UNIVERSITETET I BERGEN

Styre: Universitetsstyret **Dato:** 16.08.2019
Styresak: 67/19 **Arkivsaksnr:** 2019/1847
Møtedato: 29.08.2019

Internrevisjonsrapport - Lokalt driftede IT-systemer

Henvisning til bakgrunnsdokumenter

- Styresak 120/18 Årsplan for internrevisjon 2019
- Styresak 53/19 Styringssystem for informasjonssikkerhet og personvern

Saken gjelder:
I henhold til Årsplan for internrevisjon 2019 har PwC gjennomført revisjon av lokalt driftede IT-systemer. I denne saken legges revisjonsrapporten fram for universitetsstyret til orientering, sammen med en redegjørelse for hvordan rapporten blir fulgt opp.

Formålet med denne revisjonen har vært å gjennomgå og evaluere hvorvidt lokal drift av IT-løsninger på institutter er i tråd med UiBs rutiner og retningslinjer med fokus på organisering, driftsløsninger og sikkerhet. Revisjonen har gjennomgått driften ved tre av de instituttene som har lokalt utstyr og egne IT-ansatte.

Internrevisjonen vurderer risikoen til å være middels med behov for forbedringer. De lokale IT-ansvarlige synes å ha god kompetanse på de løsninger som driftes lokalt, er kjent med UiBs rutiner og retningslinjer knyttet til informasjonssikkerhet og har en god støtte fra og kommunikasjon med UiBs sentrale IT-avdeling. Like fullt påpeker rapporten et bredt spekter av totalt tretten forbedringsområder. Fire av disse har høy prioritet.

Det er beskrevet tiltak og oppfølging på alle områdene. På enkelte av forslagene fra rapporten vil det bli gjennomført en nærmere vurdering av kost-nytte og alternative tiltak for å dekke det underliggende behovet. Rapporten anbefaler også at man i større grad tar i bruk sentrale tjenester, og at mer IT-utstyr og løsninger driftes og forvaltes sentralt

Forslag til vedtak:

Universitetsstyret tar internrevisjonsrapporten «Lokalt driftede IT-systemer» og redegjørelsen om oppfølgingen av rapporten til orientering..
Kjell Bernstrøm
universitetsdirektør

16.08.2019/Tore Burheim (avd.dir)

Vedlegg:
1. Saksframstilling: Internrevisjonsrapport – Lokalt driftede IT-systemer
2. Internrevisjonsrapport: Lokalt driftede IT-systemer

Saksframstilling

Styre:	Styresak:	Møtedato:	Arkivsaksnr:
Universitetsstyret	67/19	29.08.2019	2019/1847

Internrevisjonsrapport - Lokalt driftede IT-systemer

Bakgrunn for internrevisjonsprosjektet

UiB sentraliserte sin IT-virksomhet i 2006 som det første av de store breddeuniversitetene i Norge. Dette var en vellykket omlegging. I årene etter har stadig mer blitt flyttet sentralt, men fortsatt driftes noe utstyr lokalt. Dette er i hovedsak utstyr knyttet til forskningsaktivitet.

Informasjonssikkerhet er et område med økende utfordringer og økende oppmerksomhet. Etter hvert som stadig mer av universitetets virksomhet er kritisk avhengig av digitale verktøy og digitaliserte data blir vi mer sårbare dersom informasjonssikkerheten ikke ivaretas. Det er derfor viktig å sikre tilgjengelighet, integritet og konfidensialitet av våre data og våre IT-systemer. Store deler av vår infrastruktur er knyttet til, avhengig av eller styres av IT-systemer. Sikring av universitetets verdier er i økende grad avhengig av sikker forvaltning og drift av våre IT-systemer. En gjennomgang høsten 2018 avdekket varierende kjennskap til rutiner, drift, systemeierskap og ansvar mv på instituttene ved UiB.

I og med at utfordringene knyttet til sikker forvaltning og drift av IT-systemer øker, var det grunnlag for internrevisjonen å se på lokal drift av IT-systemer ved UiB. Man valgte ut tre institutt ved tre ulike fakultet. Internrevisjonen ble gjennomført ved institutter som har egne ansatte med definert ansvar for de lokale IT-løsningene.

Hovedfunn i rapporten og oppfølging av disse

Internrevisjonen vurderer risikoen til å være middels med behov for forbedringer. De lokale IT-ansvarlige ved instituttene synes å ha god kompetanse på de løsninger som driftes lokalt, de er kjent med UiBs rutiner og retningslinjer knyttet til informasjonssikkerhet og de har god støtte fra og god kommunikasjon med UiBs sentrale IT-avdeling.

Like fullt peker rapporten på forbedringsområder. Det er totalt tretten ulike forbedringsområder der fire har høy prioritet. De fire med høy prioritet omfatter (a) oversikt over utstyr og systemer som driftes lokalt, (b) drift av lokalt utstyr (flytte til felles løsninger), (c) backup av lokalt driftede PCer, og (d) retningslinjer for bruk av skytjenester.

De øvrige punktene har medium prioritet. I det følgende er det gjort rede for oppfølging av alle punktene. De med høy prioritert er merket i gjennomgangen.

1. Kommunikasjon / roller og ansvar lokal IT-ansvarlig og sentral IT-avdeling

Rapporten påpeker at de lokale IT-ansvarlige stort sett er fornøyd med kommunikasjon, støtte og oppfølging fra UiBs sentrale IT-avdeling, samt rutiner og retningslinjer som er tilgjengelig på UiBs nettsider.

Samtidig påpeker rapporten behovet for bedre kommunikasjon, økt oppmerksomhet på endringer i driftsrutiner, nye løsninger mv, samt at det er en noe uklar rolle og ansvarsfordeling mellom lokalt ansatte og IT-avdelingen. Rapporten foreslår e-post som kanal for informasjon om oppdateringer, og at roller og ansvar bør tydeliggjøres.

UiB skal bytte systemløsning for «IT Service Management» i 2019-20. Dette inneholder en dokumentasjonsbase der man vurderer å samle all dokumentasjon, rutiner, mv. IT-avdelingen vil i dialog med de lokale IT-ansatte, se hvordan informasjonsbehovet kan løses på en praktisk og formålstjenlig måte. Tydeligere roller og ansvar er behandlet i punkt 7 under.

2. Sentral IT-avdeling mangler oversikt over systemer/utstyr som driftes lokalt (høy prioritet)

Det finnes ikke noen samlet oversikt over lokale IT-systemer og konfigurasjonen av disse, og det er varierende i hvor stor grad man har oversikt lokalt. Dette er viktig i forhold til blant annet sårbarhet og formelle krav til dokumentasjon (sikkerhet og personvern).

Internrevisjonen anbefaler at UiB utarbeider en mal for oversikt over IT-systemer/løsninger som driftes lokalt, og at denne fylles ut av hvert fakultet/institutt. Dette er data som normalt finnes i en såkalt konfigurasjonsdatabase. IT-avdelingen har dette for sine systemer. Det er naturlig å vurdere om det er formålstjenlig og realistisk å legge lokalt driftet utstyr inn i den sentrale konfigurasjonsdatabasen, alternativt lage en egen for lokalt driftet eget utstyr.

3. Drift av lokalt utstyr (høy prioritet)

Internrevisjonen anbefaler at alt kritisk lokalt utstyr kobles opp mot IT-avdelingens tjeneste Lab-IT og at øvrig utstyr (for eksempel lokale servere) kan benytte IT-avdelingens Infrastruktur som tjeneste (UH-IaaS).

Lab-IT har vært godt mottatt der det er tatt i bruk og ansees vellykket da det gir forskerne en vesentlig bedre arbeidssituasjon og vesentlig bedre sikkerhet. Det er arbeidskrevende å rulle dette ut, da oppsettet på hvert enkelt laboratorium må gjennomgås for å få en omlegging som sikrer kontinuitet og ivaretar det enkelte laboratorieutstyrs krav. Infrastruktur som tjeneste benytter skyteknologi og gir fleksibel og umiddelbar tilgang på servere. Lab-IT vil bli rullet videre ut og man vil vurdere behovet for en sterkere promotering og tilrettelegging av Infrastruktur som tjeneste.

4. Gammelt utstyr

Det forekommer en del gammelt IT-utstyr på ulike steder på UiB. Revisjonsrapporten anbefaler at UiB utarbeider en oversikt over lokale PCer med eldre versjoner av Windows operativsystem og vurderer risiko knyttet til dette. Rapporten foreslår ellers mer bruk av en tjeneste som Lab-IT for å håndtere gammelt og utdatert utstyr. Vi ser for oss at dette følges opp som en del av arbeidet på punkt 2 og 3 over og at det tas initiativ for å øke utskiftingstakten.

5. Backup av lokalt driftede PC-er (høy prioritet)

Internrevisjonen avdekker at det eksisterer manuelle rutiner for sikkerhetskopiering av programvare og teknisk oppsett, og fragmentert ansvar for sikkerhetskopiering av data. Dette kombinert med nøkkelmannsrisiko, og at en del av dette utstyret er gammelt, innebærer sårbarhet og behov for tiltak. Internrevisjonen anbefaler at UiB foretar en risikovurdering av lokalt driftet utstyr. I henhold til UiBs Styringssystem for informasjonssikkerhet og personvern er det systemeier (normalt instituttleder) som har ansvar for å gjøre risikovurderinger. IT-avdelingen arrangerer kurs i risiko og sårbarhetsanalyse (ROS-analyse) i september 2019 og vil gjennomføre flere kurs etter behov. I årets egenrapportering på informasjonssikkerhet vil det blir etterspurt mer utfyllende informasjon om gjennomførte risiko- og sårbarhetsanalyser.

Samtidig anbefaler internrevisjonen at systemer og data som ansees som kritiske eller sensitive kobles til Lab-IT og dermed inngår i UiBs backup-rutiner. (Se for øvrig punkt 3.)

6. Nøkkelmannsrisiko – sårbarhet

Rapporten påpeker at det er nøkkelmannsrisiko i de miljøene som har lokalt ansatte med ansvar for lokalt IT-utstyr. Med to unntak er det ikke mer enn en ansatt på instituttene. Internrevisjonen anbefaler at UiB vurderer å iverksette tiltak for å redusere

nøkkelmannsrisiko. Dette kan gjøres gjennom å spre IT-kompetanse blant flere ansatte på instituttene, men internrevisjonen sier at det kanskje viktigste tiltaket vil være å knytte flest mulig av de systemer, PC-er og annet utstyr som driftes lokalt opp mot sentral IT infrastruktur, som f.eks. Lab-IT, det vil si samme tiltak som punkt 3, samt gjennomføring av risiko og sårbarhetsanalyser.

7. UiB mangler instruks for lokale IT-ansvarlige

Internrevisjonen påpeker at UiB ikke har noen instruks for lokale IT-ansvarlige, og anbefaler at UiB utarbeider en slik som beskriver roller og ansvar for disse.

I utformingen av Gjennomførende del av UiBs Styringssystem for informasjonssikkerhet og personvern skal det utarbeides retningslinjer for drift av IT-systemer. Disse er under utarbeidelse i et samarbeid mellom IT-avdelingen og noen IT-ansvarlige lokalt. Vår vurdering er at dette vil dekke det underliggende behovet med en tydeliggjøring her.

8. Det er ikke utpekt systemeiere for systemer som driftes lokalt

I henhold til Styringssystem for informasjonssikkerhet og personvern skal alle systemer ved UiB ha en definert systemeier. Vedkommende har ansvar for at det gjennomføres risiko- og sårbarhetsanalyser, systemets sikkerhet, kontinuitetsplanlegging og fysisk sikkerhet. Internrevisjonen mener at man i varierende grad er dette eierskapet bevisst og anbefaler en med formell utpekning.

I henhold til Styringssystem for informasjonssikkerhet og personvern er øverste leder for enheten automatisk systemeier om det ikke er særskilt utpekt en systemeier. Det vil i denne sammenhengen være instituttleder eller tilsvarende for lokalt driftede systemer. Her kan det være formålstjenlig å dokumentere eierskapet i den tidligere nevnte systemoversikten (pkt 2). Vi er usikre på om det er behov for mer formell utpeking, men det er behov for en større grad av dokumentasjon, bevisstgjøring og informasjon om denne rollen. Dette tas inn i det generelle sikkerhetsarbeidet.

9. Mangler sentral brannmur mellom klienter og internett

Internrevisjonsrapporten anbefaler at UiB vurderer en sentral brannmur mellom UiBs interne nett og resten av verden. I løpet siste 12 måneder har mer enn 135 000 ulike enheter (datamaskiner, smarttelefoner, nettbrett, mv) vært koblet på UiBs nett. Alle disse vil være innenfor en slik brannmur som her anbefales. Det vil si at vi i alt vårt sikkerhetsarbeid må ta høyde for at vi har «fienden» på innsiden. UiB bygger sikkerheten i større grad rundt våre systemer, enn gjennom ytre murer selv om vi har en del filtrering og sikkerhetstiltak i vår yttergrense. Tiltaket bør derfor kost/nytte vurderes.

UiB deler i dag sitt interne nett opp i ulike segmenter med beskyttelse (brannmurer) mellom disse og mot eksterne. En ytterligere segmentering blant annet med et eget segment for lokalt utstyr, vil kunne bedre sikkerheten. Det foreslåtte tiltaket følges opp gjennom en kost/nytte-vurdering og i arbeidet med segmentering av UiBs nettverk.

10. Destruksjon av lagringsmedier som inneholder data

IT-avdelingen har praksis med destruksjon av lagringsmedier (harddisker mm) gjennom en avtale med en profesjonell aktør. Alle lagringsmedier sentralt og de som leveres til IT-avdelingen destrueres på denne måten. Revisjonsrapporten anbefaler at UiB klargjør hvilke rutiner som skal følges ved destruksjon av lagringsmedier fra lokalt utstyr. Det er naturlig å bygge dette inn i retningslinjene som tidligere er omtalt, samt at destruksjon av lagringsmedier defineres og tilbys som en tjeneste fra IT-avdelingen.

11. Skytjenester - lagring og utveksling av data (høy prioritet)

Internrevisjonen anbefaler at det etableres klare retningslinjer for bruk av skytjenester, herunder hvilke som kan benyttes og retningslinjer for lagring av data. En god del av våre forskere, særlig i internasjonale forskningssamarbeid, benytter tjenester som blant annet Dropbox og Google. UiB har ikke avtaler med disse to, herunder ikke databehandleravtaler.

I utforming av gjennomførende del av styringssystem for informasjonssikkerhet og personvern vil det være naturlig å se på hvordan man kan utdype retningslinjer i bruk av skytjenester. Samtidig er det startet et arbeid for å vurdere avtaler med Google og Dropbox i tillegg til UiBs eksisterende avtaler med Amazon, Microsoft og IBM.

12. Mangelfull fysisk sikkerhet av utstyr som driftes lokalt

IT-avdelingen har fysisk sikring av sine datarom og nettverksrom som en del av det løpende sikkerhetsarbeidet. Lokalt driftet utstyr står ulike steder med varierende sikring. Internrevisjonen anbefaler at UiB foretar en risikovurdering av lokalt driftet utstyr. Dette bør tas med i lokale ROS-vurderinger. Det kan vurderes om det bør utføres en overordnet ROS på hele institusjonen med dette temaet.

13. Andre forhold – tilgang på trådløst nett

Ett av instituttene som har deltatt i revisjonen har tatt opp konfigurasjon og tilgang til trådløse nett som et problem for faglig virksomhet. Dette konkrete tilfellet gjelder det trådløse nettet i Media City Bergen (MCB). Dette nettet eies og driftes av huseier Entra eiendom slik at dette er utenfor UiB og IT-avdelingens kontroll. Instituttet ønsket her å ta dialogen med huseier selv. IT-avdelingen leverer og drifter slike nettløsninger som etterspørres her i UiBs egne nett, blant annet i det nye universitetsmuseet. Saken følges opp i dialog med instituttet.

Universitetsdirektørens kommentar:

Informasjonssikkerhet har de siste årene fått økt oppmerksomhet både internt på UiB, hos Kunnskapsdepartementet og fra øvrige myndigheter. Bakgrunnen er både faktiske forhold med flere og mer alvorlige trusler, men også økt bevissthet på området og dermed økte krav til dokumentasjon, styring og oppfølging. Svakheter i drift og forvaltning av IT-løsninger gir svekket informasjonssikkerhet og personvern.

Rapporten avdekker at det er behov for forbedringer innen lokal IT-drift, og bekrefter og forsterker grunnlaget for det forbedringsarbeidet UiB allerede har igangsatt. Det er formålstjenlig å ta en del av forslagene fra rapporten inn i dette arbeidet, de øvrige inn i annet utviklingsarbeid. IT-avdelingen arbeider sammen med institutter for å komme fram til gode og balanserte løsninger som både kan etterleves og samtidig gi god sikkerhet. For enkelte av forslagene i rapportene er det behov for nærmere vurderinger om det eksisterer bedre måter å dekke det underliggende behovet på.

I sak 53/19 besluttet universitetsstyret Styringssystem for informasjonssikkerhet og personvern. For å oppfylle nasjonale anbefalinger og krav i utformingen av gjennomførende del av styringssystemet, legges det opp til strengere krav til drift av IT-utstyr på UiB. Forslagene i rapporten tas med i utformingen av disse. Samtidig er det etablert tjenester ved IT-avdelingen som bør redusere behovet for lokalt driftet utstyr.

Rapporten anbefaler at man i større grad tar i bruk sentrale tjenester som Lab-IT, Infrastruktur som tjeneste og tilsvarende, og at mer IT-utstyr og løsninger driftes og forvaltes sentralt. IT-avdelingen drifter i dag fagspesifikke plattformer og systemer for noen fagmiljøer. De siste årene har avdelingen hatt som strategi å flytte sine aktiviteter nærmere kjernevirksomhet til universitetet og har omdisponert både investeringsmidler og personale for å realisere dette. Dette har resultert i nye tjenester til forskning som blant annet SAFE, Lab-IT og Infrastruktur som tjeneste. Det er ønskelig å fortsette denne utviklingen og en videre oppbygging av området vil bli vurdert.

Informasjonssikkerhet ble også tatt opp i tilbakemeldingen fra departementet etter etatsstyringsmøtet. Som en oppfølging av dette vil universitetsstyret også få forlagt en sak om informasjonssikkerhet i løpet av høsten 2019.

16.08.2019/Tore Burheim (avd.dir)

Revisjonsprosjekt

Delprosjekt Nr 2019/01: Lokalt driftede IT systemer

Utkast rapport: 21.06.2019

Endelig rapport: 03.07.2019

Til: Universitetsdirektøren ved UiB

Kopi til: Sekretæriat for universitets-ledelsen

Fra: Jan Roger Hånes, PricewaterhouseCoopers AS

Sign: 

pwc

Innholdsfortegnelse

1 Introduksjon

Bakgrunn

Universitetet i Bergen har en del IT-utstyr og IT-systemer som driftes lokalt ved institutter og fakulteter. Disse skal i utgangspunktet følge UiBs rutiner og retningslinjer for sikkerhet, forvaltning og drift.

PricewaterhouseCoopers (PwC) har gjennomført en internrevisjon av utvalgte institutter for å gjennomgå og evaluere om de løsninger som driftes lokalt er i tråd med UiBs rutiner og retningslinjer med fokus på:

- Organisering av IT drift, herunder kompetanse og ressurser
- IT driftsløsninger, herunder at det er etablert rutiner knyttet til backup-/restore-, redundans, overvåkning, kontinuitets- og beredskapsplaner for kritiske systemer.
- Sikkerhet - både logisk og fysisk (datarom).

Internrevisjonen er gjennomført med utgangspunkt i revisjonsplan for 2019 vedtatt 21.02.2019 av styret.

Formål og omfang

Formål og omfang er definert i planleggingsmemo, som er godkjent av UiB.
Vi har i revisjonen vil hatt fokus på følgende områder:

- Organisering – kompetanse og ressurser
- Rutiner og retningslinjer knyttet til IT-sikkerhet (SIS)
- Rutiner for opprettelse, endring og sletting av brukere
- Sikkerhet i forhold til eksterne aktører (leverandører og samarbeidspartnere)
- Periodisk kontroll av bruker tilganger
- Nettverkssikkerhet
- Fjernpålogging
- Fysisk sikkerhet (datarom der servere og annet utsyr er plassert)
- IT drift (backup, restore, overvåkning)

Avgrensning

Revisjonsprosjektet er avgrenset til områder som er nevnt ovenfor.

Revisjonsperiode og revisjonsteam

Internrevisjonsprosjektet ble gjennomført i mai – juni 2018.

Revisjonsteamet fra PwC har bestått av Jan Roger Hånes, Olav Høsøien og Preben Nyløkken.

Gjennomført arbeid

Observasjoner med tilhørende anbefalinger er beskrevet i seksjon 3. Vår rapport er basert på arbeidsmøter med ansatte i de ulike enhetene, samt gjennomgang av innhentet dokumentasjon. Tabellen nedenfor viser en oversikt over ansatte som har vært involvert i internrevisjonsprosjektet.

Enhet	Navn
IT-avdelingen	Jan Kristian Walde Johnsen, leder Infrastruktur Magne Bergland, leder brukerstøtte Sidsel Storebø, IT-sikkerhetsansvarlig
Det samfunnsvitenskaplige fakultet – Institutt for informasjons- og Medievitenskap	Terje Thue, senioringeniør Kurt Gjerde, senioringeniør
MATNAT – Geofysisk institutt	Idar Hessevik, senioringeniør

Enhet	Navn
Det medisinske fakultet (MED) – Institutt for biomedisin	Torstein Ravnskog, overingeniør

Rapport og rapportstruktur

Vi har i vår gjennomgang hatt fokus på å identifisere forbedringsområder som vi mener vil kunne gi nyttige anbefalinger og innspill i den videre prosessen med å forbedre og videreutvikle UiBs internkontroll på dette området. UiB må selv vurdere de foreslåtte anbefalingene med hensyn til kost/nytte-effekt.

Vår rapport er delt inn som følger:

- Oppsummering av hovedobservasjoner og konklusjon på overordnet nivå.
- Detaljrapport som viser detaljerte observasjoner og anbefalinger for hvert av revisjonsområdene.

Vedlegg

Vedlegg 1 – Symboler

2 Oppsummering

Risikovurdering: Middels	**Vurdering av intern kontroll:**		**Trend:** Ikke aktuelt

Oppsummering:

Innledning
UiB har en del IT-utstyr og IT-systemer som driftes lokalt ved institutter og fakulteter. Det er egne lokale it-ansvarlige som har ansvar for drift- og sikkerhet knyttet til dette utstyret/systemene, og de skal følge UiBs rutiner for sikkerhet, forvaltning og drift av disse systemene.

Hovedinntrykk

- De lokale It-ansvarlige synes å ha god kompetanse på de løsninger som driftes lokalt og er kjent med UiBs rutiner og retningslinjer knyttet til informasjonssikkerhet og har en god støtte og kommunikasjon med UiBs sentrale IT-avdeling.
- UiB har standard oppsett Linux-, Mac- og Windows7- og Windows10-klienter, servere og PC-er, noe som bidrar til at de lokalt driftede Instituttene som inngår i revisjonen, følger UiBs innkjøpsrutiner og rammeavtaler for kjøp av IT-utstyr med mindre annet utstyr som f.eks. instrumenter har spesielle krav.
- løsningene kan sikres i henhold til UiBs retningslinjer.
- UiB har implementert Lab-IT som er en sentralt støttet infrastruktur-løsning, som vil sikre at usikrede og sårbare instrumenter kan kobles til UiB-nettverket samt tilby lagring på sentral server, gi beskyttelse mot hacking og gjør det mulig å gi tilgang til leverandører som trenger det for å yte service. Løsningen er ikke rullet ut for alle enheter enda.
- Sentral IT har i tillegg en «UH-laas»-løsning som er tilgjengelig for instituttene med kobling mot Window Server Update Services (WSUS) som fortløpende ruller ut Windows sikkerhetsoppdateringer.
- UiBs IT-avdeling har utviklet en løsning for sikker behandling av sensitive personopplysninger i forskning - SAFE. Gjennom SAFE tilbyr IT-avdelingen en løsning der ansatte, studenter og eksterne får tilgang til dedikerte ressurser for behandling av sensitive personopplysninger
- UiB har etablert rutiner som sikrer at ukjente enheter som kobles til fysiske nettverkspunkt, ikke får tilgang til Internett/intern-nettet før vedkommende autentiserer seg med brukernavn og passord eller engangskode på SMS.

Forbedringsområder / utfordringer

Vi har også identifisert en del forbedringsområder. Vi viser til seksjon 3 «Observasjoner og anbefalinger» for flere detaljer knyttet til de enkelte punktene.

Risikovurdering: Middels	**Vurdering av intern kontroll:**		**Trend:** Ikke aktuelt

Oppsummering:

Kommunikasjon / roller og ansvar lokal IT ansvarlig og sentral IT avdeling

- De lokale IT-ansvarlige er stort sett fornøyd med kommunikasjon, støtte og oppfølgning fra UiBs sentrale IT-avdeling samt rutiner og retningslinjer som er tilgjengelig via UiBs nettsider. Fordeling av roller og ansvar mellom lokal IT ansvarlig og sentral IT-avdeling synes noe uklare.

Sentral IT-avdeling mangler oversikt over systemer/utstyr som driftes lokalt

- Sentral lT-avdeling har ikke fullstendig oversikt over lokalt driftede systemer.

Drift av lokalt utstyr

- Utstyr som driftes lokalt er ikke underlagt UiBs rutiner knyttet til drift og sikkerhet, herunder backup, antivirus, sikkerhetsopp-dateringer med mer.

Gammelt utstyr

- UiB har en del utstyr som driftes lokalt med gamle versjoner av operativsystem (Win XP og Win7) samt en del gamle maskiner som det er vanskelig å få reservedeler til, noe som kan utgjøre en risiko dersom disse blir forsøkt hacket eller blir ødelagt.

Backup lokalt driftede PC-er

- Lokalt driftede PC-er som ikke er koblet opp i UiBs nett, inngår ikke i UiBs backup-rutiner

Nøkkelmannsrisiko - sårbarhet / UiB mangler instruks for lokale IT ansvarlige

- Det er ikke utpekt en formell backup-person for lokal IT-ansvarlig, og det er ikke utarbeidet instruks for lokale IT-ansvarlige.

Det er ikke utpekt systemeiere for systemer som driftes lokalt

- I følge UiBs Styringssystem for informasjonssikkerhet (SIS) er «Systemeier den øverste lederen ved enheten og er ansvarlig for de enkelte systemene innenfor enheten» når ikke annet er bestemt. Det er i praksis de lokale IT-ansvarlige som ivaretar dette ansvaret for systemer som driftes lokalt. Dette er ikke formalisert, noe som kan medføre at oppgaver som hører inn under systemeiers ansvar ikke blir ivaretatt.

Mangler brannmur mellom klienter og internett

- UiB har etablert diverse kontrolltiltak for å hindre brudd på konfidensialitet, integritet og tilgjengelighet, herunder brannmurer som dekker nett med høy risiko som SAFE, LAB IT, IOT (Internet Of Things), ADM systemer, Eiendomsdrift mm..

Risikovurdering: Middels	**Vurdering av intern kontroll:**		**Trend:** Ikke aktuelt

Oppsummering:

- UiB har ikke en sentral brannmur mellom klienter og internett. Dette betyr at ansattes maskiner står "rett på Internett". Dette kan utgjøre en sikkerhetsrisiko.

Destruksjon av lagringsmedier som inneholder data

- Det er ulik praksis når det gjelder destruksjon av medier som inneholder data. Instituttene benytter ikke Atea, som UiB har avtale med.

Skytjenester - lagring og utveksling av data

- UiB mangler klare retningslinjer for hvilke skyløsninger som er godkjent å bruke til lagring og utveksling av data.

Mangelfull fysisk sikkerhet utstyr som driftes lokalt

- Utstyr som driftes lokalt er ikke plassert i egne datarom som er sikret mot brann, vann, innbrudd osv., men utstyret er ofte plassert ofte i laboratorier eller på kontorer som normalt er sikret med adgangskontroll – kort og kode.

Andre forhold – tilgang til trådløst nett

- I følge Institutt for informasjons- og Medievitenskap har det vært utfordringer knyttet til trådløst nett eller mangelen på sådan. Dette medførte at de i fjor måtte kansellere undervisning og forskning på bruk av intelligente høyttalere siden eduroam ikke lot seg bruke i denne sammenheng.

3 Obervasjoner og anbefalinger

#	Prioritet	Observasjon	Anbefalinger
3-1	❷ Medium prioritet	***Kommunikasjon / roller og ansvar lokal IT ansvarlig og sentral IT avdeling*** De lokale IT-ansvarlige er stort sett fornøyd med kommunikasjon, støtte og oppfølgning fra UiBs sentrale IT-avdeling samt rutiner og retningslinjer som er tilgjengelig via UiBs nettsider. De lokale IT-ansvarlige deltar også på lunsjmøter og andre møter i regi av sentral It-avdeling der ulike IT-relaterte temaer gjennomgås. Av mulige punkter som kan forbedres nevnes: • Informasjon om nye driftsrutiner, f.eks. endring med hvordan MAC-klienter driftes og installeres. Bruker må aktivt inn å søke for å finne denne informasjonen. • Uklare roller og ansvar sentral IT-avdeling kontra lokale IT-ansvarlige, se pkt. 3-7 nedenfor.	Vi anbefaler at relevant personell blir gjort oppmerksom på publisering av informasjon om nye rutiner / løsninger, f.eks. via mail. Videre bør ansvar sentral IT-avdeling og lokal IT-ansvarlig klargjøres, ref. pkt. 3-7 nedenfor.
3-2	❶ Høy prioritet	***Sentral IT-avdeling mangler oversikt over systemer/utstyr som driftes lokalt*** Fakultetene/Instituttene har standard arbeidsstasjoner og servere som er koblet i UiBs nett som følger UiBs rutiner for standard oppsett, drifts-, sikkerhets- og vedlikeholds-rutiner. Instituttene har i tillegg egne fagsystemer, servere, arbeidsstasjoner som benyttes av de vitenskapelig ansatte, som driftes lokalt av lokal IT-ansvarlig ved instituttene. Sentral lT-avdeling har ikke fullstendig oversikt over lokalt driftede systemer.	Vi vil anbefale at UiB utarbeider en mal for oversikt over IT-systemer/løsninger som driftes lokalt, og at denne fylles ut av hvert fakultet/institutt. Oversikten bør minimum inneholde: • Server, PC-type - modell • Operativsystem – versjonsnummer • Antivirus • Kontaktperson • System / applikasjon som kjøres • Behandling / lagring av personopplysninger, ref. GDPR • Instrument som er koblet til

#	Prioritet	Observasjon	Anbefalinger
			• Systemeier - navn • Backup • Lokalisering - kontor/rom • Koblet i UiBs nett eller ikke • Lab-IT • Risikovurdering i forhold til kritikalitet (f.eks. Høy, Lav, Medium) Oversikten bør oppdateres fortløpende, og deles med sentral IT-avdeling, slik at de til enhver tid har oversikt over systemer/løsninger som driftes lokalt.
3-3	❶ Høy prioritet	***Drift av lokalt utstyr*** *Sentral drift* Klienter/servere som er koblet til UiBs nett og driftes av sentral it-avdeling følger automatisk UiBs standarder for oppsett samt rutiner for patching, antivirus, backup, overvåkning, brukeradministrasjon og andre relevante standarder. *Lokal drift* Instituttene har som nevnt ovenfor i tillegg en del utstyr som driftes lokalt, herunder lokale fagsystemer, instrumenter og lokale PC-er. Disse blir satt opp av lokal IT-ansvarlig ved instituttet, og skal følge UiBs standarder når det gjelder oppsett og drift (ref. ovenfor). *Lab-IT* UiB jobber med å rulle ut Lab-IT, som er en sentralt støttet infrastruktur-løsning, som vil sikre at usikrede og sårbare instrumenter kan kobles til UiB-nettverket. Lab-IT vil gjøre det mulig for forskere å overvåke og ha tilgang til instrumenter fra laboratoriene også utenfor fasilitetene samt tilby løsninger for sikker lagring og backup av data og sikkerhet mot hacking. Lab-IT er ikke tatt i bruk av alle instituttene da dette er arbeid som pågår.	*Lab-IT* Vi anbefaler at alt kritisk lokalt utstyr kobles opp mot Lab-IT for å sikre at: • eldre og usikret lab-utstyr ikke blir en "inngangsport" for hackere, • data lagres på en sikker og trygg måte • det tas backup av systemer og data • eksterne leverandører får tilgang til lab-utstyr ved behov. *«UH-laas»* Vi anbefaler videre at øvrig utstyr (for eksempel lokale servere) kan benytte UiB sin "UH-laas"-løsning. Da får instituttene tilgang på maskiner som er satt opp iht. UiB sine retningslinjer, som sikres med fortløpende sikkerhetsoppdateringer. UiBs sentrale IT-avdeling bør vurdere om det i tillegg er mulig å etablere andre løsninger for nettbasert lagring og backup, ref. kommentarer fra Geofysisk institutt.

#	Prioritet	Observasjon	Anbefalinger
		«UH-laas» UiB har i tillegg etablert «UH-laas» som er en åpen skytjeneste (driftes av UiB) hvor ansatte kan leie servere. Servere som inngår i denne løsningen vil motta løpende sikkerhetspatcher (både til Windows og Linux). Denne løsningen er slik vi forstår det ikke tatt i bruk av alle instituttene. *Kommentar fra Geofysisk institutt* *«Løsningen har - for oss iallfall - en stor ulempe: Virtuell maskin blir definert koblet opp i IT-nett på utsiden av UiB-nett (uninett ressurs) - avskåret fra rasjonelle interne UiB lagringsløsninger basert på cifs/smb, nfs o.l. Fra ulike konfigurasjoner av instrumentering har vi nettopp behov for tilgang på UiB nettverks-basert lagring, utfra hensyn til tilgang på backup og tilgang til de samme data fra UiB-nett generelt.*	
3-4	❷ Medium prioritet	***Gammelt utstyr*** *Gamle versjoner av operativsystemer* En del av de PC-ene som driftes lokalt av instituttene er av eldre dato og kjører på gamle versjoner av Windows operativsystem, herunder XP og Win7 (*). Dette skyldes blant annet at den versjonen av softwaren som kjøres på PC-ene, ikke håndterer nyere Windows-versjoner. Dette kan utgjøre en sikkerhetsrisiko, men siden disse ikke er koblet til internett, anses risikoen for datainnbrudd som relativt lav. *(*) Slik vi forstår det vil støtte / sikkerhetsoppdateringer fra Microsoft på Win7 opphøre fra og med 01.01.2020.* *Gammelt utstyr* En annen utfordring som ble nevnt av institutt for Biomedisin når det gjelder gamle PC-er, er tilgang på reservedeler. Dette har så langt latt seg løse ved at instituttet har et lager av gamle PC-er og har tatt deler fra disse, men dette kan på sikt utgjøre en risiko.	Vi vil anbefale UiB å utarbeide en oversikt over lokale PC-er med eldre versjoner av Windows operativsystem, ref. pkt. 3-2 ovenfor, og vurderer risiko knyttet til disse samt behov for å iverksette risikoreduserende tiltak. Eksempel på tiltak kan være å flytte kritisk utstyr til egne sikrede nett, f.eks. i en “Lab-IT” infrastruktur.

#	Prioritet	Observasjon	Anbefalinger
3-5	❶ Høy prioritet	***Backup lokalt driftede PC-er*** Lokalt driftede PC-er som ikke er koblet opp i UiBs nett, inngår ikke i UiBs backup-rutiner. For Institutt for Biomedisins vedkommende håndteres backup av lokal IT ansvarlig, som tar backup av programvaren som kjøres på de lokale PC-ene. Den enkelte ansatte har selv ansvar for backup av data. Dette kan medføre at det ikke blir tatt backup av kritiske/sensitive data.	Vi vil anbefale at UiB foretar en risikovurdering av lokalt driftet utsyr med fokus på kritikalitet knyttet til systemer og data som lagres på dette. Vi vil anbefale at systemer og data som anses som kritiske/sensitive kobles til Lab-IT infrastruktur og dermed inngår i UiBs backup-rutiner.
3-6	❷ Medium prioritet	***Nøkkelmannsrisiko - sårbarhet*** De tre instituttene som inngår i revisjonen, har alle egne lokale IT-ansvarlige. Disse skal primært drive fagnær IT-støtte samt ha ansvar for drift og sikkerhet knyttet til utstyr som driftes lokalt. Det er ikke utpekt en formell backup-person, og det er i liten grad utarbeidet formelle rutiner og dokumentasjon knyttet til de systemene/utstyret som driftes lokalt. Instituttene kan således være sårbare dersom lokal IT-ansvarlig blir borte over lengre tid eller slutter.	Vi anbefaler at UiB vurdere å iverksette tiltak for å redusere nøkkelmannsrisiko. Dette kan gjøres gjennom å spre IT-kompetanse blant flere ansatte på instituttene, men det kanskje viktigste tiltaket vil være å knytte flest mulig av de systemer, PC-er og annet utstyr som driftes lokalt opp mot sentral IT infrastruktur som f.eks. Lab-IT. Dette vil bidra til at patching, antivirus, backup, overvåkning, brukeradministrasjon og andre rutiner følger UiBs rutiner og dermed redusere nøkkelmannsrisiko.
3-7	❷ Medium prioritet	***UiB mangler instruks for lokale IT ansvarlige*** De lokale IT-ansvarlige skal som nevnt over primært drive fagnær IT-støtte, ha ansvar for drift og sikkerhet knyttet til utstyr som driftes lokalt. De lokale IT-ansvarlige har også tett kontakt med sentral IT-avdeling og får bistand fra dem ved behov. Det finnes imidlertid ingen instruks eller lignende som klart definerer roller og ansvar for lokal IT-ansvarlig. Dette kan medføre en risiko for at viktige oppgaver ikke blir ivaretatt.	Vi vil anbefale at UiB utarbeider en instruks for lokale IT-ansvarlige som beskriver roller og ansvar for disse. Dette vil gjøre det lettere for de lokale IT-ansvarlige å vite hva som er deres oppgaver og ansvar og hva som er sentral IT-avdelings ansvar. Dette vil kunne redusere risikoen for at viktige oppgaver ikke blir utført.

#	Prioritet	Observasjon	Anbefalinger
3-8	❷ Medium prioritet	***Det er ikke utpekt systemeiere for systemer som driftes lokalt*** I følge UiBs Styringssystem for informasjonssikkerhet (SIS) - Del 1 – Styrende del 2 pkt. 1.5 skal alle systemer ved UiB ha en definert systemeier, som blant annet har ansvaret for: • Gjennomføring av risikovurderinger (ROS-analyser) • Ivareta sikkerhet i systemet(ene) • Kontinuitetsplanlegging • Fysisk sikkerhet I følge pkt. 4.5 i SIS er «Systemeier den øverste lederen ved enheten og er ansvarlig for de enkelte systemene innenfor enheten» når ikke annet er bestemt. I praksis ivaretas de fleste av systemeieroppgavene av lokal IT-ansvarlig ved instituttene, men ikke alle. Dette kan medføre at viktige oppgaver som hører inn under systemeiers ansvar ikke blir ivaretatt.	UiB bør formelt utpeke systemeiere for de systemer som driftes lokalt i henhold UiBs styringssystem for informasjonssikkerhet (SIS), ref. pkt. 3-2 ovenfor. Dette vil kunne bidra til at viktige oppgaver som hører inn under systemeiers ansvar blir ivaretatt i henhold til UiBs rutiner og retningslinjer.
3-9	❷ Medium prioritet	***Mangler sentral brannmur mellom klienter og internett*** UiB har etablert diverse kontrolltiltak for å hindre brudd på konfidensialitet, integritet og tilgjengelighet. Kontrolltiltakene omfatter blant annet overvåkning og monitorering av nettrafikk, filtrering for å ta bort kjente uønskede ipadresser og porter, samt at det er interne brannmurer foran nett med høy risiko som blant annet SAFE, IOT, printere, SD-anlegg m.m.. UiB dumper videre netflow fra all grensetrafikk til en overvåkningsserver hvor data prosesseres. I tillegg har UiB en avtale om å benytte Uninett sin målepåle som ser all trafikk og utfører IDS funksjoner på dette. UiB har imidlertid ikke en sentral brannmur mellom klienter og internett. Dette betyr at ansattes maskiner som står utenfor definerte sikrede nettverk, ref. ovenfor, står "rett på Internett". Kun velkjente porter som eldre virus benytter er stengt ned. UiB kan for eksempel ikke blokkere nettjenester (url-adresser), for å stoppe de ansatte fra å besøke nettsider som inneholder skadelig/ulovlig innhold. All	Vi anbefaler at UiB vurderer en sentral brannmur mellom klienter og internett, som også dekker klienter og utstyr som ikke omfattes av dagens brannmurløsninger. Dette vil kunne sikre at løsninger som ikke behøver å være eksponert mot Internett, er det. Altså at maskiner som skal drifte tjenester som skal være tilgjengelig for omverden blir satt i egne DMZ-soner, og får tilhørende sikkerhets-mekanismer. Videre anbefaler vi at UiB fortsetter dagens praksis med lokale brannmurer innad i det interne nettverket, for særskilt sikring av sensitive/kritiske nettverk som Lab-IT, SAFE, IOT, Printere, SD anlegg osv.).

#	Prioritet	Observasjon	Anbefalinger
		nettverkssikkerhet hviler således på den enkeltes klient-PC, og at PC-en sin Software-brannmur er satt opp riktig. Dersom det oppstår feilkonfigurering av Software-brannmur, eller denne blir deaktivert (av brukere som har tilgang til dette), så vil deres maskin stå rett på Internett og være svært utsatt for dataangrep. Dette kan i ytterste konsekvens medføre at sensitive data kan komme på avveie, eller at en trusselaktør får utvidede tilganger til UiB sitt nettverk. Enkelte institutter har erkjent at dette er en utfordring, og satt opp en egen lokal brannmur som "skjermer" deres lokalt driftete utstyr fra å stå rett på Internett.	
3-10	❷ Medium prioritet	***Destruksjon av lagringsmedier som inneholder data*** Medier som f.eks. harddisker, minnebrikker og minnepinner som inneholder data og ikke lenger skal benyttes, skal destrueres. Det er i dag instituttene selv som destruerer medier som ikke skal benyttes lenger. Dette gjøres ved at man "knuser" eller destruerer mediene på en annen måte, slik at de ikke lenger er lesbare. Slik vi forstår det har UiB en avtale med Atea om destruksjon av data-lagringsmedier som ikke skal benyttes lenger. Denne avtalen benyttes ikke av de instituttene som er dekket i denne revisjonen.	Vi vil anbefale at UiB klargjør hvilke rutiner som skal følges ved destruksjon av lagringsmedier. Vi vil videre anbefale at instituttene i fremtiden benytter seg av avtalen med Atea. Dette vil etter vår mening bidra til en sikker destruksjon av lagringsmedier, og at alle enheter ved UiB gjør dette på en enhetlig måte.
3-11	❶ Høy prioritet	***Skytjenester - lagring og utveksling av data*** UiB benytter Office365 (Onedrive) for lagring og utveksling av data, og har inngått databehandleravtale med Microsoft. Alle ansatte og studenter ved UiB har tilgang til Office365 og 1TB lagring i Onedrive. Ansatte ved UiB som samarbeider med andre universiteter på prosjekter der det lagres og utveksles data, benytter i tillegg andre tjenester som Dropbox og Google Drive. Så vidt vi kan se, har ikke UiB utarbeidet klare retningslinjer for hvilke skyløsninger som er godkjent å bruke. Dette gjelder både skylagring	Vi vil anbfale UiB å etablere klare retningslinjer for bruk av skytjenester, herunder: • hvilke løsninger som kan benyttes • retningslinjer for lagring og utveksling av data. Dersom løsninger som Dropbox og lignende skal være tillatt, bør det vurderes om denne type løsninger skal ha egne retningslinjer - spesielt knyttet til hvilken informasjon som kan lagres i denne type løsninger som UiB ikke drifter eller har kontroll over.

#	Prioritet	Observasjon	Anbefalinger
		og utveksling av data (utenom at Office 365 m/ OneDrive er innført) og Saas-løsninger (Software As A Service). Dette kan medføre at ansatte kan ta i bruk skyløsninger fra selskaper som UiB ikke har nødvendige avtaler med (for eksempel databehandleravtaler). Videre vil ikke UiB kunne stenge ned tilgangen mot enkelte skytjenester (f.eks. dropbox.com) da det ikke eksisterer noen sentral brannmur mellom klienter og internett, ref. pkt. 3-9 ovenfor.	Dette vil sikre at alle ansatte, studenter, gjester og innleide konsulenter er klar over hvilke løsninger som er godkjent for bruk i UiB samt redusere risikoen for at sensitive data kommer på avveie.
3-12	❷ Medium prioritet	***Mangelfull fysisk sikkerhet utstyr som driftes lokalt*** Utstyr som driftes lokalt er ikke plassert i egne datarom som er sikret mot brann, vann, innbrudd osv., men ofte i laboratorier eller på kontorer. Det skyldes blant annet at noe av utstyret som driftes lokalt skal kobles til ikke-nettverk baserte interfacer til instrumenter på laboratorier, utstyr som benyttes i feltvirksomhet eller instrumentering i forbindelse med innsamling av for eksempel metrologiske observasjoner et godt stykke fra ethvert datarom. Dette kan medføre at viktige data kan gå tapt ved eventuell brann, vannlekkasje eller f.eks. tyveri. Det er i denne sammenheng viktig å påpeke at det gjerne er de innsamlede data som er verdifulle og ikke hardware/maskin. Så lenge data blir sikret (nettverkslagring, backup mot sentrale systemer), er det mindre viktig at maskinvare er innelåst på datarom. Tilgang til disse lokalene er normalt sikret med adgangskort.	Vi vil anbefale at UiB foretar en risikovurdering av lokalt driftede systemer og utstyr med fokus på kritikalitet, f.eks. i forhold til hvilke data som lagres på dette. Utstyr som inneholder kritiske data / systemer bør kobles opp mot Lab-IT. Dette vil redusere risikoen for at data går tapt ved f.eks. en brann eller vannlekkasje.
3-13	❷ Medium prioritet	***Andre forhold – tilgang til trådløst nett*** I følge Institutt for informasjons- og Medievitenskap har det vært utfordringer knyttet til trådløst nett eller mangelen på sådan. Dette medførte blant annet at de i fjor måtte kansellere undervisning og forskning på bruk av intelligente høyttalere siden eduroam ikke lot seg bruke i denne sammenheng. Å sette opp eget trådløst nettverk synes også vanskelig pga potensiell konflikt med eksisterende trådløst	Det er viktig at det blir utarbeidet gode rutiner og støtte til forsknings- og undervisningsmiljøer som ikke faller inn under det allmenne behovet ved UiB. Dette bør støttes og administreres av ITA (sentral IT-avdeling) i samarbeid med de berørte miljøene.

#	Prioritet	Observasjon	Anbefalinger
		nettverk (triangulering etc.) og vil kunne være i konflikt med UiBs retningslinjer knyttet til informasjonssikkerhet.	

Vedlegg 1 – Symboler

Evaluering av internkontroll

Grad	Forklaring
	Tilfredsstillende. Internkontrollen møter generelt akseptable standarder.
	Tilfredsstillende – Internkontrollen møter generelt akseptable standarder, men det er identifisert noen forbedringsområder.
	Behov for forbedringer - Internkontrollen møter generelt akseptable standarder, men bør forbedres.
	Behov for forbedringer– Internkontrollen møter under tvil akseptable standarder og det er identifisert flere forbedringsområder.
	Ikke tilfredsstillende – Internkontrollen møter generelt ikke minimum akseptable standarder. Kritiske kontroller er ikke på plass og tap kan oppstå uten å bli oppdaget.

Risikovurdering

Risiko	Forklaring
Høy	Risikoen er klassifisert som lav, medium eller høy, og reflekterer områdets risiko for at UiB ikke skal nå sine mål
Medium	
Lav	

Utvikling

Utvikling	Forklaring
↗	Positiv trend siden forrige gjennomgang
→	Uendret trend siden forrige gjennomgang
↘	Negativ trend siden forrige gjennomgang

Prioritet

Prioritet	Forklaring
❶ Høy prioritet	Anbefalinger som bør gjennomføres umiddelbart. Anbefalingen har kritisk betydning for risikoen i revidert enhet.
❷ Medium prioritet	Anbefalinger som bør gjennomføres så snart som mulig. Anbefalingen har moderat betydning for risikoen i revidert enhet.
❸ Lav prioritet	Anbefalinger som bør gjennomføres, men det er ikke tidskritisk. Anbefalingen har i mindre grad betydning for risikoen i revidert enhet.