UNIVERSITETET
I OSLO

Til: Universitetsstyret
Fra: Universitetsdirektøren

Sakstype: Orienteringssak
Møtesaksnr: I-sak 12-2023
Møtenr: 3/2023
Møtedato: 5. mai 2023
Notatdato: 24.04.2023
Arkivsaksnr:
Saksansvarlig: IT-direktør Lars Oftedal
Saksbehandlere: Sindre Pemmer Aalen, Isak Falck Alsos, Espen Grøndahl, Ståle Askerød Johansen, Vilde Nenseth

---

Status på arbeidet med informasjonssikkerhet og personvern

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 for styret i I-SAK 10/22 «Status for informasjonssikkerhet og personvern ved UiO 2022».

Hovedproblemstillinger i saken
I denne saken orienteres styret om følgende:

- Økende og endret trusselbilde
- Informasjonssikkerhetsløft og tofaktorautentisering
- Digitalisering og kompleksitet, særlig i fellestjenester
- Hendelseshåndtering og uønskede hendelser
- Internkontroll og ledelsessystem for informasjonssikkerhet
- Personvernsarbeidet ved UiO
- Videre arbeid og samarbeid i sektoren

Konsekvenser for økonomi, bemanning og lokaliteter
Det er tydelige og utstrakte krav til informasjonssikkerhetsarbeidet i lov- og regelverk, i tildelingsbrev, digitaliseringsstrategi mv., samtidig som trusselbildet er i endring. Svikt i informasjonssikkerhetsarbeidet kan medføre store konsekvenser for UiO, både økonomisk og omdømmemessig.

Arne Benjaminsen
universitetsdirektør

Lars Oftedal
IT-direktør

Vedlegg
- Fremleggsnotat med tilhørende vedlegg

UiO : Universitetet i Oslo

FRA
UNIVERSITETSDIREKTØREN

FREMLEGGSNOTAT
Møtesaksnr.: I-sak 12-2023
Møtedato: 5. mai 2023
Notatdato: 24. april 2023
Arkivsaksnr.:
Saksbehandlere: Sindre Pemmer Aalen, Isak Falck Alsos, Espen Grøndahl, Ståle Askerød Johansen, Vilde Nenseth

TIL
UNIVERSITETSSTYRET

Status for informasjonssikkerhet og personvern ved UiO 2023

Det siste året har vært preget av krigen i Europa og store nyhetssaker om innsidevirksomhet ved norske universiteter. Trusselbildet endrer seg raskt, og sikkerhetsmiljøet i hele Norge må tilpasse seg kontinuerlig. Samtidig ser vi at bevisstheten og oppmerksomheten på både nasjonal og digital sikkerhet øker i befolkningen. Ved UiO gjøres det mye godt sikringsarbeid i alle ledd, og bevisstheten øker. Tekniske sikringstiltak utvides, forvaltes og er viktige. Forskere viser stor interesse for å følge rutiner for riktig klassifisering og lagring av data, og vi ser at UiOs fokus på sikkerhet over mange år bidrar til at det er enklere for forskere å kunne dele data også når rettsbildet og kompleksiteten øker – nettopp fordi vi over mange år har arbeidet med å tilby systemer med innebygget personvern. Samtidig er det utfordrende med økt kompleksitet og krav til mangfold, og standardisering, bevisstgjøring og rutiner må prioriteres.

På UiO startet året med en svak nedgang i it-sikkerhetsrelaterte hendelser, men utover året så vi en trend der kontoer på avveie stadig ble forsøkt misbrukt til mer enn bare sende ut e-post. Denne trenden snudde etter hvert som tofaktorautentisering ble innført.

Om trusselbildet

Trenden fra i fjor med et økende og endret trusselbilde fortsetter. Både NSM og PST fremhever de samme truslene i år som i fjor, samtidig som flere reelle eksempler på spionasje og etterretning ved andre universiteter har kommet fram i media. I PST sin nasjonale trusselvurdering for 2023 fremheves det at norske forsknings- og

utdanningsinstitusjoner er utsatte etterretningsmål for ulovlig kunnskapsoverføring fra flere land vi ikke har et sikkerhetssamarbeid med. De skriver: «Vi har i 2022 registrert et økt antall saker ved norske forsknings- og utdanningsinstitusjoner der bakgrunn, kompetanse og fagretning hos gjesteforskere/professorer kan medføre at norsk teknologi og kunnskap benyttes på måter som strider med eksportkontrollregelverket. Denne utviklingen vil vedvare i 2023» (PST: Nasjonal trusselvurdering 2023).

- **Ulovlig kunnskapsoverføring «**Norske forsknings- og utdanningsinstitusjoner er utsatte etterretningsmål for ulovlig kunnskapsoverføring fra flere land vi ikke har et sikkerhetssamarbeid med. Disse forskningsmiljøene holder et høyt internasjonalt nivå, har gode finansieringsordninger og tilgang til avanserte laboratorier og annen forskningsinfrastruktur. Noen land har en sterk interesse av å utnytte denne tilgangen og fortrinnene ved norske universitets- og forskningsinstitusjoner. Spesielt høyere utdannet personell med koblinger til utenlandske universiteter som er relevante for militær kapasitetsbygging, representerer en trussel innen ulovlig kunnskapsoverføring. Vi har i 2022 registrert et økt antall saker ved norske forsknings- og utdanningsinstitusjoner der bakgrunn, kompetanse og fagretning hos gjesteforskere/professorer kan medføre at norsk teknologi og kunnskap benyttes på måter som strider med eksportkontrollregelverket. Denne utviklingen vil vedvare i 2023.» (PST: Nasjonal trusselvurdering 2023)

- **Innsidevirksomhet og spionasje «**I løpet av 2022 har media omtalt en rekke saker om mulig innsidevirksomhet. I Sverige ble et brødrepar som jobbet i de svenske sikkerhetstjenestene dømt for grov spionasje. En ansatt i den tyske etterretningstjenesten er siktet for å ha delt svært sensitive og hemmelige opplysninger om vestlige etterretningsoperasjoner i forbindelse med Russlands krigføring i Ukraina. Også i Norge har innsidere blitt avdekket. Samtlige av disse har til felles at de er siktet eller tiltalt for å ha jobbet på vegne av Russland. Etterretningstjenesten og PST peker på at trusselaktørene er svært interessert i flere forskningsområder ved norske universiteter, og at disse institusjonene utnyttes for å kartlegge potensielle kilder.» (NSM: Risiko 2023)

- **Etterretning mot teknologiforskning «**Nye fremvoksende teknologier er ettertraktet av statlige aktører for å sikre militær evne, politisk innflytelse og økonomisk vekst. Blant disse er varer og teknologi som også har militære bruksområder. Norske virksomheter som er ledende innenfor fremvoksende teknologier, forventes å være utsatte etterretningsmål. I tillegg er forskningsfelt ved norske universiteter og høyskoler knyttet til fremvoksende teknologier attraktive mål. Kina er en særlig relevant trusselaktør innenfor dette temaet.» (PST: Nasjonal trusselvurdering 2023)

Informasjonssikkerhetsløft

I 2022 har vi videreført det vi tidligere har kalt et informasjonssikkerhetsløft. Målsetningen har vært å redusere angrepsflaten, rydde vekk sårbare systemer og gi UiO et teknisk forsprang som gjør at vi kan møte eventuelle uforutsette hendelser på en god måte.

I 2022 har hovedaktiviteten i dette arbeidet vært innføring av tofaktorautentisering. Med UiOs brukermasse er det nærmest en umulig oppgave å hindre at ikke noen brukernavn og passord er på avveie, og vi har i de senere årene sett at misbruket av kontoer på avveie har fått en alvorligere karakter. Tidligere var det i hovedsak brukt til å sende ut spam og uønsket e-post, men de senere årene har det vært økende antall forsøk på alvorligere innbrudd. Det viktigste tiltaket mot slik misbruk er innføring av tofaktorautentisering.

Ved utgangen av 2022 var det innført tofaktorautentisering på alle interaktive tjenester der brukere kan logge seg på og kjøre programmer på UiO. Dette har drastisk tatt ned risikoen for at kontoer på avveie skal lede til en større hendelse. Ved inngangen av 2023 gjensto noen e-post tjenester samt noen webtjenester – dette skyldes tekniske utfordringer som nå er løst. 2023 vil bli brukt til å rydde opp – med målsetning om at alle tjenester ved UiO skal kreve tofaktorautentisering ved pålogging utenfra.

Innføring av tofaktorautentisering på en institusjon som UiO er et stort prosjekt, og det griper inn i arbeids- og studiehverdagen til alle. Totalt har over 35000 brukere tatt dette i bruk, og det har totalt i organisasjonen blitt brukt flere tusen timer på innføringen. Dette har generert et stort trykk på IT-helpdesk, men de har gjort en fantastisk jobb og klart å håndtere dette på toppen av alle andre henvendelser. Prosjektet har i stor grad også vært ett oppryddingsprosjekt, da innføringen har avdekket et utall av forskjellige tekniske oppsett som nå i større grad har blitt standardisert og samkjørt.

UiO-CERT har allerede sett en stor effekt av innføringen, og har ikke hatt noen kontoer misbrukt på tjenester med tofaktorautentisering.

I 2021 var det fokus på å få ned antallet eksponerte tjenester på nett, dette arbeidet har blitt videreført i 2022. I 2022 har kontinuerlige søk etter sårbare tjenester blitt satt i system. Sikt utfører nå jevnlige søk utenifra for å avdekke sårbare og eksponerte tjenester, og UiO-CERT utfører kontinuerlige søk på innsiden etter det samme. Dette har bidratt til at selv en inntrenger som kommer på innsiden vil ha vanskeligheter med å kunne utnytte systemene videre.

Andre pågående aktiviteter som vil bidra til bedre sikring

I fjorårets rapportering ble det redegjort for en ny backup-tjeneste som skal ha en sikkerhetskopi av alle data på en egen fysisk lokasjon. Denne tjenesten er nå på plass, men på grunn av enorme datamengder så er ikke all data på plass ennå. Dette vil komme på plass i løpet av våren.

UiO har hatt stor effekt av å ha gode aktivitetslogger og god deteksjon i IT-systemene. I 2023 er det startet en jobb med å fornye og forbedre disse løsningene. Vi vil i dette

arbeidet også samarbeide tettere med flere av de andre i sektoren, som UiB, NTNU og UiT, for å dele erfaringer og tekniske løsninger.

I løpet av høsten 2022 har vi klart å få på plass et samarbeid med informasjonssikkerhetsmiljøet ved IFI, slik at de kan få tilgang til anonymiserte og avidentifiserte loggdata til bruk i masteroppgaver og annen forskning, og IT-avdelingen kan få bidrag til bedre sikring og analyser.

MS365 er en stor plattform som etterhvert har blitt en sentral i UiOs IT-tjenester. Den er sentral for alle som bruker Windows-plattformen, den vil bli sentral i nytt UH-SAK, og den brukes allerede i stor grad for samskriving og samhandling i Teams. For å kunne gjøre dette kontrollert og ha oversikt er det etablert et forvaltningsregime for Microsofts skytjenester ved UiO.

Digitalisering og kompleksitet

Mer automatisering og mer komplekse IT-løsninger kommer alltid med sikkerhetsutfordringer. Dette skyldes både at våre IT-systemer blir sårbare mot flere typer angrep, og at drift og vedlikehold blir mer komplisert, slik at det er lettere å gjøre feil som kan få konsekvenser for sikkerheten.

Grunnmuren i god IT-sikkerhet er gode driftsrutiner. Økt fokus på personvern og informasjonssikkerhet for å holde tritt med et økende trusselbilde bidrar til at arbeid med IT-sikkerhet og IT-jus stadig krever mer kapasitet. I tråd med den digitale utviklingen blir også IT-sikkerhet og personvernspørsmål noe som må tas stilling til i flere og flere aktiviteter ved universitetet. For å ivareta dette kan ikke fokus på personvern og IT-sikkerhetsrelaterte utfordringer avgrenses til noen utvalgte roller i IT-avdelingen – UiO er avhengig av nok fokus på sikkerhet i driftsorganisasjonen og på enhetene. Personvernombudsrollen er viktig for UiO og vi ser også at alle personvernkontaktene ved de ulike enhetene utgjør et sentralt bidrag i dette arbeidet.

I perioden har USIT jobbet mye med informasjonssikkerhet og jus knyttet til innføringen av nytt saks- og arkivsystem for UH-sektoren, UH-SAK, og UiO er en sterk bidragsyter inn i de større sektoraktivitetene. Vi ser fremdeles at en stadig utvidet bruk av digitale tjenester og fellestjenester i sektoren innebærer at avtaler blir fremforhandlet sentralt og det kan være vanskeligere for de ulike institusjonene å ivareta sitt selvstendige ansvar ved behandling av personopplysninger. Når UiO tar i bruk et nytt saksbehandlingssystem, er det UiO sitt ansvar å etterleve alle kravene i personvernregelverket (GDPR) – også når det er en fellestjeneste der valg knyttet til leverandør og informasjonssikkerhet ikke nødvendigvis er tatt på institusjonsnivå. Det er grunn til å tro at kompleksiteten i slike fellestjenester og de ulike hensynene som må vektes ved en slik anskaffelse gjør oss mer utsatt for brudd på informasjonssikkerheten.

Fra 1. januar i år ble IT-avdelingen organisert i en ny, felles IT-organisasjon. Nå som flere IT-funksjoner ved UiO er samlet i en organisasjon, kan dette bidra til økt kontroll på informasjonssikkerheten, større grad av standardisering og profesjonalisering av IT-sikkerhetsarbeidet.

Hendelseshåndtering og uønskede hendelser

UiO sin gruppe for håndtering av IT-sikkerhetshendelser, UiO-CERT, jobber kontinuerlig med håndtering av hendelser ved UiO. Selv om 2022 var et spesielt år, så har det totalt sett vært en svak nedgang i saker.

UiO-CERT har det siste året mottatt i overkant av 3000 innkommende saker. Det er et stabilt nivå, med en svak nedgang fra året før. I forbindelse med krigen i Ukraina var det tidlig i 2022 ventet en økning i antall hendelser, men vi ser det samme som mange andre – at det på noen områder ble en nedgang.

Det er håndtert i overkant av 110 saker med brukerkontoer på avveie, dette er en økning fra året før. I 2022 har disse sakene vært mer alvorlige og krevende enn tidligere år. Vi har sett at de i større grad har kommet i byger med flere saker samtidig, og vi har hatt flere tilfeller der kontoene har vært forsøkt brukt til å bryte seg videre inn i systemene. Som nevnt tidligere ble multifaktor-autentisering rullet ut på alle tjenester ved UiO i 2022. Etter dette har antallet og alvorligheten av kontoer på avveie stupt.

Antall innmeldte brudd på reglene knyttet til håndtering av personopplysninger har gått ned sammenlignet med forrige gjennomgang. I 2022 var det 22 innmeldte avvik, mot 40 innmeldte avvik i 2021. Noe av nedgangen skyldes at en kjent utfordring med integrasjonen mellom Tjenester for sensitive data (TSD) og Nettskjema har blitt fikset, men vi har også grunn til å tro at det er mørketall og at flere brudd og avvik burde vært meldt inn til UiO-CERT i tråd med avviksrutinene. Igjen viser dette at opplæring av ansatte er et nødvendig og kontinuerlig arbeid.

Antall utgående saker har økt noe. Det er fortsatt en overvekt av saker der interne og eksterne søk finner sårbare IT-systemer som må rettes eller ryddes vekk. Økningen skyldes mer systematisk arbeid med aktive søk etter gamle og sårbare IT-systemer.

Siden forrige gjennomgang har UiO meldt tre brudd på personopplysningssikkerheten til Datatilsynet, i hovedsak knyttet til feil tilgangsstyring. Et av de meldte bruddene gjaldt utilsiktet publisering av personopplysninger til *Scholars at risk*-forskere på internett. Dette fikk noe oppmerksomhet i media, men ingen av de meldte bruddene har medført videre oppfølging fra tilsynsmyndighetene.

Ledelsessystem for informasjonssikkerhet (LSIS)

Ledelsessystem for informasjonssikkerhet (LSIS) skal gjennomgås og oppdateres årlig. I løpet av det siste året har det blitt gjort mindre endringer i ledelsessystemet.

Referanser til relevant lovverk har blitt oppdatert. Kapitlet om brukerkontoer har blitt endret for å reflektere bruk av multifaktor-autentisering. Kapitlet om beredskap har blitt gjennomgått for å sjekke at det er korrekt. Det er også gjort mindre endringer i andre kapitler for å reflektere endringer i organisasjon og prosesser. Vi vil trekke frem at LSIS kapittel 6 er oppdatert med en formulering som tillater at loggdata kan gjøres tilgjengelig for forskningsformål, gitt at visse kriterier er oppfylt.

Vi anser LSIS ved UiO som godt innarbeidet i rutiner og prosesser ved universitetet og ser også at enkelte deler av det har blitt innlemmet i ledelsessystemet i andre organisasjoner. Klassifiseringen av data og begrepet «lagringsguide» har spredt seg i hele sektoren.

Internkontroll

Dette punktet omfatter flere aktiviteter gjennom året. De formelle aktivitetene er stedlige kontroller på IT-sikkerhet og personvern, og internkontrollundersøkelsen i januar med oppfølging i form av brevkontroller hvor enkelte avdelinger får dybdespørsmål som skal svares ut skriftlig.

De mer løpende aktivitetene er en del av det daglige arbeidet i CERT og IT-sikkerhetsgruppen, og inkluderer blant annet sårbarhetsskanning, tekniske stikkprøver og tilhørende opprydningsarbeid.

Siden 2018 har vi gjennomført internkontroll av behandling av personopplysninger ved UiO ved at ledere ved hver grunnenhet har svart på et nettskjema knyttet til kjennskap og etterlevelse av regelverket. Resultatene av årets internkontrollundersøkelse viser at lederne jevnt over opplever at sin enhet har relativt god kontroll på behandlingen av personopplysninger. Resultatene fra de mer detaljerte spørsmålene viser imidlertid at det innenfor visse områder fortsatt er begrenset kjennskap til en del av UiOs rutiner og gjeldende lovkrav. Undersøkelsen avdekker videre ønsker om, og behov for, kontinuerlig opplæring, bevisstgjøring, informasjonsflyt og tydeligere kommunikasjon rundt personvern og informasjonssikkerhet.

De tidligere nevnte systemene for kontinuerlig søk etter sårbare IT-systemer gjør at vi internt kan avdekke sårbare IT-systemer før en angriper gjør det. Den store graden av automatisering gjør også at vi kan håndtere sjekk av mange systemer med få manuelle operasjoner. Vi anser disse løsningene som en kontinuerlig teknisk kontroll som suppleres med manuelle tester og kontroller.

Sent 2022 ble også UiO bedt av Riksrevisjonen om å besvare en del spørsmål som del av deres forvaltningsrevisjon innenfor informasjonssikkerhet i forskning i kunnskapssektoren. Riksrevisjonen undersøker tilstanden hos 10 utdanningsinstitusjoner, deriblant UiO. I tillegg til spørsmålene som ble besvart skriftlig, foretok de to dybdeintervjuer hos IT-avdelingen knyttet til teknisk sikring og organisatoriske tiltak. Resultatet vil foreligge sent 2023. Vår oppfatning er at det ikke er gjort vesentlige funn hos UiO, men noen funn og forslag til forbedringer er allerede under oppfølging.

Direktoratet for høyere utdanning og kompetanse gjennomførte sitt årlige kartleggingsmøte den 4. januar 2023. I deres tilbakemelding sier de blant annet «Vi legger merke til at UiO i 2022 har videreført arbeidet med etterlevelse av Kunnskapsdepartementets policy for informasjonssikkerhet og personvern. Vår vurdering er derfor at UiO overholder hovedkravene i policyen på en tilfredsstillende måte også i 2022.». Tilbakemeldingen i sin helhet ligger vedlagt.

Personvern

Fokuset på personvern har økt kraftig de siste årene, både i det offentlige ordskiftet, blant forskningsdeltagere, studenter og ansatte. Oppmerksomheten er høy også hos samarbeidsparter og dataeiere – og det er stor etterspørsel etter opplæring og bistand på personvernområdet ved UiO. Personvernspørsmål får betydning for alle deler av UiOs virksomhet; fra hvilke IT-tjenester universitetet kan benytte, hvilke sosiale medier universitetet skal være tilstede på, til deling av forskningsdata eller internasjonal studentutveksling.

Siden 2020 har UiO tilbudt et e-læringskurs i personvern for studenter og vitenskapelig ansatte. Det siste året har Det medisinske fakultetet i samarbeid med UiO sentralt utviklet en helsefaglig variant av kurset som vil bli obligatorisk for forskere ved deres enhet. Det samfunnsvitenskapelige fakultet har også gjort personvernkurset obligatorisk på sin enhet og vil tilby en helsefaglig modul av kurset. Det siste året er et mindre e-læringskurs for administrativt ansatte lansert, som foreløpig et frivillig tilbud for ansatte. Juristene i IT-avdelingen bruker mye ressurser på opplæring og å svare på henvendelser fra forskere, administrativt ansatte og studenter om personvern. I tillegg bidrar personvernkontaktene ved alle UiOs enheter å være en førstelinje for personvernsspørsmål og bevisstgjøring ved sin enhet.

Vi ser fremdeles at internasjonale forskningssamarbeid møter personvernsutfordringer da det er juridisk vanskelig å dele data utenfor EU/EØS, særlig til USA. I tillegg kan andre land og institusjoner være underlagt andre lovkrav og føringer som kan komplisere deling av forskningsdata. I slike samarbeid er det både etterspørsel etter bistand samt behov for mer utfyllende og klargjørende regulering i nasjonal lovgivning. Dette er også noe UiO har spilt inn i høringen etter Personvernkommisjonens rapport som kom høsten 2022.

Å sikre trygg og lovlig deling av forskningsdata på tvers av landegrenser viser fremdeles verdien av at IT-avdelingen tilbyr en rekke lokale IT-tjenester der UiO selv legger premissene for sikringstiltak, lagring og brukervilkår. Samtidig tar UiO også i bruk en rekke eksterne tjenester der det må gjøres komplekse og tidkrevende vurderinger knyttet til sikkerhet og lovlighet. Vurderinger som også kan være sårbare når rettstilstanden skifter; nye dommer fra EU-domstolen, nye vedtak eller retningslinjer fra tilsynsmyndighetene eller det skjer regelendringer. Vi ser for eksempel at forskere ikke alltid kan ta i bruk den IT-tjenesten de ønsker fordi tjenestene ikke møter nødvendige krav til personvern, lagring eller overføringer ut av EU. Slike avveininger problematiserer også hva som er akseptabel risiko for universitetet sett i lys av UiOs mål og strategi.

Personverntjenester i Sikt (tidligere NSD), som vurderer personvernet i forskningsprosjekter for UiO, tilbyr nå automatiske vurderinger for prosjekter med lav personvernrisiko. Dette innebærer at en rekke prosjekter får svar på dagen og ikke må vente på lengre saksbehandling. Samtidig medfører en automatisk vurdering at mer krevende problemstillinger som tidligere ble fanget opp av en saksbehandler kanskje nå ikke blir vurdert. Igjen ser vi en avveining mellom akseptabel risiko for universitetet sett i lys av effektivitetshensyn og UiOs mål.

Videre arbeid

Teknisk grunnmur

UiO har hatt en lang tradisjon for god og sikker drift av IT-systemer. Vi var tidlig ute med automasjon og overvåking. Etablering av UiO-CERT i 2005/2006 gjør også det til et av landets eldste responsteam og har gjort at håndtering av sikkerhetshendelser og avvik er godt innarbeidet i IT-organisasjonen.

Felles sikring og standard maskinoppsett har en enda lengre tradisjon ved UiO, og er – slik den fremstår nå – godt samkjørt med NSM sine grunnprinsipper og andre dokumenter som angir «beste praksis». Dette, sammen med løftet som er tatt siste år, gjør at UiO nå har en god og sikker IT-teknisk grunnmur vi kan bygge sikre tjenester på. Suksessen som for eksempel TSD og Nettskjema har hatt både i sektoren og nasjonalt viser dette.

Videre arbeid med teknisk sikring vil i stor grad fokusere på å holde eksisterende grunnmur vedlike, samt kontinuerlig fornying og forbedring.

Å etablere tilsvarende god og sikker forvaltning av de store sky- og tjenesteplattformene vil være noe vi vil måtte bruke tid på fremover. Samt å gjøre eksisterende løsninger mer robuste.

Opplæring og sikkerhetskultur

En oppnår ikke god informasjonssikkerhet kun med tekniske løsninger, vi ser derfor at det neste store løftet må flyttes til opplæring og informasjon.

Både gjennom internkontrollen og tilbakemeldinger fra ansatte ser vi at det stadig er et stort behov for opplæring innen informasjonssikkerhet og personvern. Dette arbeidet er noe av det viktigste vi gjør for å ivareta et godt personvern, og vi ser at det er viktig at vi avsetter nok ressurser til dette arbeidet.

I løpet av 2023 skal vi oppdatere vår tilnærming til opplæring og sikkerhetskultur på UiO. Vi ser i svarene fra årets internkontroll at flere ønsker opplæring og kurs innen både informasjonssikkerhet og personvern, og har valgt ut fire tiltak som vi mener vil gi best resultater for sikkerhetskulturen ved UiO:

1. Enklere og mer brukerrettede nettsider, delt inn i en side for akutte hendelser og en side for opplæring og bevisstgjøring.

2. Et tydelig beskrevet kurstilbud.

3. Jevnlige påminnelser om aktuelle temaer og gode vaner i noen prioriterte kanaler.

4. Invitere oss inn på vanlige møteserier hos fagnettverk, fakulteter, institutter og forskningsgrupper for å formidle.

Forbedring av deteksjonsevne

UiO ligger allerede langt fremme i deteksjonsevne for å oppdage og hindre hendelser. Riksrevisjonen kommenterte også dette i sin tekniske gjennomgang. Vi har målsetning om å videreutvikle disse evnene til bli like gode i sektorplattformer og i de skytjenester vi tar i bruk.

Samarbeid i sektoren

Vi skal videreutvikle samarbeidet i BOTT digital sikkerhet, som har gitt et større nettverk for fagsamarbeid.

Vedlegg:

Vedlagt følger:

- Regneark med status informasjonssikkerhet
- Regneark med status personvern
- «Arbeidet med informasjonssikkerhet og personvern hos Universitetet i Oslo», brev fra HK-dir av 20.04.2023

Krav	Tilstand 2019	Tilstand 2020	Tilstand 2021	Tilstand 2022	Tilstand 2023	Status på eksisterende tiltak	Behov for tiltak
Gjennomført/revidert ROS-analyse i 2017/2018							
ROS-analyser av administrative systemer og av infrastruktur-komponenter	God	God	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 som tjenesteleverandør	Tilfredstillende	Tilfredstillende	Tilfredstillende	God	God	Det er utført en egen ROS av USIT som driftsleverandør.	Ros analyser av USITs systemer skal gjennomgåes i 2023
ROS-analyser av systemer i forskning og utdanning	Ikke tilfredstillende	Tilfredstillende	Tilfredstillende	Tilfredstillende	Tilfredstillende	Et nettskjema for egenrapportering av mindre skytjenester til bruk i forskning og utdanning bidrar til at flere systemer blir registrert og får gjennomført en nødvendig vurdering av personvern og informasjonssikkerhet. 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	Tilstand 2022	Tilstand 2023	Status på eksisterende tiltak	Behov for tiltak
Gjennomført og evaluert en kriseøvelse							
Generell kriseøvelse	God	God	Tilfredstillende	Tilfredstillende	Tilfredstillende		
Spesifikk øvelse på informasjonssikkerhet	Tilfredstillende	God	God	God	Tilfredstillende	Gjenomført tabletop-øvelse 2022, samt kontinuerlig arbeid. UIO-CERT behandler 3000+ saker i året.	Øvelse skal gjennomføres høsten 2023
Evaluering av kriseøvelse	Tilfredstillende	God	Tilfredstillende	Tilfredstillende	Tilfredstillende		

Krav	Tilstand 2019	Tilstand 2020	Tilstand 2021	Tilstand 2022	Tilstand 2023	Status på eksisterende tiltak	Behov for tiltak
Ledelsessystem for informasjonssikkerhet - LSIS							
Ledelsessystem for informasjonssikkerhet gjort kjent i organisasjonen	God	God	God	Tilfredstillende	Tilfredstillende	Det planlegges ytterligere informasjonskampanjer om LSIS. Vi har avdekket et behov for dette.	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	Tilfredstillende	Tilfredstillende	Som en del av internkontrollen er det gjennomført en kartlegging av kjennskap til, og etterlevelse av gjeldene regelverk for informasjonssikkerhet og personvern	Kartleggingen viser behov for fortsatt og kontinuerlig opplæring.

Krav	Tilstand 2019	Tilstand 2020	Tilstand 2021	Tilstand 2022	Tilstand 2023	Status på eksisterende tiltak	Behov for tiltak
Ledelsessystem for informasjonssikkerhet - LSIS							
Oppfølging av funn i kartleggingen	Tilfredstillende	Tilfredstillende	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	God	God	Gjennomført som årlig rapportering til Universitetsstyret	
Grunnsikring - KD oppfordrer institusjonene til å løfte informasjonssikkerheten høyere enn de nasjonale minstekravene.	God	God	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. Tofaktor-autentisering var et stort løft i 2022.	Tiltakene vil kontinuerlig utvikles, vedlikeholdes og tilpasses trusselbildet utover året. Ny funksjonalitet for f. eks. deteksjon legges til ved behov.
Internkontroll på informasjonssikkerhetsområdet	God	God	God	God	God	Gjennomført årlig hver vår sammen med internkontroll for bruk av personopplysninger	

Krav	Tilstand 2019	Tilstand 2020	Tilstand 2021	Tilstand 2022	Tilstand 2023	Status på eksisterende tiltak	Behov for tiltak
Hendelseshåndtering							
Har institusjonen innført rutine for å håndtere uønskede digital hendelser?	God	God	God	God	God	UiO-CERT er UiOs operative hendelsesteam. De har eksistert siden 2005, og har gode og dokumenterte rutiner - med godt nasjonalt og internasjonalt nettverk.	
IT-beredskap og kontinuitetsplan	Tilfredstillende	Tilfredstillende	Tilfredstillende	Tilfredstillende	Tilfredstillende	IT-beredskapsplan er innført, trent og øvd. Det er fortsatt mangler ved kontinuitetsplanene.	Det må innføres kontinuitetsplaner for viktige prosesser. Dette må følges opp også utenfor USIT.
Krav	**Tilstand 2019**	**Tilstand 2020**	**Tilstand 2021**	**Tilstand 2022**	**Tilstand 2023**	**Status på eksisterende tiltak**	**Behov for tiltak**
Eksportkontroll							
Har institusjonen oversikt over kunnskapsområder som reguleres av eksportkontroll-lovgivningen?		Ikke tilfredstillende	Ikke tilfredstillende	Ikke tilfredstillende	Tilfredstillende	Internkontrollen 2019, 2020, 2021 og 2022 viser at enhetene ikke har god nok oversikt over eksportkontroll-regelverket	UiO har satt igang en rekke aktiviteter for å få dette under bedre kontroll. Arbeidsgruppe om ansvarlig internasjonalt samarbeid, verdikartlegging og tiltak etter sentrale ROS analyser.
Etterlever institusjonen eksportkontroll-lovgivningen?		Ikke tilfredstillende	Ikke tilfredstillende	Ikke tilfredstillende	Tilfredstillende	Interkontrollen 2019, 2020, 2021 og 2022 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	Tilstand 2022	Tilstand 2023	Status på eksisterende tiltak	Behov for tiltak
Krav om oversikt over all behandling av personopplysninger i forskning							
Medisinsk og helsefaglig forskning	Tilfredstillende	God	God	God	God	Forskpro er i bruk ved alle fakulteter med unntak av Det juridiske fakultet.	
Forskning på øvrige personopplysninger	God	God	God	God	God	Sikt sitt meldingsarkiv gir en oversikt over UiOs forskning på personopplysninger. Alt som skal til Sikt meldes i stor grad til Sikt.	

Krav	Tilstand 2019	Tilstand 2020	Tilstand 2021	Tilstand 2022	Tilstand 2023	Status på eksisterende tiltak	Behov for tiltak
Krav om oversikt over all behandling av personopplysninger							
Register over administrative behandlinger	Tilfredstillende	Tilfredstillende	Tilfredsstillende	Tilfredsstillende	Tilfredstillende	Det er fremdeles mangelfulle registreringer i vår oversikt over behandlinger, den såkalte "meldeapppen".	Det kreves større bevissthet og bedre kontroll fra ledelsen på enhetene om lovlig bruk av systemer og hvilke behandlinger som skal registreres i meldeappen. IT-juristene vil fortsette opplæring i bruk av meldeappen.
Oversikt over systemer brukt i forskning og utdanning	Ikke tilfredstillende	Tilfredstillende	Tilfredsstillende	Tilfredsstillende	Tilfredstillende	Nettskjemaet for egenrapportering av mindre skytjenester til bruk i forskning og utdanning bidrar 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	Tilstand 2022	Tilstand 2023	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	God	God	Sikt vurderer alle forskningsporsjekter som behandler personopplysninger, og de bistår forskere med personvernkonsekvensvurdering (DPIA) når dette er nødvendig.	
Forskning på øvrige personopplysninger	God	God	God	God	God	Sikt vurderer alle forskningsporsjekter som behandler personopplysninger, og de bistår forskere med personvernkonsekvensvurdering (DPIA) når dette er nødvendig.	

Krav	Tilstand 2019	Tilstand 2020	Tilstand 2021	Tilstand 2022	Tilstand 2023	Status på eksisterende tiltak	Behov for tiltak
Krav om internkontroll							
Generelle veiledere	God	God	God	God	Tilfredstillende	UiO har en rekke oppdaterte generelle rutiner og veiledere for behandling av personopplysninger i forskning og i administrasjonen, men etter tilbakemeldinger i internkontrollen ser vi at det er behov for forenkling og tydeliggjøring i en del rutiner.	Eksisterende rutiner for behandling av personopplysninger i forskning og administrasjon skal gjennomgås og forenkles der det er mulig.
Internkontroll/Kvalitetssystem for forskning på personopplysninger	Tilfredstillende	Tilfredstillende	Tilfredsstillende	Tilfredsstillende	Tilfredstillende	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.	
Dedikerte personer på enhetsnivå med ansvar for personvern	God	God	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	Tilfredstillende	Tilfredstillende	Utøver av behandleransvaret holder jevnlig kurs/presentasjoner for studenter og ansatte på alle enheter. E-læringskurs innen personverner utviklet og tatt i bruk hos samtlige relevante enheter. Personvernkontakter kurses slik at de kan besvare spørsmål fra egen enhet. Likevel kontinuerlig et stort behov for opplæring og kursing.	Nettsider som presenterer kurs og opplæring som tilbys skal syneliggjøres og videreutvikles.
Internkontrollsystem	God	God	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	Tilstand 2022	Tilstand 2023	Status på eksisterende tiltak	Behov for tiltak
Krav om et overordnet personvernombud	God	God	Tilfredstillende	Tilfredstillende	Tilfredstillende	Konstituert personvernombud er ansatt i 50% stilling. Stillingsinstruks er vedtatt av Universitetsstyret.	Med et stadig økende fokus på personvern bør det evalueres om personvernombudet fortsatt skal ha en 50% stilling, eller om denne bør utvides.

Direktoratet for høyere utdanning og kompetanse

UNIVERSITETET I OSLO
Postboks 1072 Blindern
0316 OSLO

Vår ref:	*Deres ref:*	*Dato:*
22/06778-14		*20.04.2023*

Arbeidet med informasjonssikkerhet og personvern hos Universitetet i Oslo (UiO)

Bakgrunn

Vi viser til kartleggingsmøtet om arbeidet med informasjonssikkerhet og personvern 4. januar 2023. Møtet ble gjennomført som del av Kunnskapsdepartementets styringsmodell for informasjonssikkerhet og personvern i høyere utdanning og forskning.

Med bakgrunn i kartleggingsmøtet, ønsker HK-dir å gi enkelte kommentarer til informasjonssikkerhets- og personvernarbeidet hos dere. Vi har også noen anbefalinger for hvordan dette arbeidet kan styrkes og forbedres.

Våre kommentarer og anbefalinger gis med utgangspunkt i «Policy for informasjonssikkerhet og personvern i høyere utdanning og forskning». Policyen er fastsatt av Kunnskapsdepartementet i rundskriv F-04-20.

Vi oppfordrer dere til å vektlegge våre anbefalinger i det videre arbeidet med overholdelse av policyen.

Arbeidet i 2022

Vi legger merke til at UiO i 2022 har videreført arbeidet med etterlevelse av Kunnskapsdepartementets policy for informasjonssikkerhet og personvern. Vår vurdering er derfor at UiO overholder hovedkravene i policyen på en tilfredsstillende måte også i 2022.

POSTADRESSE
Postboks 1093
5809 Bergen
post@hkdir.no

HOVEDKONTOR
Fortunen 1
HJEMMESIDE
www.hkdir.no

TELEFON
+47 55 30 38 00
ORG.NO
974 788 985

SAKSBEHANDLER
Mathias Gullbrekken Sandnes

Som bemerket i tidligere anbefalingsbrev, innebærer dette at (i) ledelsessystemet for informasjonssikkerhet og internkontrollen for GDPR inngår i den generelle virksomhetsstyringen ved UiO og (ii) arbeidet med informasjonssikkerhet og personvern hos grunnenhetene følges opp på en systematisk måte. Samtidig er aktiviteten i UiO sitt nettverk av personvernkontakter ved grunnenhetene opprettholdt og forbedret i 2022.

Selv om UiO ikke har økt ressursinnsatsen (årsverk) i løpet av fjoråret, har UiO likevel styrket organiseringen av arbeidet med IT-sikkerhet og personvern. Eksempler på dette er opprettelse av rollen som IT-sikkerhetskoordinator i seksjonene ved IT-avdelingen og at arbeidet med IT-sikkerhet og IT-rett, inkludert GDPR, er lagt til samme seksjon i avdelingen. Vi deler UiO sin oppfatning om at disse endringene vil bidra til å forbedre innsatsen innen disse forvaltningsområdene.

Videre merker vi oss at UiO har etablert en strukturert risikostyringsprosess på informasjonssikkerhetsområdet. Det betyr at det gjennomføres risikovurderinger av sikkerheten i informasjonsbehandlingen både på virksomhets-, avdelings- og systemnivå.

UiO har også i 2022 gjennomført målrettet kompetanseheving, spesielt e-læringstiltak innen personvern tilpasset behovene til det enkelte fakultet og intern foredragsvirksomhet. Personvernombud deltatt på ledermøter ved fakultetene for å informere om og styrke bevisstheten om personvern og krav til behandling av personopplysninger.

UiO har fullstendige rutiner for ivaretakelse av de registrertes rettigheter og en komplett behandlingsprotokoll for systemer og tjenester hvor UiO er behandlingsansvarlig. I tillegg virker bevisstheten i organisasjonen om de krav som stilles til klassifisering og lagring av informasjon å være høy.

Ut over dette har UiO iverksatt flere viktige informasjonssikkerhets- og personverntiltak i 2022. Eksempler på slike tiltak er innføring av totrinnsinnlogging for studenter og ansatte på UiO sine IT-tjenester, styrking av endepunktsikkerheten ved bruk av nye sikkerhetstjenester fra Microsoft (A5-lisens), synkronisering av back-up-data til ny datalokasjon og utarbeidelse av ny rutine for godkjenning av skytjenester.

Vi ønsker også å bemerke at UiO følger opp og løpende lukker sårbarheter som avdekkes i tekniske sikkerhetstester (sårbarhetsskann). Videre at antallet datamaskiner (servere) som er eksponert mot internettet er redusert, eldre IT-systemer blir dekommisjonert og UiO har oversikt over sikkerhetsstatusen til alle dataenheter tilkoblet institusjonens fastnett.

Anbefalinger til UiO

Vår hovedanbefaling er at UiO opprettholder og kontinuerlig forbedrer dagens arbeid med informasjonssikkerhet og personvern. Som tidligere, innebærer dette at UiO tilpasser egen innsats til endringer i det generelle trusselbildet, og sørger for at innsatsen videreutvikles i takt med de sikkerhets- og personvernutfordringer som sektoren står overfor og som digitaliseringen av kjerneaktivitetene kan innebære.

Vi anbefaler også at UiO fortsetter å vektlegge opplærings- og kompetansehevende tiltak rettet mot ansatte og studenter, for eksempel knyttet til riktig lagring av personopplysninger ved bruk av privat IT-utstyr.

UiO bør i tillegg vurderer om og på hvilke måter opplærings- og kompetansebehov hos ledere og medarbeidere som ivaretar sentrale roller i det daglige arbeidet med informasjonssikkerhet og personvern kan imøtekommes. Slik vi ser det, vil dette være viktig for ytterligere å styrke arbeidet i hele organisasjonen, og for at UiO fortsatt skal kunne overholde hovedkravene i departementets policy for informasjonssikkerhet og personvern.

Videre anbefaler vi at UiO

- sørger for at det utarbeides en tilfredsstillende behandlingsprotokoll for IT-tjenester hvor UiO er databehandler,

- informasjon om og opplæring i ledelsessystemet for informasjonssikkerhet inngår i opplæringen av nyansatte (onboardingsprosessen),

- iverksetter tiltak for å styrke tjenesteeiernes bevissthet og kompetanse om informasjonssikkerhet og oppgavene i ledelsessystemet,

- håndterer risiko med bakgrunn i gjennomførte risikovurderinger, blant annet når det gjelder eksportkontroll og komplekse verdikjeder,

- iverksetter hensiktsmessige tiltak for å redusere personvernrisiko i tilknytning til identifiserte sårbarheter i tilgangsstyringen,

- viderefører arbeidet med planverk for håndtering av alvorlige informasjonssikkerhets- eller personvernhendelser og for opprettholdelse av viktige funksjoner ved slike hendelser, herunder kartlegging av avhengigheter mellom IT-systemer/-tjenester (IT-beredskap og -kontinuitet).

Avslutningsvis anbefaler vi at UiO gjennomfører den planlagte øvelsen på håndtering av alvorlige informasjonssikkerhetsbrudd.

Vi ønsker dere lykke til med det videre arbeidet!

Med vennlig hilsen
Kristin Selvaag
avdelingsleder / Head of Department

Mathias Gullbrekken
Sandnes
rådgiver / Adviser

Dokumentet er elektronisk signert og har derfor ikke håndskrevne signaturer.

Mottaker:
UNIVERSITETET I OSLO

Kopimottaker:
KUNNSKAPSDEPARTEMENTET