Sveriges lantbruksuniversitet
Swedish University of Agricultural Sciences

Styrelsen

BESLUT

SLU ID: SLU ua 2017.1.1.2-3164

2018-06-14

Rektor

Säker fillagring, säkert arkiv?

Beslut

Styrelsen beslutar

att fastställa internrevisionens rapport *Säker fillagring, säkert arkiv?* samt

att fastställa rektors åtgärdsplan med anledning av rapporten.

Ärendet

Internrevisionen har i enlighet med revisionsplanen för 2017 granskat SLU:s hantering av fillagring och arkivering. Internrevisionens sammanfattande bedömning är att det finns brister rörande fillagring avseende effektivitet, ändamålsenlighet och säkerhet. Med anledning av detta rekommenderar internrevisionen ett antal åtgärder.

Beslut i detta ärende har fattats av styrelsen efter föredragning av universitetsdirektör Martin Melkersson. Ärendet har huvudsakligen beretts av avdelningschef Stefan Edholm. Biträdande universitetsdirektör Birgitta Wikmark Carlsson har också deltagit i handläggningen.

Maria Norrfalk

Martin Melkersson

Kopia för kännedom

Prorektor
Dekanerna
Avdelningschefer (motsv.) inom universitetsadministrationen
Universitetdjursjukhusdirektör
Överbibliotekarie

Postadress: Box 7070 75007 Uppsala
Besöksadress: Almas alle´8
Org nr: 202100-2817
www.slu.se

Tel: 018-67 10 00 (vx)
Birgitta.wikmark.carlsson@slu.se

Sveriges lantbruksuniversitet
Swedish University of Agricultural Sciences

Internrevisionen

SLU ID: SLU.ua 2017.1.1.2-3164

2018-06-14

Säker fillagring, säkert arkiv?

Rapport från internrevisionen

Postadress: Postadress
Besöksadress: Besöksadress
Org nr: 202100-2817
www.slu.se

Tel: 018-67 10 00 (vx)
Mobilnr: 072-5461355
lisbeth.sundkvist.johansson@slu.se

Innehåll

1 Sammanfattning

Internrevisionen har i enlighet med revisionsplanen för 2017 granskat SLU:s hantering av fillagring och arkivering. Syftet med granskningen var att bedöma i vilken utsträckning fillagring vid SLU är effektiv, ändamålsenlig och med tillfredsställande säkerhet. Granskningen har fokuserat på data inom forskning och fortlöpande miljöanalys (Foma).

Internrevisionens sammanfattande bedömning är att det finns brister rörande fillagring avseende effektivitet, ändamålsenlighet och säkerhet. Detta riskerar tillgänglighet och spårbarhet vilket bl.a. försvårar möjligheten att utreda misstankar om oredlighet i forskning. Det föreligger även risk att gällande regelverk inte följs, och inte heller den kommande dataskyddsförordningen.

De mest väsentliga iakttagelserna är följande:

1. Det saknas styrande dokument relaterat till IT och lagring av forskningsdata.
2. Informationssäkerhetsklassning har inte genomförts inom hela SLU.
3. Bristfälliga lagringslösningar förekommer och ej godkända molntjänster används. Detta kan leda till att forsknings- och miljöanalysdata samt känslig information inte hanteras med betryggande säkerhet. Det finns även risk för sanktionsavgifter om personuppgifter inte hanteras korrekt.
4. Det finns bristande kunskaper om vilka regler som gäller för arkivering och lagring av forskningsmaterial.

De mest väsentliga rekommendationerna är följande:

1. Att det interna regelverket inom IT och fillagring uppdateras och förankras. Det bör även ske uppföljning av att reglerna följs.
2. Att arbetet med informationssäkerhetsklassningen fullföljs enligt riktlinjerna. Arbetet bör även koordineras, stödjas och följs upp.
3. Att tillåtna lagringslösningar och molntjänster kommuniceras inom SLU. Utbildning bör prioriteras och genomföras för att säkerställa att information lagras i enlighet med interna och externa krav, exempelvis att den kommande dataskyddsförordningen efterlevs.
4. Att forskare upplyses om vilka regler som gäller för såväl fillagring som arkivering av forskningsdata.

2 Bakgrund och motiv

Säker fillagring innebär att informationen som lagras skyddas mot förlust och att användare har säker tillgänglighet till data. Det är av yttersta vikt både för SLU och för enskilda anställda att lagring sker med hög säkerhet. Forskningsmaterial som forskare upprättar tillhör universitetet och får inte skingras, bortföras eller förstöras utan giltigt beslut.

Brister i fillagring av forskningsdata kan leda till:

- att möjligheten att spåra forskningsresultat försvåras, t.ex. att ta del av data efter att någon avslutat sin anställning/utbildning vid SLU. Detta kan innebära att:
  - forskningsresultat inte kan försvaras i efterhand (spårbarhet)
  - svårigheter att utreda misstanke om oredlighet i forskning
- att känslig information sprids till obehöriga
- att data inte hanteras tillfredsställande i enlighet med dataskyddsförordningen. Detta kan innebära sanktionsavgifter vilket kan skada universitetets anseende och förtroende.

Under 2014 genomförde internrevisionen en granskning av SLU:s tjänster inom IT, bland annat IT-stöd, drift och lagring[1]. Utöver de riskområden som identifierades i granskningen 2014, har det tillkommit riskområden då behovet av att lagra större mängder data har ökat kraftigt, populariteten kring användandet av molntjänster har ökat samt högre krav på hanteringen av personuppgifter i och med den kommande dataskyddsförordningen.

SLU har en ny systemlösning, Tilda, för publicering och e-arkivering av data från forskning och fortlöpande miljöanalys. Projektet driftsattes december 2016. Då det fanns behov av vidareutveckling har lanseringen av systemet fastställts till efter sommaren 2018. En funktion har upprättats för att förvalta processen och säkerställa digital arkivering och publicering av forskningsdata. Funktionen heter DCU, Data Curation Unit, och är placerad vid SLU:s bibliotek. DCU består av representanter från biblioteket, juridik och dokumentation samt miljödatastöd.

3 Granskningens omfattning och inriktning

Syftet med denna granskning har varit att bedöma i vilken utsträckning fillagring vid SLU är effektiv, ändamålsenlig och med tillfredsställande säkerhet. Granskningen har fokuserat på forskningsdata och SLU:s arbete med fortlöpande miljöanalys (Foma).

Denna rapport sammanfattar internrevisionens iakttagelser och rekommendationer. Rapporten är skriven som en avvikelserapport.

[1] IT-verksamhet centralt och lokalt, SLU.ua.2014.1.1.2-2016.

Internrevisionen har utöver intervjuer med ett urval av nyckelpersoner, utfört dokumentgenomgång av de interna styrdokument som har upprättats inom området och tagit del av utredningar och externa regelverk. Internrevisionen har även tagit del av en enkät om hantering av forsknings- och miljöanalysdata som tagits fram av DCU. Granskade enheter är SLU:s centrala IT-avdelning samt ett antal institutioner i Alnarp, Umeå och Uppsala som helt eller delvis bedriver egen IT-verksamhet.

Granskningen har genomförts av Andreas Sandberg, IT-revisor (CISA, CISM) från Transcendent Group och Lisbeth Sundkvist Johansson, internrevisor från SLU.

4 Styrande dokument för lagring av data

Det saknas styrande dokument relaterat till IT och lagring av forsknings- och miljöanalysdata vilket ökar risken för felaktig hantering av informationen.

Syftet med ett styrande dokument är att ledningen tydliggör sina mål, inriktningar, omfattning samt styrning, detta gäller även styrning av IT. Om styrande dokument inte finns tillgängliga för universitetets anställda finns risker att anställda inte vet hur man ska förhålla sig till IT och att ledningens avsikt gällande IT inte kommuniceras.

Internrevisionens granskning har visat att det finns en strategi för bevarande av elektroniska handlingar[2], där hantering av data för forskning och Foma ingår. I strategin anges mål, ansvar och roller, bevarandeplan och dokumentation, tekniska krav och format, e-arkiv samt uppföljning. Det finns även en IT-policy från 2005 men den är inte tillgänglig på SLU:s medarbetarwebb. Enligt åtgärdsplan till internrevisionens rapport ”IT-verksamheten centralt och lokalt” anges att en ny IT-policy samt en lagringspolicy skulle ha fastställts 2015-04-30. Enligt uppföljning vid internrevisionens årsrapport 2016 framgår att IT-rådet påbörjat ett arbete med att ta fram såväl IT-policy som lagringspolicy. Internrevisionen kan konstatera att det finns brister i det formella regelverket för hur information som skapas ska hanteras. Det blir än viktigare att upprätta styrdokument kring detta då användandet av molntjänster på SLU ökar, se avsnitt 5 för mer information.

Vidare bedöms det viktigt att hantera information på ett tillfredsställande sätt då den nya dataskyddsförordningen som träder i kraft den 25 maj 2018 ställer höga krav på hanteringen av personuppgifter.

SLU har tagit fram en handbok för forskare som omfattar ett tydligt stöd för hanteringen och bevarandet av forskningsdata med fokus på arkivering. Handboken finns tillgänglig på medarbetarwebben. Miljödatastöd, som är en stödorganisation inom Foma, har upprättat en kvalitetsguide för att bedriva långsiktigt kvalitetsarbete för datahantering. Med hjälp av kvalitetsguiden kan verksamheten

[2] Strategi för bevarande av elektroniska handlingar, SLU.ua2016.2.1.2-1990.

till exempel förbättra dokumentation, tydliggöra ansvars- och rollfördelning, kontrollera och förbättra informationssäkerhet, minska personberoenden och öka tillgängligheten till data. Internrevisionen ser positivt på detta arbete som syftar till att förbättra hanteringen av data. Det är inte obligatoriskt att följa vare sig handbok eller kvalitetsguide och såvitt internrevisionen erfar sker ingen uppföljning av att fillagring sker enligt gällande regler.

Internrevisionen har noterat att val av teknisk lösning varierar både på institutionsnivå och på individnivå. Då lagringspolicy saknas finns ingen övergripande syn på hur data ska hanteras, varken ur ett tillgänglighets- eller säkerhetsperspektiv.

Granskningen har visat att ett flertal av de institutioner som hanterar egen IT-drift ställer sig positiva till att få stöd i form av styrande dokument gällande lagring.

Internrevisionen ser det som angeläget att minimikrav på säkerhet ställs, inte minst för de institutioner som hanterar sin egen IT-drift. Kraven bör vara obligatoriska att följa.

Internrevisionen rekommenderar att universitetsledningen säkerställer

A. att styrdokument för IT och fillagring upprättas och tillgängliggörs. Styrdokument för IT bör bland annat definiera syfte, mål, inriktning, omfattning och ansvarsfördelning. För fillagring bör bland annat minimikrav beslutas för säkerhet, tillgänglighet och lagringsformer. Styrdokumenten bör förankras i verksamheten, helst redan vid framtagandet för att underlätta implementeringen. Det bör även ske uppföljning av att fillagring sker enligt uppställda regler.

Vidare rekommenderas att ledningen bedömer om styrdokument för IT och fillagring ska vara policyer eller om de ska utformas som riktlinjer och därmed vara ett mer bindande styrdokument.

Internrevisionen rekommenderar att universitetsledningen överväger

B. att styrdokumenten för IT och fillagring knyts till strategin för bevarande av elektroniska handlingar.

5 Informationssäkerhet

Informationssäkerhetsklassning har inte genomförts inom hela SLU vilket riskerar leda till att information inte ges nödvändigt skydd.

Informationssäkerhetsklassning är en process som syftar till att bedöma informations värde och skyddsbehov så att rätt åtgärder kan vidtas för att informationen ska få rätt hantering och skydd. Myndigheten för samhällsskydd och

beredskap, MSB, beslutade 2016 om en föreskrift[3] gällande statliga myndigheters informationssäkerhet. Föreskriften nämner bland annat att myndigheter ska, genom informationssäkerhetsklassning, identifiera och vidta åtgärder som krävs för att uppfylla informationens skyddsbehov.

Granskningen har visat att SLU har påbörjat arbete med informationssäkerhetsklassning. Det har bland annat upprättats riktlinjer[4], instruktioner och en mall för informationssäkerhetsklassning samt påbörjats en sammanställning över institutioner som genomfört informationssäkerhetsklassning. Det saknas dock tydliga krav på att all verksamhet ska bedöma värdet och skyddsbehovet på sin information. Det saknas även uppgifter om hur långt SLU har kommit med klassningsarbetet.

Internrevisionen rekommenderar att universitetsledningen säkerställer

C. att arbetet med informationssäkerhetsklassningen fullföljs enligt riktlinjerna. Detta för att ge all information ett lämplig skydd men även säkerställa att universitetet efterlever föreskriften som beslutats av MSB. Ägaren av informationen är den som är ansvarig för genomförandet av informationssäkerhetsklassningen och detta bör tydliggöras och kommuniceras.

D. att arbetet med informationssäkerhetsklassningen koordineras, stödjs och följs upp.

Ej godkända molntjänster används vilket kan innebära att känslig information kommer obehöriga tillhanda.

Molntjänster innefattar bland annat lagring som tillhandahålls av leverantörer som tjänster över internet. Granskning har visat att forskare på SLU använder sig av olika molntjänster, bland annat för att kunna dela information med andra parter på ett enkelt och smidigt sätt.

Internrevisionen har tagit del av underlag från en genomsökning som IT-avdelningen utförde under oktober 2017 som visar vilka molntjänster som används inom SLU. Genomsökningen visade att vid undersökningstillfället användes 12 olika molntjänster, bland annat den populära tjänsten Dropbox. Det kan inte uteslutas att känslig information lagras i dessa molntjänster. Internrevisionen anser att lagring i molntjänster innebär en hög risk då den nya dataskyddsförordningen ställer höga krav på hanteringen av personuppgifter. Om SLU inte efterlever de krav som ställs i den nya dataskyddsförordningen finns risk för allvarliga påföljder som Datainspektionens sanktionsavgifter på upp till 20 mnkr.

[3] Myndigheten för samhällsskydd och beredskaps föreskrifter om statliga myndigheters informationssäkerhet (MSBFS2016:1).
[4] Riktlinjer för informationssäkerhetsklassning, SLU ua 2015.2.10-2115.

Under sommaren 2017 tog SLU ett beslut[5] om att molntjänsterna Office365, inkl. Onedrive och Azure får användas inom SLU, förutsatt att det säkerställs att informationen som lagras uppfyller lagar och andra krav. Beslutet uppdaterades januari 2018. I beslutet nämndes även att information ska kommuniceras och utbildning ska genomföras gällande molntjänster på SLU. I samband med beslutet om molntjänster genomfördes en risk- och sårbarhetsanalys, RSA, på de två molntjänsterna.

Det pågår för närvarande ett arbete med att ta fram förslag till beslut om ytterligare molntjänster som får användas för lagring och för backup. Internrevisionen ser positivt på detta arbete då det bör leda till att säkrare molntjänster erbjuds anställda.

Internrevisionen rekommenderar att universitetsledningen säkerställer

E. att anställda informeras om vilka molntjänster som är tillåtna respektive inte tillåtna att använda vid SLU. Information och utbildning bör prioriteras för att minska riskerna för otillåten användning av molntjänster och till följd av det, felaktig hantering av allmänna handlingar och känslig information.

Internrevisionen rekommenderar att universitetsledningen överväger

F. att regelbundet följa upp eventuell kommunikation mellan SLU och olika molntjänster för att försöka minimera risken för användning av osäkra och ej godkända molntjänster.

Informationssäkerhetskrav i projektet Tilda har inte beaktats vilket kan leda till att forskningsdata i systemet inte blir tillräckligt skyddad.

Inom systemutveckling bör säkerhetskrav identifieras och dokumenteras i ett tidigt skede i utvecklingsprocessen. På detta sätt minskas risken för eventuella säkerhetsbrister i utvecklingen av system.

SLU har en säkerhetsorganisation där informationssäkerhet är ett av fyra områden.[6] De har i uppdrag att bland annat ansvara för informationssäkerhetsarbetet vid SLU och ge stöd till verksamhet och ledning i säkerhetsfrågor.[7] Det är oklart om krav på informationssäkerhet har beaktats i projektet Tilda. Vid granskningen har det framkommit att ansvarig för informationssäkerhet inte var involverad under projekttiden för identifiering av informationssäkerhetsrisker. Om inte krav på informationssäkerhet beaktas anser internrevisionen att det finns risk för att informationen inte hanteras korrekt i Tilda.

[5] Molntjänster på SLU, SLU.ua 2017.1.1.1-2768.
[6] SLU Säkerhet ligger under infrastrukturavdelningen och hanterar säkerhetsfrågor inom egendomsskydd, informationssäkerhet, personsäkerhet samt kris- och incidenthantering.
[7] Universitetsadministrationens strategi 2017-2020 och verksamhetsplan 2018, SLU.ua.2017.1.1.1-4763.

Internrevisionen rekommenderar att universitetsledningen överväger

G. att informationssäkerhetsrisker identifieras, dokumenteras och hanteras vid den fortsatta utvecklingen av systemet Tilda. Om informationssäkerhetsrisker inte omhändertas kan detta innebära att eventuell känslig information inte blir tillräckligt skyddad.

6 Backuplösningar

Säkerhetskopior för information som inte lagras via IT-avdelningen är inte tillräckligt geografiskt avskilt. Detta kan innebära att SLU förlorar information vid händelse av en katastrof.

Enligt standarden för informationssäkerhet, ISO/IEC 27002, bör säkerhetskopior/backuper förvaras på annan plats och på tillräckligt avstånd för att inte utsättas för eventuella skador vid katastrof på det ordinarie driftstället. MSB har tillsammans med Riksarkivet tagit fram en vägledning om hur IT-utrymmen ska utformas för att ge tillräckligt bra skydd för information på olika skyddsnivåer.

Flertalet av SLU:s institutioner köper lagringstjänster av IT-avdelningen. Central fillagring innebär bland annat att information lagras i systemet och kopieras över till en annan server för att skydda informationen mot förlust. Enligt de uppgifter som internrevisionen tagit del av har 14 institutioner, helt eller delvis, egen lagring av information. Granskningen har visat att det hos vissa institutioner som hanterar sin egen IT-drift förekommer lagring av information som geografiskt sett befinner sig på två ställen i samma byggnad hos SLU. I händelse av en katastrof finns risk att information förstörs och inte går att återläsa.

I granskningen har det framkommit att det är vanligt förekommande att bärbara lagringslösningar som exempelvis externa hårddiskar och USB används. I de fall forskningsdata enbart lagras lokalt i bärbar lagringsmedia, har inte prefekt eller SLU vetskap om att data existerar och var den lagras. Detta kan innebära stora utmaningar för att kunna efterleva de krav som ställs i bland annat den kommande dataskyddsförordningen.

Vidare har det noterats brister i att flera institutioner som hanterar sin egen drift saknar grundläggande beskrivningar och rutiner kring sin IT-drift. Internrevisionen har noterat att de institutioner som har egen IT-drift har olika bemanning för driften. Vissa institutioner har en heltidstjänst medan andra institutioner har ca 25 procent. IT-avdelningen anordnar informationsträffar för IT-samordnarna två gånger per termin där aktuella ämnen inom IT tas upp. Då ett stort nyckelpersonsberoende noterades vid vissa institutioner finns behov av styrande/stödjande dokument som beskriver hur driften hanteras.

Internrevisionen hänvisar till rekommendation A under avsnitt 4 om att upprätta styrdokument för fillagring.

Internrevisionen rekommenderar att universitetsledningen säkerställer

H. att de institutioner som hanterar sin egen IT-drift, upprättar rutinbeskrivningar avseende drifthantering för att minska den sårbarhet som ett stort personberoende innebär.

7 Arkivering

Det finns bristande kunskaper om vilka regler som gäller för arkivering och lagring av forskningsmaterial. Om forskningsmaterial inte lagras och arkiveras korrekt kan bland annat utredning vid misstanke om oredlighet i forskning försvåras.

SLU:s handlingar ska hanteras enligt arkivlagen (SFS 1990:782), arkivförordningen (SFS 1991:446) och offentlighets- och sekretesslagen (SFS 2009:400). Arkivlagen samt Offentlighets- och sekretesslagen (OSL) ställer krav på systematisk ordning, lättöverskådlighet och redovisning. SLU har ett ovillkorligt ansvar för att arkivera såväl forskningsmaterial som annan information eftersom det tillhör universitetet. Det formella ansvaret för bevarande på institutionsnivå har institutionens prefekt.

Granskningen har visat att ett flertal institutioner, som hanterar sin egen IT-drift, inte efterlever dessa lagar och regler. Under hösten och våren 2014/2015 genomförde enheten för juridik och dokumentation en arkivrevision[8] på samtliga institutioner. Revisionen påvisade ett antal brister relaterat till arkivering. Internrevisionen kan konstatera att detta är ett område SLU fortfarande har brister inom.

I granskningen har institutioner lyft fram att det inte finns ett systematiskt och strukturerat sätt för att såväl lagra som arkivera data elektroniskt eller fysiskt. Vissa institutioner kunde inte svara på hur man efterlever de krav som finns kring arkivering. Exempelvis har det funnits tillfällen där en forskare har slutat och forskningsdata har funnits lagrad på institutionens filkatalog. Då institutionen inte har lagrat/arkiverat forskningsdata på ett strukturerat sätt så har de inte kunnat hitta viss forskningsdata. Samtidigt har institutionen inte lyckats komma i kontakt med forskaren vilket ökar problematiken med att kunna efterleva arkivlagens samt offentlighets- och sekretesslagens krav på systematisk ordning, lättöverskådlighet och redovisning. Även säkerställandet av spårbarhet och möjligheten att utreda forskningsfusk påverkas negativt.

[8] Rapport efter arkivrevision inom SLU:s kärnverksamhet 2014/2015, SLU.ua.2015.2.1.1-2853.

I arbetet med att utveckla systemet Tilda har DCU gjort en enkät till SLU:s forskare. En av frågorna avser i vilken grad forskare känner till de arkivkrav som en myndighet ska uppfylla och hur det påverkar hanteringen av deras forskningsdata. Endast 10 procent svarade att de i stor grad känner till krav och påverkan. 45 procent svarade att de i viss grad känner till detta och 45 procent svarade att de i liten grad/inte alls känner till kraven på myndigheten och hur det kan påverka deras hantering av forskningsdata. Internrevisionen anser att detta visar att det finns ett behov av information om hur både fillagring och arkivering av forskningsdata ska ske inom SLU. Det finns även behov av att lyfta fram handboken för hantering av forskningsmaterial.

Internrevisionen har noterat att det ännu inte är bestämt om det ska vara obligatoriskt att använda Tilda vid publicering eller e-arkivering. Om Tilda inte blir obligatoriskt kan det medföra att olika typer av lösningar används, vilket motverkar syftet att upprätta en SLU-gemensam systemlösning för e-arkivering och publicering av forskningsdata och fortlöpande miljöanalys. Granskningen visar att institutionerna har mycket olika förutsättningar och arbetar på olika sätt med forskningsdata vilket innebär en utmaning att utveckla ett system som tillfredsställer samtliga institutioners behov och samtidigt följer de lagkrav som finns kring säker och tillgänglig data.

Internrevisionen rekommenderar att universitetsledningen säkerställer

I. att SLU efterlever de lagar och regler som är upprättade gällande arkivering

J. att forskare upplyses om vilka regler som gäller för såväl fillagring som arkivering av forskningsdata.

K. att användning av Tilda på sikt blir obligatoriskt för all forsknings- och miljöanalysdata för att säkerställa en enhetlig hantering av publicering och e-arkivering. Om behovet av en enhetlig lösning för publicering och e-arkivering inte kan tillgodoses inom Tilda bör en alternativ lösning tillhandahållas.

Inga Astorsdotter
Internrevisionschef

Lisbeth Sundkvist Johansson
Internrevisor

Sveriges lantbruksuniversitet
Swedish University of Agricultural Sciences

Universitetsledningen
Biträdande universitetsdirektör

BESLUT

2018-06-20

SLU ID: SLU.ua 2017.1.1.2-3164

Åtgärdsplan med anledning av internrevisionens rapport ”Säker fillagring, säkert arkiv?”

Övergripande kommentarer.

Internrevisionen har noterat ett antal brister i hur filer lagras och hur forskningsdata arkiveras vid SLU.

Många av internrevisionens rekommendationer kommer sig av att ansvaret för fillagring är distribuerat och därmed vilar på prefekterna. Detta medför risk för, och kan leda till skillnader i kvalitet och rutiner för lagring.

Universitetsledningens uppfattning är att den enklaste lösningen är att uppdra åt IT-avdelningen att ansvara för all fillagring vid SLU och att arkivfunktionen vid ledningskansliet ansvarar för all arkivhantering.

Nedan refereras till punkterna i internrevisionens rekommendationer:

Internrevisionen rekommenderar att universitetsledningen säkerställer

A. att styrdokument för IT och fillagring upprättas och tillgängliggörs. Styrdokument för IT bör bland annat definiera syfte, mål, inriktning, omfattning och ansvarsfördelning. För fillagring bör bland annat minimikrav beslutas för säkerhet, tillgänglighet och lagringsformer. Styrdokumenten bör förankras i verksamheten, helst redan vid framtagandet för att underlätta implementeringen. Det bör även ske uppföljning av att fillagring sker enligt uppställda regler.

Vidare rekommenderas att ledningen bedömer om styrdokument för IT och fillagring ska vara policyer eller om de ska utformas som riktlinjer och därmed vara ett mer bindande styrdokument.

Internrevisionen rekommenderar att universitetsledningen överväger

B. att styrdokumenten för IT och fillagring knyts till strategin för bevarande av elektroniska handlingar.

Postadress: Box 7070, 750 07 Uppsala
Besöksadress: Almas allé 8
Org nr: 202100-2817
www.slu.se

Tel: 018-67 10 00 (vx)
Mobilnr: 076-135 1774
birgitta.wikmark.carlsson@slu.se

A. IT-avdelningen har tagit fram ett förslag till en riktlinje för fillagring. Riktlinjen ska förankras och fastställas.
B. Det föreslagna styrdokumentet är idag anpassat till strategin för bevarande av elektroniska handlingar.

Ansvarig: Universitetsdirektören Klart: 2018-12-31

Internrevisionen rekommenderar att universitetsledningen säkerställer

C. att arbetet med informationssäkerhetsklassningen fullföljs enligt riktlinjerna. Detta för att ge all information ett lämplig skydd men även säkerställa att universitetet efterlever föreskriften som beslutats av MSB. Ägaren av informationen är den som är ansvarig för genomförandet av informationssäkerhetsklassningen och detta bör tydliggöras och kommuniceras.

D. att arbetet med informationssäkerhetsklassningen koordineras, stödjs och följs upp.

C. Informationssäkerhetssamordnaren får i uppdrag att riktlinjerna uppdateras med krav på en bedömning av värdet och skyddsbehovet av informationen.

Ansvarig: Informationssäkerhetssamordnaren Klart: 2018-12-31

D. Informationssäkerhetssamordnaren får i uppdrag att koordinera, stödja och följa upp att informationssäkerhetsklassning genomförs av verksamheten.

Ansvarig: Informationssäkerhetssamordnaren Klart: 2019-12-31

Internrevisionen rekommenderar att universitetsledningen säkerställer

E. att anställda informeras om vilka molntjänster som är tillåtna respektive inte tillåtna att använda vid SLU. Information och utbildning bör prioriteras för att minska riskerna för otillåten användning av molntjänster och till följd av det, felaktig hantering av allmänna handlingar och känslig information.

Internrevisionen rekommenderar att universitetsledningen överväger

F. att regelbundet följa upp eventuell kommunikation mellan SLU och olika molntjänster för att försöka minimera risken för användning av osäkra och ej godkända molntjänster.

E. IT-chefen får i uppdrag att informera hela organisationen om vilka molntjänster som är godkända samt motivet till detta. En speciell sida på medarbetarwebben tas fram där all aktuell information om molntjänster finns.

Ansvarig: IT-chefen Klart: 2018-12-31

F. IT-avdelningen får i uppdrag att rapportera användandet av icke tillåtna molntjänster till Informationssäkerhetssamordnaren.

Ansvarig: IT-chefen **Klart: 2019-06-30**

Internrevisionen rekommenderar att universitetsledningen överväger

G. att informationssäkerhetsrisker identifieras, dokumenteras och hanteras vid den fortsatta utvecklingen av systemet Tilda. Om informationssäkerhetsrisker inte omhändertas kan detta innebära att eventuell känslig information inte blir tillräckligt skyddad.

G. Universitetsledningen delar inte bilden att informationssäkerhet inte beaktats i projektet. Tilda är dock mycket beroende av den underliggande lagringen, vilket innebär att den lagringen måste uppfylla gällande riktlinjer. Tilda-administratörerna ska tilldelas administrativa rättigheter som är separerade från deras vanliga inloggning.

Ansvarig: Universitetsdirektören **Klart: 2018-12-31**

Internrevisionen hänvisar till rekommendation A under avsnitt 4 om att upprätta styrdokument för fillagring.

Internrevisionen rekommenderar att universitetsledningen säkerställer

H. att de institutioner som hanterar sin egen IT-drift, upprättar rutinbeskrivningar avseende drifthantering för att minska den sårbarhet som ett stort personberoende innebär.

H. För att uppfylla standaren för informationssäkerhet ISO/IEC 27002 samt uppfylla MSB:s vägledning för IT-utrymmen så ska en utredning genomföras rörande obligatorisk användning av universitetets gemensamma fillagring. Utredningen ska bland annat innehålla en analys av kostnaderna för lagring samt av vilka eventuella undantag som ska göras från ett obligatorium.

Ansvarig: Universitetsdirektören **Klart: 2018-12-31**

Internrevisionen rekommenderar att universitetsledningen säkerställer

I. att SLU efterlever de lagar och regler som är upprättade gällande arkivering

J. att forskare upplyses om vilka regler som gäller för såväl fillagring som arkivering av forskningsdata.

K. att användning av Tilda på sikt blir obligatoriskt för all forsknings- och miljöanalysdata för att säkerställa en enhetlig hantering av publicering och e-arkivering. Om behovet av en enhetlig lösning för publicering och e-arkivering inte kan tillgodoses inom Tilda bör en alternativ lösning tillhandahållas.

I. Det finn en strategi för bevarande av elektroniska handlingar (Bilaga till: Beslut, SLU ID: SLU.ua.2016.2.1.2-1990-2). Den behöver uppmärksammas igen.

Ansvarig: Chefen för ledningskansliet **Klart: 2018-12-31**

J. Inför lanseringen av TILDA är det viktigt med utbildning till dem som kommer att använda sig av systemet. I samband med detta är det lämpligt att upplysa om reglerna för fillagring och övriga relevanta regler som de måste förhålla sig till. Viktigt är att det ska vara så förmånligt och enkelt att använda system som uppfyller lagkraven att användaren inte behöver fundera på alternativ. Genom att kanalisera användarna till dessa system minskar risken för att filer lagras eller hanteras felaktigt.

Ansvarig: Chefen för ledningskansliet **Klart: 2018-12-31**

K. Eftersom Tilda för närvarande är det enda system vid SLU som uppfyller arkivkraven, och SLU är skyldiga att följa arkivlagen, så innebär det att Tilda kommer att bli obligatoriskt för all arkivering av forsknings- och miljöanalysdata.

Ansvarig: Chefen för ledningskansliet **Klart: 2020-12-31**