DNR: SLU ua 2014.1.1.2-841
Exp. den: 2014-06-___

Sveriges lantbruksuniversitet
Swedish University of Agricultural Sciences

Styrelsen

BESLUT
2014-06-17

Sändlista

Granskning av informationssäkerhet

Styrelsen beslutar:

att fastställa internrevisionens rapport Informationssäkerhet, samt

att fastställa rektors åtgärdsplan med anledning av rapporten.

Ärendet

I mars – april 2014 har internrevisionen genomfört en granskning av informationssäkerheten vid SLU med avseende på ändamålsenlighet och effektivitet i organisation, styrning, ledning och uppföljning. Granskningen har genomförts av Roger Karlsson KPMG AB. Sammanfattningsvis bedömer internrevisionen att kvaliteten i arbetet bör förbättras för att säkerställa effektivitet, ändamålsenlighet samt god intern styrning och kontroll.

Åtgärdsplanen har utarbetats av universitetsdirektör Martin Melkerson. I beredningen av ärendet har informationssäkerhetschef Anette Lindberg samt säkerhetschef Per-Olov Skatt deltagit.

Beslut i detta ärende har fattats av styrelsen efter föredragning av universitetsdirektör Martin Melkersson.

Rolf Eriksson Brennerfelt

Martin Melkersson

Kopia för kännedom

Prorektor
Dekanerna
Universitetsdirektören
Avdelningschefer (motsv.) inom universitetsadministrationen

P.O Box 7070 SE-750 07 Uppsala, Sweden.
Besök/visits: Adressgatan 123.
www.slu.se/xxx

tel: +46 (0)18-67 10 00
mob: +46 (0)703-21 21 95
namn.efternamn@slu.se

Sveriges lantbruksuniversitet
Swedish University of Agricultural Sciences

Internrevisionen

DNR: SLU ua 2014.1.1.2-841

Informationssäkerhet

Rapport från internrevisionen

Innehåll

Sammanfattning

Det är väsentligt att SLU har en väl fungerande process för informationssäkerhet. Tidigare granskningar har indikerat att arbetet med informationssäkerhet kan förbättras. Internrevisionen har granskat universitets processer för informationssäkerhet med avseende på ändamålsenlighet och effektivitet i organisation, styrning, ledning och uppföljning.

De väsentligaste iakttagelserna är följande:

1. Det interna regelverket har bristande struktur och följer inte gällande föreskrifter.
2. Ansvar för IT- och informationssäkerhet är otydligt.
3. Modellen för informationssäkerhetsklassificering riskerat bli alltför omfattande och det saknas regler för hantering av klassad information.

Sammanfattningsvis bedömer internrevisionen att kvaliteten i arbetet bör förbättras för att säkerställa effektivitet, ändamålsenlighet samt god intern styrning och kontroll.

De väsentligaste rekommendationerna är följande:

1. Att arbetet med informationssäkerhet följer Myndigheten för samhällsskydd och beredskaps (MSB) föreskrifter.
2. Strukturera styrande dokument så att de ger bättre möjligheter för effektiv och ändamålsenlig ledning, styrning och uppföljning.
3. Att Avdelning för infrastrukturs och IT-avdelningens ansvar och mandat tydliggörs.
4. Att ledningen minst årligen erhåller skriftlig rapportering om arbetet med informationssäkerhet.
5. Utvärdera befintlig modell för informationssäkerhetsklassning avseende tillämpning, effektivitet och ändamålsenlighet
6. Att verksamheten får kunskap om informationssäkerhetsklassificering.
7. Utarbeta styrande dokument för hur information ska skyddas beroende på resultat av informationssäkerhetsklassificering.

1. Bakgrund och motiv

Informationssäkerhet är ett samlingsbegrepp på åtgärder som syftar till att undvika, förhindra eller försvåra förlust, skada, eller obehörig åtkomst av information och data. Begreppet informationssäkerhet är ett vitt begrepp som omfattar all typ av information; muntlig, tryckt eller elektronisk.

Ett effektivt och ändamålsenligt informationssäkerhetsarbete är ett viktigt stöd till verksamheten att minska risker och nå sina mål med god intern kontroll. Svagheter i dessa rutiner kan leda till att informationen har bristande tillgänglighet, riktighet och att kraven på sekretess och spårbarhet blir åsidosatta. Risk finns även att ärenden hamnar ”mellan stolarna” och inte utförs alls eller att samma typ av ärende hanteras på olika sätt inom organisationen. Risk finns även för nyckelpersonberoende.

2. Granskningens omfattning och inriktning

Målet med granskningen har varit att bedöma om informationssäkerhetsarbetet organiseras, styrs och följs upp effektivt och ändamålsenligt.

Denna rapport sammanfattar de observationer och rekommendationer som internrevisionen gjort inom ramen för denna granskning. Rapporten är av formatet avvikelserapport varför förhållanden som bedömts fungera tillfredsställande inte omnämns.

Granskningen har primärt omfattat IT-baserad information.

3. Externt regelverk

Myndigheten för samhällsskydd och beredskap har i sina föreskrifter om statliga myndigheters informationssäkerhet” (MSBFS 2009:10) föreskrivit hur statliga myndigheter ska arbeta med informationssäkerhet.

Av föreskrifterna framgår att en myndighet ha ett ledningssystem för informationssäkerhet. Det innebär att myndigheten ska upprätta en informationssäkerhetspolicy och andra styrande dokument som behövs för myndighetens informationssäkerhet. Det ska utses en eller flera personer som leder och samordnar arbetet med informationssäkerhet. Myndigheten ska klassificera sin information med utgångspunkt i krav på konfidentialitet, riktighet och tillgänglighet. Myndigheten ska även utifrån risk- och sårbarhetsanalyser och inträffade incidenter avgöra hur risker ska hanteras, samt dessutom besluta om åtgärder för informationssäkerhet.Granskningar och säkerhetsåtgärder av större betydelse ska dokumenteras.

Informationssäkerhetsarbetet ska enligt bedrivas enligt Ledningssystem för informationssäkerhet (ISO 27001) och Riktlinjer för styrning av informationssäkerhet (ISO 27002).

Av föreskrifterna framgår även att myndighetens ledning löpande ska informera sig om arbetet med informationssäkerhet samt minst en gång per år följa upp och utvärdera informationssäkerhetsarbetet på myndigheten. [1]

4. Internt regelverk

Det interna regelverket har bristande struktur och följer inte MSB:s föreskrifter.

SLU har en av rektor fastställd ”Säkerhetspolicy”[2] som beskriver ansatsen för det samlade säkerhetsarbetet vid universitetet inklusive informationssäkerhet samt en ”IT-säkerhetspolicy”. I februari 2013 fastställdes riktlinjer och anvisning för Informationssäkerhetsklassning[3].

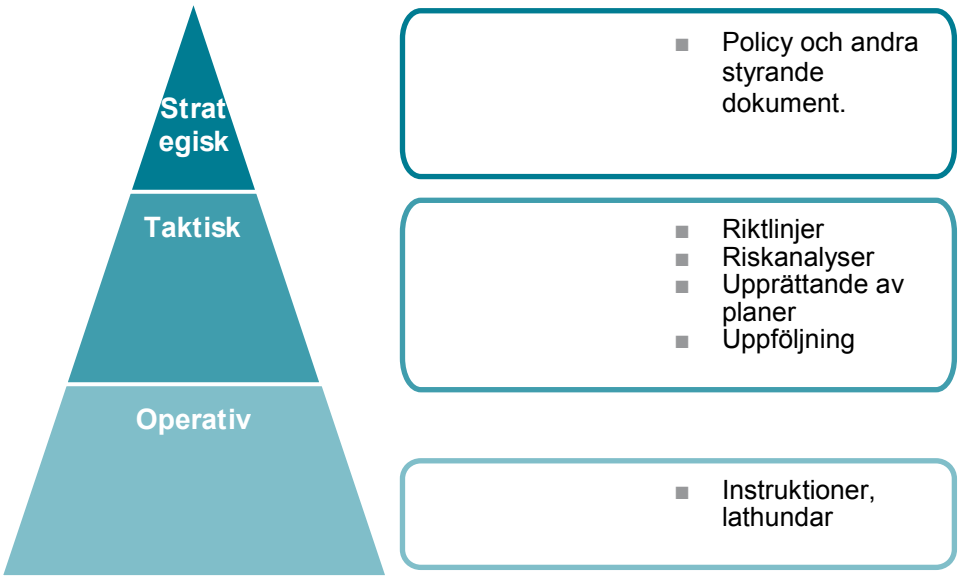
Internrevisionens granskning visar att de styrande dokumenten inte tydligt knyter an till tillämpningen av den standard som MSB beslutat ska ligga till grund för arbetet.

Vid tidpunkten för granskningen pågick ett arbete vid avdelning för infrastrukturs (Infra) enhet för Säkerhet med att utarbeta och införa ytterligare styrande dokument inom området såsom ”Riktlinjer för informationssäkerhet” och tillhörande rutiner/instruktioner/anvisningar.

Internrevisionen har tagit del av det pågående arbetet med att utveckla nya styrande dokument. Internrevisionens bedömning är att dokumenten kan göras mer stringenta för att bättre beskriva hur det strategiska, taktiska och operativa arbete ska hänga ihop. Kopplingen finns i Riktlinjer för Informationssäkerhetsklassning men då mer som hänvisning för att förklara innebörden av vissa termer.

Internrevisionen saknar en tydlig beskrivning dels av hur ramverkets olika delar hänger ihop, exempelvis enligt nedanstående figur, dels en för universitetet gemensam begreppsdefinition som fastslår vad olika begrepp betyder och ger universitetet en gemensam grund att stå på.

[1] Ledningssystem för informationssäkerhet (SS-ISO/IEC 27001: 2006 fastställd 2006-01-19) och Riktlinjer för styrning av informationssäkerhet (SS-ISO/IEC 27002:2005 fastställd 2005-08-12).
[2] SLU ua110-3557/09
[3] SLU ua 2013.2.10-650



Internrevisionen rekommenderar att universitetsledningen säkerställer att arbetet med informationssäkerhet följer MSB:s föreskrifter vilket bland annat innebär att arbetet ska drivas efter Ledningssystem för informationssäkerhet, SS-ISO/IEC 27001/27002.

Internrevisionen rekommenderar att universitetsledningen säkerställer att de styrande dokumenten struktureras så att de ger bättre möjligheter för ledning, styrning och uppföljning av informationssäkerhetsarbetet.

5. Organisation och ansvar

Ansvar för IT- och informationssäkerhet är otydligt.

Av rektorsbeslutet ”Förändrat uppdrag i säkerhetsprocessen”[4] från 2009 framgår att: ”Säkerhetsfunktionens uppdrag är att vara en övergripande funktion som ansvarar för att leda universitetets IT- och informationssäkerhetsarbete. Det operativa säkerhetsarbetet sker inte inom säkerhetsfunktionen, utan utförs i huvudsak av IT-funktionen”. Beslutet innebar bland annat att befattningen som informationssäkerhetschef flyttades från IT till Säkerhet inom Infra.

[4] SLU ua 10-3557/09 2009-12-14

Infra har enligt universitetsadministrationens verksamhetsplan ansvar för att "leda universitetets IT- och informationssäkerhetsarbete". IT-avdelningen har enligt verksamhetsplanen inget uppdrag inom IT-säkerhetsarbetet. [5]. Avdelningen har dock en resurs som arbetar med IT -säkerhet och köper motsvarande en heltidstjänst från Uppsala universitet.

Internrevisionen konstaterar att beskrivning av roller och ansvar i verksamhetsplanen är otydlig avseende vad som förväntas ske inom Infra och vad som hanteras inom IT-avdelningen. Verksamhetens syn på vem som är ansvarig för IT-säkerhet överensstämmer inte med vad som framgår av verksamhetsplanen. Detta innebär även en osäkerhet för informationssäkerhetsfunktionens roll, ansvar och mandat. Proaktivitet och uppföljning kan därmed bli eftersatt med risk för bl.a. onödiga kostnader.

Internrevisionen konstaterar att det inte skett någon systematisk och löpande återrapportering av arbetet med informationssäkerhet till ledningen, vilket ska göras enligt MSB:s föreskrifter. Den återrapportering som gjorts har skett i samband med verksamhetens budgetarbete eller på förekommen anledning. Internrevisionen har noterat att flera enheter upplever att det arbete som Infra bedriver inom informationssäkerhet är anonymt.

Internrevisionen rekommenderar att universitetsledningen säkerställer att Infras och IT-avdelningens ansvar och mandat blir tydligare.

Internrevisionen rekommenderar att universitetsledningen säkerställer att MSB:s föreskrifter följs avseende ledningens roll; att löpande hålla sig informerad om arbetet med informationssäkerhet samt att minst en gång per år följa upp och utvärdera SLU:s informationssäkerhetsarbete. Arbetet bör ske skriftligt.

Universitetet saknar en effektiv och ändamålsenlig samordning av informationssäkerhetsarbetet.

Internrevisionens granskning visar att arbetet med informationssäkerhet och nära relaterade områden som datakvalitet etc. sker på olika sätt, på olika håll och med olika resurser och organisationer inom universitetet. Internrevisionen saknar effektivitet och ändamålsenlighet i universitetets samverkan kring informationssäkerhet. Det finns en stor risk att universitetet inte återanvänder erfarenheter och metoder utan i stället gör ”samma sak” på olika håll inom organisationen. Värdefulla erfarenheter som olika enheter har gjort kommer då inte

[5] Se Uadm:s Verksamhetsplaner 2011-2014
https://internt.slu.se/sv/styrning-och-organisation/verksamhetsplanering-och-anslagsfordelning/

hela universitetet till godo. Konsekvens kan bli ökade kostnader och bristande kvalitet. Ett exempel på detta är att det inte finns en gemensam struktur för kommunikation via medarbetarportalen för informationssäkerhetsfrågor. Det finns samma typ av information på både Infra och IT-avdelningens hemsidor.

Internrevisionens granskning visar även att det inte sker någon strukturerad, systematisk och regelbunden information eller utbildning av personal och studenter avseende informationssäkerhet. Detta innebär svårigheter att etablera och kommunicera en gemensam ”lägsta” nivå i tillämpningen av säkerhetsåtgärder.

Internrevisionen rekommenderar att universitetsledningen överväger att se över hur arbetet med informationssäkerhet ska bedrivas inom universitetet, vilka olika forum som det finns behov av.

Internrevisionen rekommenderar även att universitetsledningen överväger att införa tydligare strukturer för hur information om informationssäkerhet ska kommuniceras inom universitetet. I detta sammanhang bör behovet av regelbunden och målgruppsanpassad utbildning beaktas.

6. Informationssäkerhetsklassning

Modellen för informationssäkerhetsklassificering riskerat bli alltför omfattande och det saknas regler för hantering av klassad information

I revisionsrapport 2010-02-08 framförde Riksrevisionen ett antal synpunkter på SLU:s arbete med styrning och uppföljning av universitetets informationssäkerhetsarbete. I regleringsbrev för 2013 gav regeringen SLU i uppdrag att redovisa vidtagna och planerade åtgärder för en förbättrad styrning och kontroll av myndigheten med utgångspunkt i Riksrevisionens revisionsrapport (dnr 32-2011-0632), där bland annat uppföljning av status i informationssäkerhetsarbetet ingår.

I rektors rapporten till regeringen framgår bland annat att en modell för informationssäkerhetsklassning och en införandeplan har fastställts. Informationssäkerhetsklassificering har därefter skett i ett antal analyser under 2013 och enligt rektors beslut är en utvärdering av modellen planerad att ske under 2014.

Många organisationer arbetar idag med att införa rutiner för informationssäkerhetsklassning. En av utmaningarna är att hitta ett effektivt och ändamålenligt arbetssätt för att genomföra klassificeringen utan att den är tidskrävande och tar stora resurser i anspråk. Detta sker bla genom att minska antalet säkerhetsklasser och bedömningsvariabler samt att hårt styra prioriteringen av vilka objekt som ska klassificeras.

Internrevisionen konstaterar att modellen för informationssäkerhetsklassning i huvudsak följer sk best practise inom området. Internrevisionens uppfattning är dock att antalet bedömningsvariabler kan vara för omfattande för att modellen ska vara effektiv och ändamålsenlig. Risk finns att klassificeringen blir alltför finmaskig och svåröverblickbar eftersom modellen innehåller många variabler, bland annat två lagningskriterier. Internrevisionens bedömer dessutom att riktlinjer och instruktioner inte tydligt beskriver **hur** informationen ska skyddas beroende på resultat av klassificering.

Internrevisionens granskning visar även att det är begränsat med information kring informationssäkerhetsklassning på medarbetarwebben. Detta kan medföra att delar av organisationen inte känner till att dessa metoder och modeller ska tillämpas.

Internrevisionen rekommenderar universitetsledningen säkerställer att den av rektor beslutade modellen för informationssäkerhetsklassning utvärderas. I detta sammanhang bör det övervägas om det finns behov av verksamhetsspecifika modeller för kärnverksamhet respektive administration, samt om det går att införa en gemensam basninvå för att underlätta klassificering.

Internrevisionen rekommenderar att universitetsledningen säkerställer att verksamheten får kunskap om informationssäkerhetsklassificeringen antingen via medarbetarwebben eller på annat sätt.

Internrevisionen rekommenderar även att universitetsledningen säkerställer att styrande dokument tas fram för hur informationen ska skyddas beroende på resultat av informationssäkerhetsklassificering.

7. Internrevisionens uppföljning

Internrevisionen avser följa upp lämnade rekommendationer inför internrevisionens årsrapport för 2014.

Inga Astorsdotter
Internrevisionschef

Roger Karlsson

Sveriges lantbruksuniversitet
Swedish University of Agricultural Sciences

Universitetsdirektören 2014-06-04

Åtgärdsplan med anledning av internrevisionens rapport Informationssäkerhet

Internrevisionen har reviderat informationssäkerhetsarbetet vid SLU och leverarat en rapport till styrelsen, ”Informationssäkerhet Rapport från internrevisionen” DNR: SLU ua Fe 2014.1.1.2-841. Rapporten innehåller iakttagelser inom tre bedömningsområden och varje iakttagelse kompletteras med förklarande text och av internrevisionen föreslagna rekommendationer. Internrevisionens rekommendationer redovisas nedan, kompletterade med kommentarer och förslag till åtgärder.

Internt regelverk

Internrevisionen rekommenderar att universitetsledningen:

R1 säkerställer att arbetet med informationssäkerhet följer MSB:s föreskrifter vilket bland annat innebär att arbetet ska drivas efter Ledningssystem för informationssäkerhet, SS-ISO/IEC 27001/27002.

R2 säkerställer att de styrande dokumenten struktureras så att de ger bättre möjligheter för ledning, styrning och uppföljning av informationssäkerhetsarbetet.

Kommentarer:

Det interna regelverket strider inte mot standarden men tydligare hänvisningar och kopplingar till den behövs liksom tydligare beskrivning av hur de olika dokumenten i det interna regelverket förhåller sig till varandra.

Åtgärder:

Å1 Befintliga dokumenten ska uppdateras med referens till standarden, beskrivning av inbördes förhållande samt koppling till de strategiska, taktiska och operativa nivåerna.
Ansvar: SLU Säkerhet. Klartid: 2015-06-30. Dok: i befintliga dok i regelverket.

Å2 Nya dokument ska förses med referens och tydligare koppling till standarden, beskrivning av inbördes förhållande samt koppling till de strategiska, taktiska och operativa nivåerna.
Ansvar: SLU Säkerhet. Klartid: löpande. Dok: i nya dok i regelverket.

Å3 En SLU-gemensam begreppsdefinition ska tas fram och presenteras på medarbetarweb och eventuellt biläggas fastställda riktlinjer för informationssäkerhet.
Ansvar: SLU Säkerhet. Klartid: 2014-12-31. Dok: Medarbetarwebb och eventuellt bilagd dokumentet riktlinjer för informationssäkerhet.

Organisation och ansvar

Internrevisionen rekommenderar att universitetsledningen:

R3 säkerställer att Infras och IT-avdelningens ansvar och mandat blir tydligare.

R4 säkerställer att MSB:s föreskrifter följs avseende ledningens roll; att löpande hålla sig informerad om arbetet med informationssäkerhet samt att minst en gång per år följa upp och utvärdera SLU:s informationssäkerhetsarbete. Arbetet bör ske skriftligt.

R5 överväger att se över hur arbetet med informationssäkerhet ska bedrivas inom universitetet, vilka olika forum som det finns behov av.

R6 överväger att införa tydligare strukturer för hur information om informationssäkerhet ska kommuniceras inom universitetet. I detta sammanhang bör behovet av regelbunden och målgruppsanpassad utbildning beaktas.

Kommentarer:

Tidigare var IT och SLU Säkerhet gemensamt organiserade under avdelningen för infrastruktur, vilket de inte längre är. De av rektor nyligen beslutade ”Riktlinjer för informationssäkerhet vid SLU” (ua 2014.2.10-1368) förtydligar ansvar och roller inom SLU. SLU Säkerhet ansvarar för informationssäkerhet och IT för it-säkerhet.

Rapportering till universitetsledningen har till största delen skett incidentstyrt och allmän informationssäkerhetsutbildning har hittills skett på förfrågan, vid uppsökande verksamhet eller inom specifika områden.

Åtgärder:

Å4 Kommande verksamhetsplan för universitetsadministrationen ska uppdateras med information gällande ansvar och mandat gällande informationssäkerhet och it-säkerhet.
Ansvar: Universitetsledningen. Klartid: 2014-12-31. Dok: verksamhetsplan för uadm

Å5 Årlig och skriftlig redovisning till universitetsledningen.
Ansvar: SLU Säkerhet. Klartid: 2014-12-31. Dok: SLU Säkerhets interna verksamhetsplanering och rapport skickas till universitetsledningen.

Å6 Behov av utbildning för studenter och anställda ska utredas.
Ansvar: SLU Säkerhet. Klartid: 2015-03-31. Dok: Förslag till universitetsledningen.

Å7 Det ska utreda på vilket sätt informationssäkerhetsarbetet ska bli tydligare och synligare inom organisationen.
Ansvar: Universitetsledningen. Klartid: 2014-12-31. Dok: Analys till universitetsledningen.

Informationssäkerhetsklassning

Internrevisionen rekommenderar att universitetsledningen:

R7 säkerställer att den av rektor beslutade modellen för informationssäkerhetsklassning utvärderas. I detta sammanhang bör det övervägas om det finns behov av verksamhetsspecifika modeller för kärnverksamhet respektive administration, samt om det går att införa en gemensam basninvå för att underlätta klassificering.

R8 säkerställer att verksamheten får kunskap om informationssäkerhetsklassificeringen antingen via medarbetarwebben eller på annat sätt.

R9 säkerställer att styrande dokument tas fram för hur informationen ska skyddas beroende på resultat av informationssäkerhetsklassificering.

Kommentarer:

Klassning genomförs för att värdera information utifrån tillgänglighet, riktighet och konfidentialitet. Modellen bygger på MSB:s klassningsguide i grunden och har kompletterats med en klass. Enligt föredrag av MSB kommer även deras guide att kompletteras med samma klass.

MSB kommer enligt samma föredragning att ta fram en ”skyddsmatris” som beskriver på vilket sätt det är lämpligt att skydda respektive klass alternativt de vanligaste kombinationer av klasser.

Åtgärder:

Å8 SLU:s klassningsmodell kommer att utvärderas, både genom jämförelse med andra universitet och genom undersökning av analysdeltagarnas åsikter.
Ansvar: SLU Säkerhet. Klartid: 2014-12-31. Dok: Analys.

Å9 Information om klassningsmodellen publiceras på webben efter att den är utvärderad och beslutad.
Ansvar: SLU Säkerhet. Klartid: 2014-12-31. Dok: På webben.

Å10 Planering gällande implementering av och utbildning inom klassningsområdet ska ske.
Ansvar: SLU Säkerhet. Klartid: 2014-12-31. Dok: Plan.

Å11 Det ska tas fram styrande dokument avseende skydd utifrån klassning med MSB:s kommande skyddsmatris som grund.
Ansvar: SLU Säkerhet. Klartid:2015-03-31. Dok: Eget dokument.

Å12 Möjlighet till gemensam basnivå för klassning utreds.
Ansvar: SLU Säkerhet. Klartid: 2015-03-31. Dok: Analys.