekker, har hatt en nedgang, og er nå på samme nivå som internkontrollen som ble gjennomført i 2019.

Personvern

I juli 2020, avsa EU-domstolen en avgjørelse i Schrems II-saken[3]. I etterkant av avgjørelsen har Unit anbefalt institusjonene til å ikke ta i bruk nye tjenester som medfører en overføring til land utenfor EØS, og da særlig til USA. Unit har satt ned en arbeidsgruppe som jobber med oppfølging av eksisterende fellestjenester i sektoren, og utarbeidelse av felles retningslinjer i sektoren. UiO deltar aktivt i arbeidsgruppen. Det er ventet at arbeidsgruppen skal komme med sitt forslag i løpet av vårsemesteret.

Det er ventet endelige retningslinjer fra Det europeiske personvernrådet (EDPB) i løpet av våren 2021, som gir veiledning om hvordan virksomheter lovlig kan overføre personopplysninger til land utenfor EØS. Det er publisert foreløpige retningslinjer som har vært på offentlig høring.[4] UiO har sammen med FHI inngitt høringssvar til retningslinjene. Det er sannsynlig at det blir juridisk

[3] C-311/18, https://curia.europa.eu/juris/document/document.jsf?text=&docid=228677&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=8607144

[4] https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/recommendations-012020-measures-supplement-transfer_en

vanskelig for europeiske virksomheter å bruke skytjenester som lagrer og håndterer personopplysninger i USA. Til tross for dette har rettsavgjørelsen skapt mindre problemer innen forskningssamarbeid på tvers av landegrensene, og det er ikke forventet at de endelige retningslinjene vil negativt påvirke forskningssamarbeid med samarbeidspartnere utenfor EØS.

UiO har i løpet av 2020 kommet med oppdaterte rutiner for lyd- og bildeopptak ved UiO. Rutinene måtte oppdateres for å være i tråd med gjeldende personvernregelverk. Ved oppdateringene av rutinene, har det også vært fokus på å forenkle rutinene, noe som har resultert i at det nå i mange tilfeller er enklere å gjennomføre opptak av undervisning og arrangementer.

På oppdrag fra UV-fakultetet utviklet LINK i samarbeid med juristene i IT-direktørens stab et e-læringskurs i personvern til forskere og studenter i 2020. Kurset for UV-fakultetet er ferdigstilt, og juristene i IT-direktørens stab tilbyr nå å lage tilpassede kurs til de fakultetene som ønsker det. Per april 2021 jobber USIT med tilpassede kurs til alle fakultetene med unntak av Det juridiske fakultet. USIT vil i løpet av 2021 lage innhold til e-læringskurs innen personvern for administrativt ansatte.

Teknisk gjeld

UiO var tidlig ute med å ta i bruk informasjonsteknologi, og det har historisk vært stor interesse på tvers av hele organisasjonen for å ta i bruk ny teknologi. En bieffekt av dette er at det er en stor del gamle systemer som i varierende grad er i bruk. De er satt opp uten at USIT eller lokal-IT- har vært involvert og de blir dårlig vedlikeholdt. UiO-CERT får stadige henvendelser fra eksterne sikkerhetsforskere som påpeker sårbarheter i systemer på UiO-nett. Situasjonen hos Universitetet i Tromsø viser viktigheten av å ha sikker og stabil drift, i alle ender. Enkeltsystemer som ikke blir vedlikeholdt kan medføre alvorlige konsekvenser på tvers, de kan bli en vei inn på innsiden av infrastrukturen vår. En tjeneste som virker uskyldig og ikke inneholder noen beskyttelsesverdige data, kan bli et farlig springbrett inn mot annen kritisk infrastruktur. Det er derfor viktig at UiO klarer å ta tak i dette problemet før det treffer oss på tilsvarende måte som hos UiT. USIT følger opp problemstillingen i sikkerhetsløftet.

Videre arbeid

UiO arbeider godt med informasjonssikkerhet, men på grunn av det økte trusselbilde og teknologisk utvikling, er det behov for å gjennomføre et sikkerhetsløft på UiO. USITs sikkerhetsløft for 2021 der innføring av multifaktorautentisering på sluttbrukertjenester og opprydding i teknisk gjeld er blant de viktigste tiltakene som UiO kan gjennomføre for å beskytte UiO mot trusselaktører i fremtiden.

Vedlegg:

- Status informasjonssikkerhet
- Status personvern

Krav	Tilstand 2019	Tilstand 2020	Tilstand 2021	Status på eksisterende tiltak	Behov for tiltak
Gjennomført/revidert ROS-analyse i 2017/2018					
ROS analyser på administrative systemer og på infrastruktur komponenter	God	God	God	Som en del av GDPR prosjektet i 2018 ble det gjennomført og/eller oppdatert ROS på alle kartlagte IT-systemer. Disse følges opp annenhvert år, eller ved større endringer.	
ROS analyse av USIT	Tilfredstillende	Tilfredstillende	Tilfredstillende	Det er ikke ferdigstilt en egen ROS av USIT som driftsleverandør, men arbeidet er påbegynt	
ROS av systemer i forskning og utdanning	Ikke tilfredstillende	Tilfredstillende	Tilfredstillende	Et nettskjema for egenrapportering av mindre skytjenester til bruk i forskning og utdanning bidrar nå til at flere systemer blir registrert og får gjennomført en nødvendig vurdering av personvern og informasjonssikkerhet. Det oppdages fremdeles flere systemer i bruk på UiO som ikke er godkjent, men oftere enn i fjor er dette systemer som brukes i mindre skala. Det er etablert strategiske koordineringsgrupper innen forskning og utdanning.	Det må etableres en prosess for å styre valg av verktøy og tjenester i bruk for forskning og utdanning. Det må sikres at tjenester som er tatt i bruk skjer lovlig, med de nødvendige avtaler på plass.

Krav	Tilstand 2019	Tilstand 2020	Tilstand 2021	Status på eksisterende tiltak	Behov for tiltak
Gjennomført og evaluert en kriseøvelse					
Generell kriseøvelse	God	God	Tilfredstillende	Planlagt for høsten 2021	
Spesifikk øvelse på informasjonssikkerhet	Tilfredstillende	God	God	Gjenomført våren 2021	
Evaluering av kriseøvelse	Tilfredstillende	God	Tilfredstillende	Planlagt for høsten 2021	

Krav	Tilstand 2019	Tilstand 2020	Tilstand 2021	Status på eksisterende tiltak	Behov for tiltak
Ledelsessystem for informasjonssikkerhet - LSIS					
Ledelsessystem for informasjonssikkerhet gjort kjent i organisasjonen	God	God	God	Ila. 2020 er det gjennomført en bred informasjonsrunde med bekjentgjøring av LSIS i hele organisasjonen.	Informasjonsrunden har avdekket at det er et kontinuerlig behov for opplæring og informasjon om temaet. Det jobbes med å få på plass e-læring.
Kartlegging av kjennskap og etterlevelse av LSIS	God	God	God	Som en del av internkontrollen er det gjennomført en kartlegging av kjennskap til, og etterlevelse av gjeldene regelverk for informasjonssikkerhet og personvern	

Krav	Tilstand 2019	Tilstand 2020	Tilstand 2021	Status på eksisterende tiltak	Behov for tiltak
Ledelsessystem for informasjonssikkerhet - LSIS					
Oppfølging av funn i kartleggingen	Tilfredstillende	Tilfredstillende	Tilfredstillende	Kartleggingen viser tildels store mangler i kjennskap og etterlevelse ved enkelte enheter	Målrettede tiltak mot enkelte enheter.
Ledelsens gjennomgang	Tilfredstillende	God	God	Gjennomført som årlig rapportering til Universitetsstyret	
Grunnsikring - KD oppfordrer institusjonene til å løfte informasjonssikkerheten høyere enn de nasjonale minstekravene.	God	God	God	UiO har i LSIS videreført krav om grunnsikring. UiO har lange tradisjoner for felles drift, oppsett og konfigurasjon av systemer. Med noen lokale tilpassinger er alle tiltak i NSMs «ti viktige tiltak mot dataangrep» iverksatt på UiO.	Informasjonssikkerhetsløft i 2021
Internkontroll på informasjonssikkerhetsområd	God	God	God	Gjennomført årlig hver vår sammen med internkontroll for bruk av	

Krav	Tilstand 2019	Tilstand 2020	Tilstand 2021	Status på eksisterende tiltak	Behov for tiltak
Hendelseshåndtering					
Har institusjonen innført rutine for å håndtere uønskede digital hendelser	God	God	God	UiO-CERT er UiOs operative hendelsesteam. De har eksistert siden 2005, har gode og dokumenterte rutiner med god nasjonalt og internasjonalt nettverk.	
IT-beredskap og kontinuitetsplan	Tilfredstillende	Tilfredstillende	Tilfredstillende	IT-beredskapsplan er innført, trent og øvd. Det er mangler ved kontinuitetsplaner	Det må innføres konfinuitetsplaner for viktige prosesser. Dette må følges opp også utenfor USIT.
Krav	**Tilstand 2019**	**Tilstand 2020**	**Tilstand 2021**	**Status på eksisterende tiltak**	**Behov for tiltak**
Eksportkontroll					
Har institusjonen oversikt over kunnskapsområder som reguleres av eksportkontroll-lovgivningen		Ikke tilfredstillende	kke tilfredstillend	Interkontrollen 2019 og 2020 viser at enhetene ikke har god nok oversikt over eksportkontroll-regelverket	UiO må innføre oppdaterte retningslinjer når dette foreligger fra UD
Etterlever institusjonen eksportkontroll-lovgivningen		Ikke tilfredstillende	kke tilfredstillend	Interkontrollen 2019 og 2020 viser at enhetene ikke har god nok etterlevelse av eksportkontroll-regelverket	UiO må kartlegge hva som er underlagt regelverket og gjøre nødvendige tiltak

Krav	Tilstand 2019	Tilstand 2020	Tilstand 2021	Status på eksisterende tiltak	Behov for tiltak
Krav om oversikt over all behandling av personopplysninger i forskning					
Medisinsk og helsefaglig forskning	Tilfredstillende	God	God	Oversikt over medisinsk- og helsefaglige forskningprosjekter (tidligere Helseforsk) ble i 2019 utvidet til å kunne registrere alle forskningsprosjekter ved UiO og skiftet navn til Forskpro. Forskpro er i bruk ved alle fakulteter med unntak av Det juridiske fakultet.	
Forskning på øvrige personopplysninger	God	God	God	NSDs meldingsarkiv gir en oversikt over UiOs forskning på personopplysninger. Alt som skal til NSD meldes i stor grad til NSD.	

Krav	Tilstand 2019	Tilstand 2020	Tilstand 2021	Status på eksisterende tiltak	Behov for tiltak
Krav om oversikt over all behandling av personopplysninger					
Register over administrative behandlinger	Tilfredstillende	Tilfredstillende	Tilfredsstillende	Oversikt over administrative behandlinger av personopplysninger (meldeappen) er oppdatert i 2020 for å gjøre den mer brukervennelig. Det er fremdeles mangelfulle registreringer.	Kreves større bevissthet og bedre kontroll fra ledelsen på enhetene om lovlig bruk av systemer og større bevissthet rundt hvilke systemer og behandlinger som skal registreres i meldeappen. Det arbeides med en veiledning for hva som skal registreres for å sikre etterlevelse.
Oversikt over systemer brukt i forskning og utdanning	kke tilfredstillend	Tilfredstillende	Tilfredsstillende	Et nytt nettskjema for egenrapportering av mindre skytjenester til bruk i forskning og utdanning bidrar nå til at flere systemer blir registrert og får gjennomført en nødvendig vurdering av personvern og informasjonssikkerhet. Det oppdages fremdeles flere systemer i bruk på UiO som ikke er godkjent, men oftere enn i fjor er dette systemer som brukes i mindre skala.	Det må fremdeles kommuniseres tydelig fra enhetene at man kun kan ta i bruk systemer som UiO har godkjent slik at UiO har kontroll på informasjonssikkerheten og personvernet. Nettskjemaet for egenrapportering av mindre tjenester må bli bedre kjent på enhetene.

Krav	Tilstand 2019	Tilstand 2020	Tilstand 2021	Status på eksisterende tiltak	Behov for tiltak
Krav om intern forankring/godkjennelse av alle forskningsprosjekt som behandler personopplysninger					
Medisinsk- og helsefaglige forskningsprosjekter	Tilfredstillende	God	God	Tjenesteavtalen med NSD om vurderinging av forskningsporsjekter som behandler personopplysninger, er utvidet til også å omfatte medisinske og helsefaglige prosjekter. NSD bistår forskere med personvernkonsekvensvurdering (DPIA) når dette er nødvendig.	

Krav	Tilstand 2019	Tilstand 2020	Tilstand 2021	Status på eksisterende tiltak	Behov for tiltak
Krav om internkontroll					
Generelle veiledere	God	God	God	Oppdaterte generelle rutiner og veiledere for behandling av personopplysninger i forskning og i administrasjonen.	

Internkontroll/Kvalitetssystem for forskning på personopplysninger	Tilfredstillende	Tilfredstillende	Tilfredsstillende	Rutine for forskning med personopplysninger er vedtatt og publisert. Kvalitetssystemet for medisinsk og helsefaglig forskning er oppdatert for å speile de nye rutinene om søknad til NSD for all forskning med personopplysninger.	Rutinene for forskning på personopplysninger skal utvides til å tydeligere avklare roller og ansvar på UiO ved behandling av personopplysninger i forskning.
Dedikerte personer på enhetsnivå med ansvar for personvern	God	God	God	Personvernkontakter på alle enheter blir kurset til å kunne besvare personvernspørsmål fra egen enhet. Bidrar til kompetanseheving og oversikt over personverrettslige problemstillinger og løsninger på egen enhet.	

Kursing og veiledning av ansatte/forskere/studenter	Tilfredstillende	Tilfredstillende	Tilfredstillende	Opplæringsprogram på UiOs enheter ved behov og på forespørsel. Utøver av behandleransvaret holder jevnlig kurs/presentasjoner for studenter og ansatte på alle enheter, men antall avholdte kurs i 2020 er lavere enn tidligere år. E-læringskurs innen personvern i forskning er utviklet og tatt i bruk hos UV-fakultetet. Tilpassede kurs til alle andre fakultet en Det juridiske fakultet er under arbeid. Spørsmål om personvern besvares fortløpende på telefon og e-post. Personvernkontakter kurses slik at de kan besvare spørsmål fra egen enhet.	Innhold til e-læringskurs for administrativt ansatte innen personvern er planlagt utarbeidet i løpet av 2021
Internkontrollsystem	God	God	God	Internkontrollsystem i form av årlig skriftlig interkontroll/brevkontroll og stedlig kontroll er revidert og implementert. Ledere ved alle enheter besvarer en skriftlig internkontroll i februar/mars og stedlige kontroller gjennomføres fortløpende med spesifikke tema i fokus.	

Krav	Tilstand 2019	Tilstand 2020	Tilstand 2021	Status på eksisterende tiltak	Behov for tiltak
Krav om ett overordnet personvernombud	God	God	Tilfredstillende	Konstituert personvernombud er ansatt i 50% stilling. Stillingsinstruks er vedtatt av Universitetsstyret.	Evaluering av ombud i en 50 % stillling skal gjennomføres i løpet av 2021