Sveriges lantbruksuniversitet
Swedish University of Agricultural Sciences

Styrelsen

BESLUT

SLU ID: SLU ua 2021.1.1.2-2665

2022-02-18

Rektor

Informations- och it-säkerhet

Beslut

Styrelsen beslutar

att lägga internrevisionens rapport *Informations- och it-säkerhet* till handlingarna, samt

att fastställa rektors åtgärdsplan med anledning av rapporten.

Ärendet

Internrevisionen har i enlighet med 2021 års revisionsplan genomfört en granskning av informations- och it-säkerhet på SLU. Syftet med granskningen har varit att bedöma om arbetet med informationssäkerhet är ändamålsenligt och i enlighet med gällande regelverk inom området.

Internrevisionens sammanfattande bedömning är att det finns omfattande brister i SLU:s styrning av informations- och it-säkerhet. Detta medför en förhöjd risk att kritisk information går förlorad, att användarna inte kommer åt informationen eller att obehöriga får åtkomst till skyddsvärd information. Med anledning av detta har ett antal rekommendationer lämnats. Av rektors åtgärdsplan framgår vilka åtgärder som ledningen bedömer bör vidtas.

Beslut i detta ärende har fattats av styrelsen efter föredragning av internrevisor Lisbeth Sundkvist Johansson. Åtgärdsplanen har föredragits av säkerhetschef Robert Arvidsson. Åtgärdsplanen har beretts av universitetsdirektör Martin Melkersson, Miika Wallin, chef för ledningskansliet, P-O Skatt avdelningschef för service, säkerhet och miljö, Petra Lagerkvist, it-direktör och Robert Arvidsson, säkerhetschef.

Rolf Brennerfelt

Lisbeth Sundkvist Johansson

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

Tel: 018-67 10 00 (vx)
Lisbeth.sundkvist.johansson@slu.se

Kopia för kännedom

Prorektor
Dekanerna
Avdelningschefer (motsv.) inom gemensamma verksamhetsstödet
Universitetdjursjukhusdirektör
Överbibliotekarie
SLUSS

Sveriges lantbruksuniversitet
Swedish University of Agricultural Sciences

Internrevisionen

SLU ID: SLU.ua 2021.1.1.2-2665

2021-12-17

Informations- och it-säkerhet

Rapport från internrevisionen

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

Tel: 018-67 10 00 (vx)

Lisbeth.sundkvist.johansson@slu.se

Innehållsförteckning

1. Sammanfattning

Internrevisionen har i enlighet med 2021 års revisionsplan genomfört en granskning av informations- och it-säkerhet på SLU. Syftet med granskningen har varit att bedöma om arbetet med informationssäkerhet är ändamålsenligt och i enlighet med gällande regelverk inom området, såsom föreskrifter från MSB.

Granskningen visar att det finns omfattande brister i SLU:s styrning av informations- och it-säkerhet. Området har varit eftersatt under flera år och det saknas etablerade roller, arbetssätt och processer för att uppnå en ändamålsenlig styrning och kontroll av att universitetets information är tillgänglig, korrekt och skyddad i nödvändig utsträckning. Detta medför en förhöjd risk att kritisk information går förlorad, att användarna inte kommer åt informationen eller att obehöriga får åtkomst till skyddsvärd information.

Det finns ett flertal områden där SLU inte lever upp till de krav som fastställs i MSB:s föreskrifter om informationssäkerhet och säkerhetsåtgärder i informationssystem. Internrevisionen vill dock lyfta fram att det finns positiva tendenser inom området. Under granskningen har det betonats att det nu finns ett tydligare stöd från ledningen och att det även finns ett mer konstruktivt samarbetsklimat och en tydligare styrning kring informations- och it-säkerhet. Under 2021 uppdrog rektor åt universitetsdirektören att genomföra en modernisering av SLU:s it-infrastruktur, vilket inkluderar ett nytt nätverk, livscykelhantering av it-infrastrukturen, nytt e-postsystem och förbättringar inom it-säkerhet.

De väsentligaste rekommendationerna är i korthet följande:

- Att styrande dokument i form av policy, riktlinjer och instruktioner avseende informations- och it-säkerhet utvärderas, uppdateras och tillgängliggörs.
- Att det upprättas ett formellt informationssäkerhetsråd för styrning och samordning.
- Att upprätta tydliga roller, mandat, struktur och styrning av informationssäkerhet för att möjliggöra ett systematiskt och riskbaserat arbetssätt.
- Att rutiner upprättas för regelbunden rapportering till universitetsledningen.
- Att regelbundna utbildningar i informationssäkerhet tillhandahålls.
- Att informationsklassning genomförs för relevanta klassningsobjekt.
- Att åtgärdsplan upprättas för förbättringsåtgärder kring it-säkerhet.
- Att kartläggning och analys genomförs kring leverantörer/tjänster som nyttjas där information riskerar att överföras till länder som saknar ändamålsenligt dataskydd.

2. Bakgrund och motiv

Informationssäkerhet är ett samlingsbegrepp på åtgärder som syftar till att skydda all information utifrån krav på tillgänglighet, konfidentialitet och riktighet; vare sig det är muntlig, tryckt eller elektronisk information. Eftersom informationshantering i stor utsträckning sker med stöd av it-system är informationen alltmer exponerad för olika typer av hot, såsom dataintrång, bedrägerier och spridning av skadlig kod. Hoten kan komma från såväl enskilda individer som organiserad brottslighet och statsmakter.

Myndigheten för samhällsskydd och beredskap (MSB) har uppdaterat föreskrifterna om informationssäkerhet och it-säkerhet för statliga myndigheter som började gälla 1 oktober 2020. Det innebär att det ställs högre krav på att SLU ska bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete. Det omfattar all verksamhet inom SLU som utbildning, forskning, fortlöpande miljöanalys samt administration. Brister inom området kan leda till att verksamheten inte kan bedrivas ändamålsenligt, effektivt och säkert.

MSB förväntas ge ut en vägledning inom kort som ska stötta myndigheter i implementeringen av de nya föreskrifterna. Det pågår en dialog mellan MSB och it-chefsnätverket för universitet och högskolor där de speciella förutsättningarna för universitet och högskolor lyfts fram.

Internrevisionen granskade informationssäkerhet 2014. Även om SLU efter den genomförda granskningen vidtog ett antal åtgärder för att förbättra situationen, har internrevisionen fått indikatorer på att regelefterlevnaden är ojämn. Mot bakgrund av att det gått sju år sedan granskningen genomfördes samt det ökade hotet kring säkerhet och nya krav i regelverket kring informationssäkerhet har internrevisionen bedömt att det är relevant med en ny granskning av området för att erhålla en uppdaterad riskbild.

3. Syfte och mål

Syftet med granskningen har varit att bedöma om SLU:s arbete med informations- och it-säkerhet är ändamålsenligt och i enlighet med gällande regelverk med fokus på:

- MSBFS 2020-6, Föreskrifter om informationssäkerhet för statliga myndigheter
- MSBFS 2020-7, Föreskrifter om säkerhetsåtgärder i informationssystem för statliga myndigheter
- MSBFS 2020-8, Föreskrifter om rapportering av it-incidenter för statliga myndigheter

3.1 Omfattning, avgränsningar och metoder

Granskningen har genomförts via dokumentstudier och intervjuer med nyckelpersoner inom universitetsadministrationen och vid sex institutioner. Granskningens grunder för bedömning har utgått från de krav som ställs i ovan angivna föreskrifter från MSB och avser både informations- och it-säkerhet.

Granskningen genomfördes genom utvärdering av ändamålsenlighet i styrande processer och arbetsmetoder och har inte i detalj testat efterlevnaden av enskilda rutiner.

Informations- och it-säkerhet är nära sammanlänkat med såväl dataskydd som kris- och kontinuitetplanering. Därav granskar internrevisionen även dessa områden under 2021.

Granskningen har genomförts med stöd av Magnus Thyllman, it-revisor från Transcendent Group.

4. Styrning av informations- och it-säkerhet

Det finns omfattande brister i SLU:s styrning av informations- och it-säkerhet. Det saknas etablerade roller, arbetssätt och processer för att uppnå en ändamålsenlig styrning och kontroll av att universitetets information är tillgänglig, korrekt och skyddad i nödvändig utsträckning.

Det finns ett flertal områden där SLU inte lever upp till de krav som fastställs i MSB:s föreskrifter om informationssäkerhet för statliga myndigheter samt föreskrifter om säkerhetsåtgärder i informationssystem för statliga myndigheter.

Internrevisionen vill dock lyfta fram att det finns positiva tendenser inom området där flertalet av de intervjuade framhäver att det nu finns ett mer konstruktivt samarbetsklimat och en tydlig ambition att hitta samverkansformer och en tydligare styrning kring informations- och it-säkerhet. Ledningens stöd har också lyfts fram som positiv utveckling inom området. Det bör även nämnas att rektor under 2021 beslutat[1] att uppdra åt universitetsdirektören att genomföra en genomgripande översyn och modernisering av SLU:s it-infrastruktur, vilket inkluderar ett nytt nätverk, livscykelhantering av it-infrastrukturen och ett nytt e-postsystem. Dessutom föreslås förstudie som kartlägger vilka åtgärder SLU bör vidta för att bevara hög säkerhet i AD:t[2] samt prioriterar och kostnadsätter skyddsåtgärder sprungna från MSB:s krav samt det systematiska säkerhetsarbetet.

[1] Rektors beslut Finansiering av förstärkt IT-infrastruktur, SLU.ua.2021.1.1.1-2911
[2] Active Directory (AD) är en tjänst som används för att hantera och organisera användare, resurser, behörigheter, klienter och servrar i ett nätverk.

4.1 Styrdokument

Det finns brister i underhåll och förankring av styrdokumenten som ökar risken för att SLU:s information hanteras på ett olämpligt sätt.

Styrande dokument inom informationssäkerhetsområdet finns i viss utsträckning tillgängliga på medarbetarwebben men flera av dessa har inte uppdaterats på många år. Det framgår även vid genomförda intervjuer att kännedomen om dessa är låg ute i verksamheten. Merparten av styrdokumenten, som policy, riktlinjer och instruktioner, har inte uppdaterats de senaste fem åren. Säkerhetsenheten har haft begränsad bemanning och har inte haft förmåga att underhålla styrdokumenten inom informationssäkerhetsområdet. Det saknas generellt rutiner för att med regelbundenhet uppdatera styrande dokument inom universitetet.

Enligt säkerhetsenheten har ett arbete påbörjats som avser översyn och uppdatering av styrdokumenten kopplat till informationssäkerhet.

Internrevisionen bedömer att brister i underhåll och förankring av styrdokumenten ökar risken för att SLU:s information hanteras på ett olämpligt sätt. Detta är särskilt allvarligt inom informations- och it-säkerhetsområdet där förändringar sker snabbt p.g.a. den tekniska utvecklingen. Detta kan leda till brister i tillgänglighet och skydd av informationen.

Internrevisionen rekommenderar universitetsledningen att säkerställa

A. att styrande dokument i form av policyer, riktlinjer och instruktioner avseende informationssäkerhet och it-säkerhet utvärderas, uppdateras och tillgängliggörs.

4.2 Organisation och ansvar

Roller, ansvar och mandat för styrning och samverkan kring informationssäkerhetsarbetet mellan de centrala stödfunktionerna och institutionerna är inte tydligt definierat och fördelat. Detta kan leda till att nödvändiga förbättringar inte genomförs och ökar risken för driftstörningar, dataförluster och cyber-attacker.

I riktlinjer för informationssäkerhet från 2015 finns översiktlig beskrivning av roller, såsom exempelvis informationsägare och systemägare. Internrevisionens bedömning är dock att dessa roller inte förankrats tillräckligt i praktiken, speciellt inte vid institutionerna.

It-avdelningen har ett otydligt ansvar och mandat där institutionerna i stor utsträckning upphandlar, utvecklar och hanterar egna informationssystem utan it-avdelningens inblandning. Detta gör det utmanande att åstadkomma en ändamålsenlig struktur och kontroll avseende säkerhet i myndighetens informationssystem.

Samverkan mellan centrala stödfunktioner avseende informationssäkerhet har under flera år varit bristfällig och det har funnits samarbetssvårigheter mellan säkerhetsenheten och it-avdelningen. Samverkansklimatet är nu betydligt bättre och säkerhetschef, it-direktör och it-säkerhetschef har regelbundna möten. Vid dessa möten medverkar numera även dataskyddsombudet. Det saknas dock ett formellt organ, som t.ex. informationssäkerhetsråd eller motsvarande, för strategisk och taktisk planering samt samordning kring informationssäkerhet inom hela universitetet.

För att stärka kompetensen inom it-säkerhet på it-avdelningen så har två nya roller, it-infrastrukturchef och it-säkerhetschef inrättats och tillsatts. Det har varit personalomsättning på viktiga funktioner inom säkerhetsenheten de senaste åren. Även om tillfälliga vakanser har bidragit till att arbetet med informationssäkerhet varit eftersatt, så har SLU även när dessa roller varit bemannade haft svårt att driva informationssäkerhetsarbetet tillsammans med institutionerna. Det saknas tydliga motparter ute i verksamheten för dialog kring informationssäkerhetsfrågor och utifrån den kapacitet som säkerhetsenheten har avseende informationssäkerhet är det utmanande att nå ut till samtliga verksamheter inom SLU.

Vid de intervjuer som genomförts vid institutionerna framkom att roller och ansvar på institutionsnivå avseende informations- och it-säkerhet inte är tydligt definierade. Exempelvis har rollen som informationsägare inte förankrats tillräckligt. Prefekten har det övergripande ansvaret men det finns en osäkerhet kring vem som har det operativa ansvaret för säkerheten kring den information som hanteras inom institutionen.

På institutionsnivå finns ett antal administrativa roller[3] definierade, däribland it-samordnarroll och säkerhetsroll. Dessa roller omfattar vissa mindre delar av informationssäkerhetsområdet men är inte heltäckande. Dessutom finns inte dessa roller på alla institutioner. Det finns även en registrerings- och arkiveringsroll som inte behöver vara institutionsvis utan kan vara kopplad till byggnader, kluster eller campus. I den rollbeskrivningen anges informationshantering och dataskydd men inget specifikt kring informationssäkerhet. Avsaknaden av en tydlig motpart på institutionsnivå gör att det blir svårt för den centrala säkerhetsenheten och it-avdelningen att nå ut och samverka med institutioner/motsvarande kring informationssäkerhetsfrågor. Internrevisionen har vid granskning av dataskyddsförordningen noterat att problem att nå ut till verksamheten även finns avseende dataskyddsarbetet[4].

Vid ovan nämnda granskning framkom även att det pågår diskussioner om att bygga upp en ny dataskyddsfunktion. Den tidigare funktionen bestod av dataskyddsombud, en jurist och ett nätverk av kompetenser från bland annat

[3] Administrativa roller infördes 2011 vid SLU i syfte att kunna ge rätt information och stöd åt rätt person och därmed få bättre fungerande administrativa processer. Beslut om uppdatering av administrativa roller augusti 2020, SLU ID: SLU.2020.1.1.1-3142.
[4] IR:s rapport Hantering av dataskyddsförordningen, SLU ID: SLU.ua 2021.1.1.2-388.

informations- och it-säkerhet. Då informations- och it-säkerhet samt dataskydd är så sammanlänkade avseende informationshantering anser internrevisionen att det är viktigt att fokusera på samtliga tre delarna vid uppbyggnad av ny funktion och inte enbart se informations- och it-säkerhet som stödjande kompetenser till dataskyddet. Även arkiveringskompetens kan behövas.

Internrevisionen bedömer att bristfällig central koordinering kring strategiska och taktiska informationssäkerhetsfrågor samt otillräcklig samverkan ökar risken för att förbättringsåtgärder inte prioriteras eller att de fördröjs.

Internrevisionen bedömer vidare att bristande involvering och styrning av informationssäkerhet på institutionsnivå ökar risken för att SLU drabbas av driftstörningar, förlust av data eller cyber-attacker.

Internrevisionen rekommenderar universitetsledningen att överväga

B. att det upprättas ett formellt råd inom informationssäkerhetsområdet för styrning och samordning, där förslagsvis it-avdelningen (it-säkerhet), säkerhetsenheten (informationssäkerhet), ledningskansliet (dataskydd samt arkivfunktion), biblioteket samt forsknings- och utbildningsverksamheten är representerade. Rådets syfte och mandat liksom motparter på ledningsnivå för rapportering och beslutsfattande bör tydligt definieras.

C. att utreda möjligheten att utforma en roll som informationssäkerhetssamordnare som en obligatorisk administrativ roll på institutioner/motsvarande. Rollen bör omfatta ett samordningsansvar för frågor kring informationssäkerhet, it-säkerhet och dataskydd.

D. att en utvärdering görs kring möjligheterna att tillsätta centralt finansierade informationssäkerhetsspecialister (förslagsvis en per fakultet) med uppgift att koordinera, samverka och stötta i arbetet med informationssäkerhet ute i forsknings- och utbildningsverksamheten på institutionsnivå.

4.3 Systematik i arbetssätt

Det saknas struktur och styrning för ett systematiskt och kontinuerligt informationssäkerhetsarbete, inklusive riktade utbildningar för kritiska roller, vilket ökar riskerna för att universitet drabbas av driftstörningar, förlust av data eller cyber-attacker.

Det saknas ett strukturerat och systematiskt arbete kring informationssäkerhet inom universitetet. Det saknas även en struktur för riskbedömning av SLU:s it-miljö som helhet samt för enskilda informationssystem. Regelbundna riskanalyser genomförs inte på institutionsnivå. Inom it-avdelningen har dock projektkontoret initierat ett riskanalysarbete där förvaltningsledare börjat genomföra riskanalyser med stöd av MSB:s mallar.

Ett ledningssystem för informationssäkerhet finns upprättat i form av policy, riktlinjer och instruktioner på området. Det saknas däremot roller, mandat, struktur och styrning för att med ett systematiskt och riskbaserat arbetssätt införa, följa upp och åtgärda nödvändiga skyddsåtgärder. Säkerhetsenheten har under 2021 genomfört en intern mognadsbedömning med hjälp av MSB:s verktyg ”Infosäkkollen”. Den visar att SLU ligger på en genomsnittlig mognadsnivå strax under 1 i en 4-gradig skala, vilket benämns som ”organisationer som har grunderna i informationssäkerhetsarbetet på plats, åtminstone i begränsad omfattning”. Resultatet visar att särskilda förbättringsområden finns i arbetet med uppföljning, utvärdering och upphandling.

Informationssäkerhetsaktiviteter har utförts men oftast ad hoc och utan nödvändig spårbarhet och dokumentation. Det saknas även en strukturerad uppföljning och rapportering till universitetsledningen om informationssäkerheten på universitetet. Tidigare har säkerhetsenheten haft genomgång med ledningen kring informationssäkerhet men det har inte genomförts de senaste åren. En bidragande orsak till detta kan vara de personalförändringar som har skett både på säkerhetsenheten och på rektorspositionen. Rektor och universitetsdirektör har enligt intervjuerna visat stort intresse, engagemang och stöd gällande it-säkerhetsfrågor och får numera återkommande uppdateringar kring arbetet med it-säkerhet.

Att öka den generella medvetenheten och kunskapsnivån är en viktig del av informationssäkerhetsarbetet. Ett antal korta så kallade ”Nano-learnings” har genomförts där utskick via e-post använts för att nå ut till alla anställda. Utbildningsformen har upplevts positiv och är något som efterfrågas igen. Någon riktad utbildning mot kritiska roller såsom informationsägare och systemägare har inte genomförts.

SLU har tidigare inte haft någon systemförvaltningsmodell men 2020 beslutades att införa en sådan modell.[5] Modellen är en modifiering av den s.k. Pm3-modellen[6] och är under uppbyggnad. Ett flertal förvaltningsobjekt har skapats vid it-avdelningens projektkontor men även här upplevs det utmanande att hitta lämpliga motparter inom SLU för samverkan kring förvaltning av informationssystemen.

Internrevisionen bedömer att avsaknad av ett strukturerat arbetssätt i kombination med bristfällig uppföljning och rapportering kring informationssäkerhet medför att universitetet saknar förmågan att upprätthålla en ändamålsenlig säkerhetsnivå samt att universitetsledningen inte får tillräcklig insyn i detta. Utan tillräcklig kunskap om hot, risker och nödvändiga skyddsåtgärder för att hantera och skydda SLU:s

[5] Universitetsdirektörsbeslut SLU ua 2020.1.1.1-680

[6] Pm3 - en styrningsmodell för förvaltning av it-styrningssystem. Modellen används av flera lärosäten. Pm3 används idag vid flera lärosäten i Sverige t ex vid Linnéuniversitetet, Luleå tekniska universitet, Uppsala universitet, Chalmers tekniska högskola, KTH.

information ökar också riskerna för att universitet drabbas av driftstörningar, förlust av data eller cyber-attacker.

Internrevisionen rekommenderar universitetsledningen att säkerställa

E. att det upprättas tydliga roller, mandat, struktur och styrning av informationssäkerhet för att med ett systematiskt och riskbaserat arbetssätt införa, följa upp och åtgärda nödvändiga skyddsåtgärder, exempelvis i form av riskanalyser och informationsklassningar.

F. att rutiner upprättas för regelbunden rapportering till universitetsledningen om informations- och it-säkerhetsarbetet samt om identifierade hot och risker inom området. Se över möjligheten att samordna detta med rekommendation B.

G. att kortare web-utbildningar i informationssäkerhet, s.k. nano-learning, regelbundet riktas till samtliga anställda, samt att specialanpassade återkommande informationssäkerhetsutbildningar tillhandahålls till systemägare, informationsägare, systemförvaltare och andra nyckelroller (se rekommendation C).

4.4 Informationsklassning

Det finns information och system som inte har klassats och därmed saknar en tydlig bedömning av hur informationen ska hanteras och skyddas. Detta innebär en förhöjd risk för brister i tillgänglighet, datakvalitet och säkerhet.

En riktlinje för informationsklassning (2015) och en instruktion för informationsklassning (2014) finns framtagna och de finns tillgängliga på medarbetarwebben. Det förefaller dock utifrån genomförda intervjuer vid ett urval av institutioner att dessa dokument inte är kända ute i verksamheten och inte nyttjas i någon större utsträckning. För de system som förvaltas lokalt på de intervjuade institutionerna saknas i stor utsträckning informationsklassning och det finns ingen central uppföljning kring detta. I internrevisionens granskning 2017, Säker fillagring, säkert arkiv, konstaterades att informationssäkerhetsklassningen inte hade genomförts inom hela SLU.

Internrevisionen har från säkerhetsenheten tagit del av en systemsammanställning där det framgår vilka av de centralt förvaltade systemen som informationsklassats. De flesta av systemen som förvaltas av it-avdelningen saknar klassning (exempelvis incidenthanteringssystem och e-postsystem). Detta gäller även system som tillhör ekonomiavdelningen och personalavdelningen. De flesta av de system som är klassade tillhör avdelningen för lärande och digitalisering. Ett stort antal system saknar dock informationsklassning. Utöver de system som ingår i den nämnda sammanställningen finns även en stor mängd system som förvaltas av institutionerna som i de allra flesta fall saknar informationsklassning.

Internrevisionen gör bedömningen att informationsmängder och system som inte klassats, och därmed saknar en tydlig bedömning av hur informationen behöver hanteras och skyddas, har en förhöjd risk för brister i tillgänglighet, datakvalitet och säkerhet.

Internrevisionen rekommenderar universitetsledningen att säkerställa

H. att informationsklassning genomförs för relevanta klassningsobjekt såsom projekt, lagringsytor och system inom hela SLU:s verksamhet samt att stöd och mallar för informationsklassning kommuniceras och följs upp.

4.5 Hantering av forsknings- och miljödata

Det finns brister i styrning, samordning och uppföljning kring hanteringen av forsknings- och miljödata. Ur ett informationssäkerhetsperspektiv ökar detta risken för att SLU inte uppfyller nödvändiga krav på kvalitet, spårbarhet och skydd av denna information.

En stor del av den information som hanteras inom SLU utgörs av forsknings- och miljödata. Informationen omfattar både underliggande material och de analyser som ligger till grund för forskningsresultaten samt de slutresultat som publiceras via olika kanaler. För närvarande saknas en enhetlig och strukturerad hantering av forsknings- och miljödata för att säkerställa att informationen har en ändamålsenlig spårbarhet och tillgänglighet samt att den är tillräckligt skyddad. Dock pågår sedan ett antal år tillbaka ett arbete[7] med att möjliggöra ändamålsenliga tekniska lösningar för publicering och lagring för forsknings- och miljödata.

It-avdelningen har inte haft möjligheter att tillhandahålla centrala lösningar för forsknings- och miljödata som uppfyller institutionernas behov. Därför lagras i viss utsträckning sådan data lokalt på forskarnas datorer och externa hårddiskar som köps in lokalt. För miljödatahantering finns riktlinjer, kvalitetsmål och kvalitetskrav samlade i en kvalitetsguide beslutad av rektor.[8] För övrig forskningsdata saknas tydliga riktlinjer eller instruktioner för vilka kriterier som behöver uppfyllas för att säkerställa tillräcklig kvalitet, spårbarhet och skydd av informationen. I många forskningsprojekt ställs krav från externa finansiärer på datahanteringsplan där det ska beskrivas hur informationen ska hanteras under projektet. Intervjuer på institutionsnivå visar dock att detta inte alltid upprättas och det saknas en kvalitetskontroll kring detta. Intervjuade representanter från institutionerna har även efterfrågat ett tydligare stöd kring detta. Internrevisionen har i en tidigare granskning, Säker fillagring, säkert arkiv[9], rapporterat att det

[7] Tilda-projektet arbetade under 2013-2018 med att ta fram ett systemstöd för publicering och elektronisk arkivering för forsknings- och miljöanalysdata. Erfarenheterna från det projektet utgör nu grunden för vidare arbete med lösningar för publicering och lagring av forsknings- och miljöanalysdata.
[8] Kvalitetsguide för SLU:s miljödatahantering, ua.2020.5.3-569.
[9] SLU ua 2017.1.1.2-3164.

saknas styrande dokument relaterat till lagring av forsknings- och miljöanalysdata. Rekommendationen är ännu inte åtgärdad.

Data Management Support, DMS, vid SLU Bibliotek tillhandahåller stöd inom både lagring och publicering av forsknings- och miljödata och har upprättat en mall för datahanteringsplan. I nuläget är det dock endast ett fåtal institutioner som samverkar med DMS. För e-arkivering kan institutioner använda en lösning med systemen DSpace och Archivematica[10] som i nuläget har begränsad lagringskapacitet. När ett forskningsprojekt är slutfört finns behov av såväl långtidslagring som arkivering av både forskningsresultatet och underliggande data. Det finns dock behov av att tydliggöra och ta beslut om hur lösningar för långtidslagring av forsknings- och miljödata ska upprättas inom SLU för en ändamålsenlig hantering.

Hantering av forsknings- och miljödata behöver koordineras med ett flertal intressenter inom universitetet. Såväl it-avdelningen och säkerhetsenheten som biblioteket, juridikfunktionen och arkivfunktionen behöver samverka med institutionerna kring detta. I den styrgrupp som upprättades för Tilda-projektet har ett arbete påbörjats kring hur denna hantering av forsknings- och miljödata kan organiseras för hela SLU. Under januari 2022 förväntas beslut om att denna styrgrupp framåt ska leda universitets förflyttning in i ett digitalt arbetssätt för hantering av forsknings- och miljödata. Internrevisionen har även informerats om att en datahanteringspolicy för universitetet är under framtagande.

Internrevisionen bedömer att det ur ett informationssäkerhetsperspektiv finns brister i styrning, samordning och uppföljning kring hanteringen av forsknings- och miljödata. Detta ökar risken för att SLU inte uppfyller nödvändiga krav på kvalitet, spårbarhet och skydd av denna information.

Internrevisionen rekommenderar universitetsledningen att överväga

I. att det upprättas en organisation (att en verksamhet ges ansvaret) för styrning av hur forsknings- och miljödata hanteras. Organisationen/verksamheten bör ha i uppgift att ge institutionerna stöd och support samt tillhandahålla centrala lagringslösningar, åtminstone för långtidsarkivering av slutförda forskningsprojekt.

4.6 Skydd av nätverk, system och it-infrastruktur

Det saknas ändamålsenliga skyddsåtgärder avseende nätverk, system och it-infrastruktur vilket ökar risken för att säkerhetsincidenter och driftstörningar uppstår samt att dessa inte upptäcks eller kan hanteras i tid.

SLU har en relativt låg mognadsgrad kring it-säkerhet och det finns väsentliga brister inom såväl de tekniska skyddsåtgärderna som den organisatoriska förmågan

[10] Tillhandahålls av Arkiv, informationshantering och registratur (AIR), Ledningskansliet

i form av arbetssätt och rutiner för att skydda universitetets information. SLU saknar en tydlig struktur för att bedöma vilket skydd som är nödvändigt för såväl enskilda informationssystem som för it-infrastrukturen och nätverket i sin helhet. I styrdokumentet Skyddsåtgärder utifrån informationssäkerhetsklassning (2015) finns definierade it-säkerhetskrav men dokumentet bedöms inte väl förankrat och svårt att nyttja i praktiken då informationsklassning i stor utsträckning saknas. Flera av de krav som ställs efterlevs inte i praktiken och det finns inget uttalat ansvar för uppföljning av kraven.

Även om stora brister finns inom såväl den tekniska som den organisatoriska förmågan att upprätthålla en god it-säkerhet så pågår det flera initiativ och förbättringsaktiviteter inom it-avdelningen. Som nämnts tidigare ska en omfattande förstudie genomföras för att kartlägga vilka åtgärder SLU bör vidta för att upprätthålla hög säkerhet i AD:t och prioritera samt kostnadssätta skyddsåtgärder utifrån MSB:s krav samt det systematiska säkerhetsarbetet. Det har genomförts externa utredningar kring informations- och it-säkerhet. It-säkerhetsfunktionen har också påbörjat en intern gapanalys för it-avdelningen gentemot ramverket CIS Controls (Center of Internet Security) som en utgångspunkt för sitt förbättringsarbete kring it-säkerhet. Det samarbete som utvecklats mellan it-avdelningen och säkerhetsenheten ger bättre förutsättningar för att skapa tydligare säkerhetsfokus inom it-avdelningens processer.

Internrevisionen bedömer att avsaknaden av ändamålsenliga skyddsåtgärder ökar risken för att säkerhetsincidenter och driftstörningar uppstår samt att dessa inte upptäcks eller kan hanteras i tid.

Internrevisionen rekommenderar universitetsledningen att säkerställa

J. att åtgärdsplan med tydliga prioriteringar upprättas utifrån gapanalysen gentemot CIS Controls samt utifrån rekommendationer i andra externa utredningar som omfattar tydliga målsättningar för att öka SLU:s mognadsgrad inom it-säkerhet och uppgifter om hur lämpliga skyddsåtgärder ska utformas. Detta bör synkroniseras med den pågående förstudien avseende skyddsåtgärder.

4.7 Rapportering av säkerhetspåverkande it-incidenter

En riktlinje för rapportering av säkerhetspåverkande it-incident (2016) finns upprättad. Enligt riktlinjen ska it-avdelningen rapportera säkerhetspåverkande incidenter till MSB. Säkerhetschefen och it-direktören har dock kommit överens om att det är säkerhetschefen som ska rapportera till MSB. It-avdelningen ska rapportera säkerhetspåverkande incidenter till CERT[11] och till säkerhetschefen som i sin tur gör en bedömning utifrån MSB:s definierade kriterier och mall. Den senast

[11] Computer Emergency Response Team vid MSB som stöttar myndigheter vid it-incidenter

inträffade säkerhetsrelaterade it-incidenten diskuterades med MSB vilket resulterade i att det inte bedömdes som nödvändigt med en rapportering.

4.8 Överföring av uppgifter till tredje land

Informationen om vilka molntjänster som är tillåtna inom SLU är bristfällig. En otillräcklig uppföljning och kontroll kring nyttjandet av molntjänster ökar risken för otillbörlig överföring av personuppgifter till länder utanför EU, vilket strider mot dataskyddsförordningen.

EU-domstolen avkunnade i juli 2020 en dom rörande överföring av personuppgifter till tredje land, den s.k. Schrems II-domen[12]. Detta har medfört problem med överföring av personuppgifter till tredje land vilket även noterades vid internrevisionens granskning Hantering av dataskyddsförordningen. Internrevisionen har noterat att det finns information på medarbetarwebben om hur man inom SLU ska agera vid överföring av personuppgifter.

Användandet av molntjänster är ett känt och svårhanterat problemområde som bl.a. belysts i internrevisionens granskningen Säker fillagring, säkert arkiv. Det är viktigt att kunna erbjuda molnlösningar där personuppgifter och annan information hanteras säkert. Molntjänsterna är attraktiva för framförallt SLU:s forskare som har många och omfattande globala forskningssamarbeten. Flera av de molntjänster som tidigare bedömts vara godkända inom SLU är efter Schrems II-domen att betrakta som otillåtna ur ett säkerhetsperspektiv. Vid intervjuer vid internrevisionens granskning av dataskyddsförordningen framgick att kunskapen och informationen om vilka molntjänster som är tillåtna är bristfällig. IT-avdelningen gjorde i en mätning under hösten 2020 och identifierade en stor mängd olika externa nätverkstjänster som nyttjades från SLU:s interna nätverkstjänst. Dropbox var den mest förekommande molntjänsten. Även om tjänsten inte är tillåtet bedöms det som mycket svårt att tillämpa regelverket vid internationella forskningssamarbeten eftersom Dropbox ofta anses som en standard. Av de centrala system som nyttjas av SLU är Microsoft Teams ett exempel på system som skulle kunna innebära otillåten överföring till USA. Enligt uppgift har lösningar för att hantera Schrems-II-domen utretts under hösten 2021 av en sektorgemensam arbetsgrupp som dock inte kommit fram till någon gemensam lösning.

Det finns en stor osäkerhet kring i vilken utsträckning SLU nyttjar tjänster där informationen riskerar att överföras till länder som saknar ändamålsenligt dataskydd. Det finns en otydlighet i ansvar för styrning och uppföljning kring nyttjandet av molntjänster. Det har inte heller gjorts någon formell konsekvensanalys och åtgärdsplan för de tjänster som är kända. Det är enligt internrevisionens bedömning viktigt att hitta säkra, smidiga lösningar att erbjuda

[12] Schrems II-domen – En EU-dom kring ändrade förutsättningar för tredjelandsöverföringar för laglig överföring av personuppgifter till USA och andra länder utanför EU.

framförallt forskare då mycket av SLU:s forskningssamarbeten sker globalt där material skickas/delas via molntjänster.

Internrevisionen bedömer att en otillräcklig uppföljning och kontroll kring nyttjandet av molntjänster ökar risken för otillbörlig överföring av personuppgifter till länder utanför EU och därmed är i strid med dataskyddsförordningen. Om information innehåller personuppgifter och behandlas felaktigt kan det också leda till att forskningen inte kan publiceras.

Internrevisionen rekommenderar universitetsledningen att överväga

K. att en kartläggning genomförs både centralt och lokalt kring vilka leverantörer och tjänster som SLU nyttjar där information riskerar att överföras till länder som saknar ändamålsenligt dataskydd. För dessa bör en konsekvensanalys genomföras och en åtgärdsplan tas fram.

L. att besluta om vilka molntjänster som kan nyttjas av verksamheten på ett säkert och lagenligt sätt.

Inga Astorsdotter
Internrevisionschef

Lisbeth Sundkvist Johansson
Internrevisor

Sveriges lantbruksuniversitet
Swedish University of Agricultural Sciences

Internrevisionen

ÅTGÄRDSPLAN SLU ID:ua 2021.1.1.2-2665

2022-02-04

Rektors åtgärdsplan till internrevisionens rapport Informations- och it-säkerhet

Nr	**Noterade brister** (internrevisionen fyller i)	**Rekommendation** (internrevisionen fyller i)	**Åtgärd** (ledning/verksamhet fyller i)
A	Det finns brister i underhåll och förankring av styrdokumenten som ökar risken för att SLU:s information hanteras på ett olämpligt sätt. Detta kan leda till brister i tillgänglighet och skydd av informationen.	Att universitetsledningen säkerställer att styrande dokument i form av policyer, riktlinjer och instruktioner avseende informationssäkerhet och it-säkerhet utvärderas, uppdateras och tillgängliggörs.	**Ansvarig avdelning/enhet:** Avd. för SSM (för informations-säkerhetsområdet) och IT avdelningen (för IT-säkerhetsområdet). ☒ Åtgärdas enligt rekommendation ☐ Åtgärdas på annat sätt, ange vilket under kommentar nedan ☐ Åtgärdas inte, ange varför under kommentar nedan **Kommentar:** Arbetet redan påbörjat. Uppdatering av dokumenten pågår kontinuerligt. **Åtgärdas senast:** Uppdatering (i en första omgång) klar till 2022-06-30 **Dokumentation** (om det ej framgår ovan)**:**

B	Samverkan avseende informationssäkerhet är bristfällig mellan centrala stödfunktioner.	Att universitetsledningen överväger att det upprättas ett formellt råd inom informationssäkerhetsområdet för styrning och samordning, där förslagsvis it-avdelningen (it-säkerhet), säkerhetsenheten (informationssäkerhet), ledningskansliet (dataskydd samt arkivfunktion), biblioteket samt forsknings- och utbildningsverksamheten är representerade. Rådets syfte och mandat liksom motparter på ledningsnivå för rapportering och beslutsfattande bör tydligt definieras.	**Ansvarig avdelning/enhet:** Ledningskansliet med stöd av Avd. för SSM och IT-avdelningen. ☐ Åtgärdas enligt rekommendation ☒ Åtgärdas på annat sätt, ange vilket under kommentar nedan ☐ Åtgärdas inte, ange varför under kommentar nedan **Kommentar:** Arbete med att ta fram ett förslag till en samordningsgrupp är påbörjad och hanteras av ledningskansliet. En viktig uppgift för gruppen är att se över nya IT-system utifrån IT-säkerhets-, informationssäkerhets- och GDPR-perspektiv. En viktig förutsättning för gruppens arbete kommer vara att den har tillgång till alla IT-system i organisationen. SLU har i likhet med många andra lärosäten en decentraliserad IT-verksamhet, där inköp och konstruktion av programvaror sker inte bara centralt utan även ute på institutioner/motsv. För att gruppen ska kunna arbeta effektivt måste även IT-verksamheten vid institutioner/motsv kunna granskas. Det kan fö nämnas att ett flertal universitet har infört eller planerar att införa en mer central styrning av inköp och konstruktion av programvaror pga. säkerhetsaspekter. Givet ökade de högre kraven på säkerhet och ökande säkerhetshoten finns anledning att göra en generell översyn och ett ställningstagande kring IT-organisationen vid universitetet som helhet. För att säkerhetshot mm ska kunna hanteras så finns sannolikt behov av en mer strikt styrning av IT-verksamheten. Denna fråga behöver utredas.

			Åtgärdas senast: Förslag till etablering av central samordningsgrupp för IT-, informationssäkerhetsfrågor bör vara klar senast 2022-04-01. Utredning/översyn av hur mandat och roller kring IT-verksamheten inom universitetet ska fördelas för att garantera säkerhets- och GDPR-aspekter bör ske och vara klar senast 2022-12-31. Dessa två åtgärder sker parallellt med andra prioriterade åtgärder inom IT-säkerhetsområdet, främst den speciella säkerhetsöversyn som sker inom IT-infrastrukturprojektet samt översynen av AD-protokollet. **Dokumentation** (om det ej framgår ovan)**:**

C	Roller och ansvar på institutionsnivå avseende informations- och it-säkerhet är inte tydligt definierade. Bristande involvering och styrning av informationssäkerhet på institutionsnivå ökar risken för att SLU drabbas av driftstörningar, förlust av data eller cyber-attacker.	Att universitetsledningen överväger att utreda möjligheten att utforma en roll som informationssäkerhetssamordnare som en obligatorisk administrativ roll på institutioner/motsvarande. Rollen bör omfatta ett samordningsansvar för frågor kring informationssäkerhet, it-säkerhet och dataskydd.	**Ansvarig avdelning/enhet:** Universitetsdirektör i samråd med SSM ☐ Åtgärdas enligt rekommendation ☒ Åtgärdas på annat sätt, ange vilket under kommentar nedan ☐ Åtgärdas inte, ange varför under kommentar nedan **Kommentar:** Förslaget om en ny administrativ roll är enligt ledningens mening inte effektiv, eftersom detta är en specialistroll som kräver mycket goda kunskaper i informationshantering och informationssäkerhet. Sådan kompetens är normalt sett svår att rekrytera in på institutionsnivå. Ledningen förordar istället en satsning på en starkare central informationssäkerhetsfunktion som kan arbeta utåt mot institutioner och fakulteter i enlighet med punkt D nedan. Rimligen bör den föreslagna samordningsgruppen enligt B ovan kunna vara en del av ett sådant system. De nuvarande innehavarna av den administrativa säkerhetsrollen kan fungera som kontaktpersoner på institutionsnivå mot en förstärkt central informationssäkerhetsenhet. **Åtgärdas senast:** Frågan klargörs inom ramen för de översyner/utredningar som föreslås ske i B och D. Det finns ett uppenbart behov av att stärka informationssäkerhetsfunktionen oavsett vad de föreslagna översynerna i B och D resulterar i och ett arbete med detta bör påbörjas redan nu. **Dokumentation** (om det ej framgår ovan)**:**

D	Central koordinering kring strategiska och taktiska informationssäkerhetsfrågor är bristfällig. Tillsammans med otillräcklig samverkan ökar detta risken för att förbättringsåtgärder inte prioriteras eller att de fördröjs. Avsaknad av en tydlig motpart på institutionsnivå försvårar den centrala säkerhetsenhetens och it-avdelningens möjlighet att nå ut och samverka kring informationssäkerhetsfrågor.	Att universitetsledningen överväger att en utvärdering görs kring möjligheterna att tillsätta centralt finansierade informationssäkerhetsspecialister (förslagsvis en per fakultet) med uppgift att koordinera, samverka och stötta i arbetet med informationssäkerhet ute i forsknings- och utbildningsverksamheten på institutionsnivå.	**Ansvarig avdelning/enhet:** Avd. för SSM med stöd av IT-avdelningen och ledningskansliet. ☐ Åtgärdas enligt rekommendation ☒ Åtgärdas på annat sätt, ange vilket under kommentar nedan ☐ Åtgärdas inte, ange varför under kommentar nedan **Kommentar:** Behovet av ökat stöd till fakulteter och institutioner och även stödfunktioner inom universitetet är tydligt. Som framgår av C ovan anser ledningen att bäst effekt kan uppnås med inte bara centralt finansierade utan även centralt placerade specialister som stöttar fakulteter och institutioner. **Åtgärdas senast:** En utredning/översyn bör göras av inriktning och omfattning för informationssäkerhetsarbetet vid universitetet. Den ska täcka rekommendationerna C, D, E, F och G. Klar senast 2022-12-31. **Dokumentation** (om det ej framgår ovan)**:**

E	Ett ledningssystem för informationssäkerhet finns upprättat i form av policy, riktlinjer och instruktioner på området. Det saknas däremot roller, mandat, struktur och styrning.	Att universitetsledningen säkerställer att det upprättas tydliga roller, mandat, struktur och styrning av informationssäkerhet för att med ett systematiskt och riskbaserat arbetssätt införa, följa upp och åtgärda nödvändiga skyddsåtgärder, exempelvis i form av riskanalyser och informationsklassningar.	**Ansvarig avdelning/enhet:** Avd. för SSM ☒ Åtgärdas enligt rekommendation ☐ Åtgärdas på annat sätt, ange vilket under kommentar nedan ☐ Åtgärdas inte, ange varför under kommentar nedan **Kommentar:** Den grundläggande strukturen och systematiken i informationssäkerhetsarbetet finns, men den har ännu inte utvecklats och anpassats fullt ut till gällande krav och förutsättningar. Exempelvis behöver roller och mandat enligt MSB:s regelverk klargöras tydligare. **Åtgärdas senast:** 2022-12-31. Ingår som en del i utredningen enl. punkt D ovan. **Dokumentation** (om det ej framgår ovan)**:**

F	Det görs återkommande rapporteringar av arbetet med it-säkerhet till rektor och universitetsdirektör. Det saknas däremot en strukturerad uppföljning och rapportering om informationssäkerheten på universitetet.	Att universitetsledningen säkerställer att rutiner upprättas för regelbunden rapportering till universitetsledningen om informations- och it-säkerhetsarbetet samt om identifierade hot och risker inom området. Se över möjligheten att samordna detta med rekommendation B.	**Ansvarig avdelning/enhet:** Avd. för SSM med IT avdelningen och ledningskansliet ☒ Åtgärdas enligt rekommendation ☐ Åtgärdas på annat sätt, ange vilket under kommentar nedan ☐ Åtgärdas inte, ange varför under kommentar nedan **Kommentar:** Etablering av rutiner för kontinuerlig rapportering och uppföljning till myndighetsledningen har påbörjats i enlighet med gällande före-skrifter. I samband med att en samordningsgrupp etableras enligt B ovan så bör övervägas om en samlad avrapportering till myndighetsledningen kan ske via den gruppen. **Åtgärdas senast:** 2022-12-31 **Dokumentation** (om det ej framgår ovan)**:**

G	Utbildningsformen ”nano-learning” har upplevts positiv och är något som efterfrågas igen. Någon riktad utbildning mot kritiska roller såsom informationsägare och systemägare har inte genomförts.	Att universitetsledningen säkerställer att kortare web-utbildningar i informationssäkerhet, s.k. nano-learning, regelbundet riktas till samtliga anställda, samt att specialanpassade återkommande informationssäkerhetsutbildningar tillhandahålls till systemägare, informationsägare, systemförvaltare och andra nyckelroller (se rekommendation C).	**Ansvarig avdelning/enhet:** Avd. för SSM ☒ Åtgärdas enligt rekommendation ☐ Åtgärdas på annat sätt, ange vilket under kommentar nedan ☐ Åtgärdas inte, ange varför under kommentar nedan **Kommentar:** Behovet av olika typer av utbildning är sedan tidigare identifierat och har genomförts i viss omfattning, dock inte i den utsträckning och takt som bedöms nödvändigt. **Åtgärdas senast:** 2022-12-31 (omfattas av utredningen enl. punkt D) **Dokumentation** (om det ej framgår ovan)**:**

H	Det finns information och system som inte har klassats och därmed saknar en tydlig bedömning av hur informationen ska hanteras och skyddas. Detta innebär en förhöjd risk för brister i tillgänglighet, datakvalitet och säkerhet.	Att universitetsledningen säkerställer att informationsklassning genomförs för relevanta klassningsobjekt såsom projekt, lagringsytor och system inom hela SLU:s verksamhet samt att stöd och mallar för informationsklassning kommuniceras och följs upp.	**Ansvarig avdelning/enhet:** Avd. för SSM med stöd av IT-avdelningen och ledningskansliet ☒ Åtgärdas enligt rekommendation ☐ Åtgärdas på annat sätt, ange vilket under kommentar nedan ☐ Åtgärdas inte, ange varför under kommentar nedan **Kommentar:** Detta arbete bör prioriteras för de system som förvaltas centralt vid universitetet. Men för att genomförandet av klassningar ska kunna ske fullt ut krävs att universitetet centralt har kontroll på vilka system och projekt som existerar även ute i kärnverksamheten (i enlighet med den föreslagna översynen i punkt B). Frågan har även en direkt koppling till säkerhetsskyddsområdet, där informationssäkerheten är en viktig del. Informationsklassning av system bör rimligen vara en uppgift som läggs på den i punkt B föreslagna samordningsgruppen. Vidare bör rutiner för informationssäkerhetsklassning och GDPR-hantering också vara del av universitetets gemensamma systemförvaltningsmodell. **Åtgärdas senast:** 2023-06-01 **Dokumentation** (om det ej framgår ovan)**:**

I	Det finns brister i styrning, samordning och uppföljning kring hanteringen av forsknings- och miljödata. Ur ett informationssäkerhetsperspektiv ökar detta risken för att SLU inte uppfyller nödvändiga krav på kvalitet, spårbarhet och skydd av denna information.	Att universitetsledningen överväger att det upprättas en organisation (att en verksamhet ges ansvaret) för styrning av hur forsknings- och miljödata hanteras. Organisationen/verksamheten bör ha i uppgift att ge institutionerna stöd och support samt tillhandahålla centrala lagringslösningar, åtminstone för långtidsarkivering av slutförda forskningsprojekt.	**Ansvarig avdelning/enhet:** DMS med stöd av IT-avdelningen ☐ Åtgärdas enligt rekommendation ☒ Åtgärdas på annat sätt, ange vilket under kommentar nedan ☐ Åtgärdas inte, ange varför under kommentar nedan **Kommentar:** Arbetet med att strukturera upp och samordna hanteringen av forsknings- och miljödata har pågått vid SLU under flera års tid, ursprungligen i det sk Tildaprojektet. Uppgiften har varit och är fortfarande en stor utmaning och den har inte har fått sin lösning fullt ut. En central funktion, DMS, finns etablerad vid universitetsbiblioteket och arbetet styrs på central nivå via en särskild arbetsgrupp för e-infrastruktur under ledning av vicerektor för samverkan och fortlöpande miljöanalys tillsammans med berörda chefer vid gemensamma verksamhetsstödet och biblioteket. Samverkan och benchmarking sker också med andra lärosäten och SND. Detta eftersom en systematisk forsknings- och miljödatahantering är en strategisk utmaning inte bara för SLU utan för hela högskolesektorn, och det är mycket svårt att ange en tidpunkt för när den skulle kunna vara tillfredsställande löst. Den av vicerektor ledda arbetsgruppen har dock tagit fram ett utkast för beslut för ett utvecklingsprogram på datahanteringsområdet som är tänkt att fastställas av rektor efter förankring i organisationen. I programmet finns förslag för en framtida organisation och utvecklingsaktiviteter. IT-avdelningen har rekryterad en förvaltningsledare för datahanteringsområdet som påbörjar sin tjänst 1 februari. **Åtgärdas senast:** Rektorsbeslut senast 2022-04-01. **Dokumentation** (om det ej framgår ovan)**:**

J	Det saknas ändamålsenliga skyddsåtgärder avseende nätverk, system och it-infrastruktur vilket ökar risken för att säkerhetsincidenter och driftstörningar uppstår samt att dessa inte upptäcks eller kan hanteras i tid.	Att universitetsledningen säkerställer att åtgärdsplan med tydliga prioriteringar upprättas utifrån gapanalysen gentemot CIS Controls samt utifrån rekommendationer i andra externa utredningar som omfattar tydliga målsättningar för att öka SLU:s mognadsgrad inom it-säkerhet och uppgifter om hur lämpliga skyddsåtgärder ska utformas. Detta bör synkroniseras med den pågående förstudien avseende skyddsåtgärder.	**Ansvarig avdelning/enhet:** IT-avdelningen med stöd av Avd. för SSM. ☒ Åtgärdas enligt rekommendation ☐ Åtgärdas på annat sätt, ange vilket under kommentar nedan ☐ Åtgärdas inte, ange varför under kommentar nedan **Kommentar:** Åtgärdsplan utifrån gapanalys är del av den större förstudie för IT-säkerhet som görs som del av programmet för ny IT-infrastruktur (som presenterades för styrelsen i september 2021). **Åtgärdas senast:** Åtgärdsplanen med prioriteringar utifrån gapanalys klar 2022-08-31. **Dokumentation** (om det ej framgår ovan)**:**

K	Uppföljning och kontroll av nyttjandet av molntjänster är otillräcklig. Detta ökar risken för otillbörlig överföring av personuppgifter till länder utanför EU, vilket strider mot dataskyddsförordningen.	Att universitetsledningen överväger att en kartläggning genomförs både centralt och lokalt kring vilka leverantörer och tjänster som SLU nyttjar där information riskerar att överföras till länder som saknar ändamålsenligt dataskydd. För dessa bör en konsekvensanalys genomföras och en åtgärdsplan tas fram.	**Ansvarig avdelning/enhet:** Ledningskansliet/Enheten för juridik i samverkan med IT-avdelningen och inköpsenheten ☐ Åtgärdas enligt rekommendation ☒ Åtgärdas på annat sätt, ange vilket under kommentar nedan ☐ Åtgärdas inte, ange varför under kommentar nedan **Kommentar:** Denna åtgärd har redan påbörjats för de system som förvaltas centralt vid SLU. Men för att kartläggning ska kunna ske fullt ut krävs att universitetet centralt har kontroll på vilka system och projekt som existerar även ute i kärnverksamheten (i enlighet med den föreslagna översynen i punkt B). Uppgiften kan läggas på den föreslagna samordningsgruppen enligt punkt B, men kräver ett aktivt deltagande från kärnverksamheten för att säkerställa att forskningens behov inte hämmas. **Åtgärdas senast:** 2023-06-01 **Dokumentation** (om det ej framgår ovan)**:**

L	Molntjänster som tidigare bedömts vara godkända inom SLU är efter Schrems II-domen att betrakta som otillåtna ur ett säkerhetsperspektiv. Informationen om vilka molntjänster som är tillåtna inom SLU är bristfällig.	Att universitetsledningen överväger att besluta om vilka molntjänster som kan nyttjas av verksamheten på ett säkert och lagenligt sätt.	**Ansvarig avdelning/enhet:** Ledningskansliet/Enheten för juridik i samverkan med IT-avdelningen och inköpsenheten ☐ Åtgärdas enligt rekommendation ☒ Åtgärdas på annat sätt, ange vilket under kommentar nedan ☐ Åtgärdas inte, ange varför under kommentar nedan **Kommentar:** Beslut kring vilka molntjänster som kan nyttjas måste ske löpande, eftersom rättsläget är osäkert och grunderna för IT-systemens kompabilitet med GDPR-lagstiftningen förändras hela tiden, tex med nya tekniska lösningar. Inledningsvis behöver ställning tas till hur universitetet ska förhålla sig till nuvarande situation och ett övergripande beslut fattas om hur molntjänster ska hanteras på ett säkert sätt. Som framgår av internrevisionens rapport har en högskolegemensam utredningsgrupp försökt hitta rekommendationer till hantering av Schrems II domen men inte lyckats. Detta bör kunna vara en uppgift för den i B föreslagna samordningsgruppen. **Åtgärdas senast:** 2022-12-31 **Dokumentation** (om det ej framgår ovan)**:**