Sveriges lantbruksuniversitet
Swedish University of Agricultural Sciences

Styrelsen

BESLUT

SLU ID: SLU.ua-2019.1.1.2-963

2019-09-26

Rektor

Behörighetshantering

Beslut

Styrelsen beslutar

att lägga internrevisionens rapport Behörighetshantering till handlingarna samt

att fastställa rektors åtgärdsplan med anledning av rapporten.

Ärendet

Internrevisionen har i enlighet med revisionsplanen för 2019 granskat SLU:s Behörighetshantering. Internrevisionens sammanfattande bedömning är att hanteringen av behörigheter och attester kan förbättras. Det finns brister som riskerar att påverka styrning och säkerhet vilket kan innebära risk för att obehöriga får tillgång till information och att väsentlig information kan ändras, spridas eller tas bort. Med anledning av detta har ett antal rekommendationer lämnats. Av rektors åtgärdsplan, bilaga 2, framgår vilka åtgärder som ledningen bedömer bör vidtas med anledning av detta.

Beslut i detta ärende har fattats av styrelsen efter föredragning av internrevisor Lisbeth Sundkvist Johansson. Åtgärdsplanen har i huvudsak beretts av IT-direktör Petra Lagerkvist.

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 universitetsadministrationen
Universitetdjursjukhusdirektör
Överbibliotekarie

Sveriges lantbruksuniversitet
Swedish University of Agricultural Sciences

Internrevisionen

SLU ID: SLU.ua 2019.1.1.2-963

2019-08-28

Behörighetshantering

Rapport från internrevisionen

Postadress: Box 7086, 750 07 Uppsala
Besöksadress: Almas allé 8
Org nr: 202100-2817
www.slu.se

Tel: 018-67 10 00 (vx)

Lisbeth.sundkvist.johansson@slu.se

Innehåll

1 Sammanfattning

Internrevisionen har i enlighet med revisionsplanen för 2019 granskat behörighetshantering. Syftet med granskningen har varit att bedöma om hanteringen av behörigheter är effektiv, ändamålsenlig och bedrivs med tillfredsställande kontroll och säkerhet. Granskningen har omfattat fem administrativa system; Idis, Proceedo, Agresso, Primula och Lins.

Internrevisionens sammanfattande bedömning är att hanteringen av behörigheter och attester kan förbättras. Det finns brister som riskerar att påverka styrning och säkerhet vilket kan innebära risk för att obehöriga får tillgång till information och att väsentlig information kan ändras, spridas eller tas bort. Internrevisionens bedömning grundar sig i huvudsak på följande;

- Det saknas styrande dokument för behörighetshantering på övergripande nivå vilket ökar risken för felaktig och avvikande hantering av behörigheter.
- Roller för systemägare och systemansvariga är inte tydliggjorda på en övergripande nivå vilket kan innebära ett otydligt ansvar för respektive system.
- Det finns brister i kontrollen över tilldelade behörigheter och det sker ingen bedömning av behovet av titt-behörigheter. Detta kan leda till att obehöriga får tillgång till uppgifter samt att känsliga uppgifter kan spridas.
- Det saknas dokumenterade rutiner för uppföljning/inventering av behörigheter och attester. Uppföljning av behörigheter sker inte regelbundet eller inte alls.

De väsentligaste rekommendationerna är;

- Att övergripande styrdokument för behörighetshantering upprättas och tillgängliggörs.
- Att roller och ansvar formaliseras och tydliggörs för systemägare/systemansvariga och övriga roller som hanterar behörigheter.
- Att samtliga anställdas och verksammas möjlighet att se alla leverantörsfakturor i Proceedo utvärderas och att säkerhetsrisken med tittbehörighet beaktas.
- Att regelbunden uppföljning av tilldelade behörigheter och attesträtter inom respektive system genomförs samt att rutiner och ansvarsfördelning för uppföljning införs för att säkerställa att registrerade behörigheter är aktuella och riktiga.

2 Bakgrund och motiv

Väl fungerande rutiner för administration av användares behörigheter är viktigt för att skydda och bevara information och för att hålla en rimlig säkerhetsnivå när det gäller åtkomst till IT-system. Det bör finnas tydliga rutiner för tilldelning, förändring, avslut och granskning av behörigheter.

Behörighetshantering kan kortfattat sägas handla om att ge rätt person tillgång till rätt information vid rätt tillfälle. Behörigheter bör tilldelas enligt principen lägsta behörighet, d.v.s. att användare inte tilldelas högre behörighet än vad som behövs för att man ska kunna utföra sina arbetsuppgifter. Behörighetshantering inklusive attestflöden bör även vara utformade på ett sådant sätt att de främjar en säker, effektiv och ändamålsenlig process.

Om det finns brister i behörighetshantering kan det innebära att användare kan ha åtkomst till information som de inte ska ha tillgång till. Det kan leda till att användare medvetet eller omedvetet kan ändra, sprida eller ta bort väsentlig information vilket kan medföra risk för oegentligheter. Om användare inte har en unik identitet i system finns risk att det inte går att spåra vem som gjort ändringar/tagit bort information i systemet. Risken för oegentligheter ökar om användare i system har möjlighet att attestera sina egna kostnader. Brister i behörighetshanteringen kan även leda till att känsliga uppgifter läcker ut till obehöriga vilket kan innebära att registrerade personer förlorar kontrollen över sina uppgifter och rättigheter.

3 Granskningens omfattning och inriktning

Syftet med granskningen har varit att bedöma om hanteringen av behörigheter inom SLU är effektiv, ändamålsenlig och bedrivs med tillfredsställande kontroll och säkerhet.

Granskningen har omfattat behörighetshantering i ett urval av administrativa system. I granskningen har ingått att även granska attestflöden. Följande system har ingått i granskningen:

- Idis - Identitets- och informationssystem, en katalog över anställda, verksamma och studenter inom SLU. Kontrollerar vilka personer vid SLU som har tillgång till vissa resurser som exempelvis e-post.
- Proceedo – system för inköp/beställning och fakturahantering.
- Agresso[1] – SLU:s huvudsakliga ekonomisystem som innehåller huvudbok, kund- och leverantörsreskontra. I systemet registreras konto- och objektplan.
- Primula – Personal- och lönesystem. Hanterar olika ärendetyper som anställning/bemanning, semester, ledigheter, ersättning, reseräkningar samt bisysslor.

[1] I april 2019 bytte Agresso namn till UBW (Unit4 Business World).

- Lins – SLU:s ledningsinformationssystem. I systemet finns rapporter som baseras på data från andra system som exempelvis Agresso, Primula och Ladok.

Internrevisionen har genomfört intervjuer med nyckelpersoner inom de granskade systemen, bland annat systemägare, systemansvariga, lönespecialister och administrativa roller som katalogroll och personalregistreringsroll. Intervjuer har även genomförts med chefer inom IT-avdelningen. Internrevisionen har gjort dokumentstudier av såväl centrala som systemspecifika dokument.

I granskningen har ingått test av behörigheter och attester. 26 tester har genomförts på slumpvis utvalda användare. Utöver behörigheter och attester ingick att testa om anställda som avslutat sin anställning vid SLU under perioden 20180101 - 20190405 är borttagna i systemet Idis. Därtill har testats om användare i systemet Proceedo som granskar leverantörsfakturor även kan attestera dem. I Primula har attestflöde för ledighet, semester och ersättning samt reseräkningar granskats.

Granskningen har genomförts med stöd av Anna Ganetz, IT-revisor (CISA, CIA) från Transcendent Group.

4 Behörighetshantering

4.1 Styrande och stödjande dokument för behörighetshantering

Det saknas styrande dokument för behörighetshantering på övergripande nivå vilket ökar risken för felaktig och avvikande hantering av behörigheter.

Syftet med styrande dokument är att ledningen tydliggör inriktningen avseende behörighetshanteringen.

I riktlinjer för informationssäkerhet vid SLU (ua 2015.2.10-2118) anges systemägarens ansvar kring säkerheten i system. Det pågår även ett arbete inom SLU Säkerhet, tillsammans med it-avdelningen, med att ta fram en instruktion kring åtkomsthantering till it-system med fokus på behörighetshantering ur ett informationssäkerhetsperspektiv. Det finns även ett beslut[2] av universitetsdirektören om rollägare för administrativa roller[3] där det anges att rollägare har ansvar för att avgöra om rollinnehavare uppfyller de krav som anges för respektive roll och om de kan tilldelas behörighet till de administrativa systemen. I övrigt saknas övergripande dokument som är relaterade till behörighetshantering.

[2] Beslut – Rollansvariga för de administrativa rollerna, SLU ua Fe.2011.1.0-1280
[3] Administrativa roller är en samling likartade administrativa arbetsuppgifter som ska utföras för varje institutions/motsvarande räkning. Exempel på administrativa roller är: katalogroll, ekonomiregistreringsroll, personalroll, inköpsroll.

Det saknas även en samlad bild över vilka system som finns inom SLU och vilka system som it-avdelningen har förvaltnings- och driftsansvar för. Det pågår enligt uppgift en översyn av detta.

För respektive system finns dokument som i olika omfattning beskriver ansvar, hantering och praktiskt utförande. För Idis finns manualer för de funktioner som hanterar roller i systemet. Där beskrivs hur godkännande, aktivering/avaktivering av roller i Idis ska ske. För Proceedo och Agresso finns upprättade förvaltningsplaner som bland annat beskriver ansvar för systemägare och systemansvarig samt rutiner för behörighetsbeställning. För Primula finns dokumentet Behörighetsadministration, som beskriver hur man praktiskt ska skapa, tilldela och ta bort behörigheter men det saknas uppgifter om vilka funktioner som ansvarar för vad.

Enligt internvisionens bedömning finns brister i det interna regelverket då det saknas övergripande beskrivning av hur behörighetshantering ska ske inom SLU. Avsaknad av övergripande styrdokument kan medföra att behörighetshanteringen inte sker enhetligt inom myndigheten. Det kan även innebära att behörigheter hanteras felaktigt. Bristande system- och förvaltningsdokumentation innebär dessutom risk för sårbarhet och personberoende.

IR rekommenderar att universitetsledningen säkerställer

A. att övergripande styrdokument för behörighetshantering upprättas och tillgängliggörs. Styrdokument för behörighetshantering bör bland annat definiera syfte, mål, inriktning, omfattning, roller och ansvarsfördelning.

4.2 Roller och ansvar

Roller för systemägare och systemansvariga är inte tydliggjorda på en övergripande nivå vilket kan innebära ett otydligt ansvar för respektive system.

Det finns utnämnda systemägare och systemansvariga för respektive system. Internrevisionen har noterat att det för systemet Idis finns angivna systemägare och systemansvariga från fem olika avdelningar. Enligt uppgift beror det på att personer från dessa avdelningar var involverade vid utveckling/start av Idis. Flera av angivna systemägare/ansvariga hade inte kännedom om att de var ägare/ansvariga och var osäkra på vad rollen innebär. Systemägarskapet för Lins ansågs felplacerad och borde flyttas till samma avdelning som systemansvaret. För Proceedo och Agresso anges roller och ansvar för systemägare och systemansvarig i förvaltningsplaner.

På medarbetarwebben finns uppgifter om vilken roll som hanterar tillägg och borttagning av roller i Idis samt att godkännande ska ske av prefekt och rollansvarig. Denna information avser enbart roller i Idis och inte de övriga granskade systemen.

Prefekt/motsvarande har utifrån sin roll som chef ansvar att initiera behörighetsbehov samt godkänna att ansökan skickas till respektive system. Övriga roller som är involverade i hantering av behörigheter är fördelade på institution/motsvarande (de administrativa rollerna) och på avdelningar inom universitetsadministrationen.

I beskrivningen av administrativa roller anges vilka system som respektive roll ska ha tillgång till. Det finns tydligt angivet att katalogrollen har i uppgift att hantera tillägg och borttagande av uppgifter i Idis. I övrigt framgår inte vilka administrativa roller som har i uppgift att beställa/kontrollera/följa upp de behörigheter/roller som initierats av prefekt/motsvarande. Behörigheter till respektive system beviljas/registreras i systemet av funktion vid den avdelning inom universitetsadministrationen som ansvarar för systemet.

Internrevisionen bedömning är att roller och ansvar för de olika delarna inom behörighetshantering inte framgår tydligt. Internrevisionen ser framförallt ett behov av att tydliggöra systemägares och systemansvarigas roller. Om dessa roller inte är tydligt definierade avseende ansvar, såväl generellt för alla system som för respektive system, finns risk att systemen inte hanteras på ett effektivt och säkert sätt, exempelvis att beslut inte tas av behörig och att informationssäkerhetsfrågor inte hanteras i den utsträckning som behövs.

Internrevisionen ser en risk med att det finns flera systemägare till Idis samt att ansvaret inte finns angivet. Detta ökar risken för att systemet inte hanteras effektivt, säkert och ändamålsenligt. Däremot är det en fördel att det finns flera systemansvariga då Idis hanterar tre identitetsgrupper; anställd, verksam och student.

Att det finns en fördelning av behörighetshanteringen mellan institutioner/motsvarande och centrala avdelningarna anser internrevisionen är bra. Med sådan fördelning minskar risken för felaktig hantering. Det finns dock behov av att uppdatera de administrativa rollerna med tydligare uppgifter om vilka roller som är involverade i behörighetshantering. Dokumenterade rollbeskrivningar är grundläggande förutsättningar för att veta vad som förväntas av rollerna samt vilket ansvar de har.

IR rekommenderar att universitetsledningen säkerställer

B. att det enbart finns en utsedd systemägare för Idis.

C. att roller och ansvar formaliseras och tydliggörs för såväl systemägare/systemansvariga som för övriga roller som hanterar behörigheter.

4.3 Behörigheter i granskade system

Det finns brister i kontrollen över tilldelade behörigheter och det sker ingen bedömning av behovet av titt-behörigheter. Detta kan leda till att obehöriga får tillgång till uppgifter samt att känsliga uppgifter kan spridas.

När en person anställs, är verksam[4] eller är student får hen en unik identitet i systemet Idis. Anställda tilldelas identitet i Idis automatiskt via uppdatering från Primula. Studenter tilldelas identitet i Idis i huvudsak via uppgifter från Ladok för att få tillgång till lokaler och e-post. Personer som tillhör gruppen verksam läggs in i Idis manuellt av den som har katalogrollen för respektive institution/motsvarande. Prefekt/motsvarande godkänner tilldelning av olika roller i Idis.

Behörigheter till Primula, Proceedo, Agresso och Lins beställs av administrativa roller på institution/motsvarande. Beställningen skickas efter godkännande av prefekt/motsvarande till respektive system. Vid de centrala avdelningar som ansvarar för systemen finns utsedda personer som registrerar och ger användare behörigheter till system.

När en anställning avslutas får Idis informationen om detta automatiskt via systemet Primula. Då får användaren i systemet Idis status vilande under en månad efter avslutad anställning och därefter sätts status inaktiv. För verksamma sätter kataloganvarig ett slutdatum redan vid tilldelning av en identitet i IDIS. Det är dock möjligt att sätta datum för mycket långa perioder. Innan slutdatum skickas förfrågan om eventuell förlängning till den som beställt identiteten. När slutdatumet passeras sätts status inaktiv automatiskt och därmed har personen inte tillgång till något av de granskade systemen. En identitet i Idis tas aldrig bort utan får status inaktiv för att inte riskera att en redan använd identitet ska tilldelas någon annan.

Vid förändringar, t.ex. om en anställd eller verksam byter arbetsplats inom SLU behålls identiteten i Idis. Om personen ska ha behörigheter till olika system på den nya arbetsplatsen beställs dessa av den arbetsplatsen enligt samma rutin som vid nyanställning. Vid intervjuer framkom att det är den gamla arbetsplatsen som ska avsluta behörigheter. Det saknas dock dokumenterade rutiner för de administrativa rollerna att sådan kontroll regelbundet ska ske vid byte av arbetsplats. Detta innebär enligt internrevisionen en risk för att personer kan ha kvar felaktiga behörigheter i systemen.

Nedan anges noteringar specifikt per system utifrån iakttagelser som i huvudsak gjorts vid de tester som genomförts.

Idis
En användare finns i systemet som verksam samtidigt som användaren finns registrerad som anställd. Användaren hade från början icke svenskt personnummer

[4] Till verksam räknas person som inte är anställd eller student vid SLU men som har en tydlig och aktiv koppling till en institution/motsvarande, t.ex. konsult.

och när användaren fick svenskt personnummer ändrades status till anställd utan att status verksam togs bort.

Rutinen är att när en person som ännu inte fått svenskt personnummer blir föreslagen till en anställning registreras hen i Idis som verksam med ett fiktivt personnummer. När hen får sitt svenska personnummer läggs anställningen in i Primula och uppgifterna importeras till Idis som status anställd. Innan anställningsuppgifterna går genom Primula bör berörd institution/motsvarande meddela IT-avdelningen om personnummerbyte i Idis så att hens verksamma identitet får det korrekta personnumret. Om detta inte sker så kommer individen ha två identiteter i Idis med olika personnummer och olika status som IT sedan måste göra om till en. Då användaren oavsett ett eller två konton enbart har en inloggningsuppgift så innebär det ingen ökad risk för felaktig tillgång till andra system.

Proceedo
Samtliga anställda och verksamma registreras in i Proceedo. Användare får automatiskt titt-behörighet och kan därmed se samtliga fakturor inom SLU. Övriga behörigheter beställs av respektive institution/motsvarande utifrån rolltilldelningen i Idis och godkänns/registreras av ekonomiavdelningens Proceedosupport.

Under granskningen framkom att informationssäkerhetssamordnaren diskuterat titt-behörigheten med systemgruppen för Proceedo. Vid det tillfället fanns 3400 anställda och 1685 verksamma med titt-behörighet. Bland annat lyftes det upp att det förekommer fakturor som innehåller känslig information som rör exempelvis personuppgifter, inköp av kemikalier, potentiella sprängämnen och vapen och att en generell titt-behörighet kan utgöra en säkerhetsrisk om informationen sprids till obehöriga. Systemgruppen har angett att de ska se över vem som ska se vad i systemet och diskutera möjligheten med systemleverantören att lägga begränsningar på titt-behörighet. Det finns möjligheter att sekretessmärka fakturor men hittills har den möjligheten inte använts.

Internrevisionen anser att det är viktigt att bedöma behovet av åtkomst till leverantörsfakturor i Proceedo. Att samtliga anställda och verksamma kan se alla leverantörsfakturor i systemet innebär en säkerhetsrisk där känsliga uppgifter kan spridas till obehöriga. Internrevisionen ser positivt på att problematiken och alternativ på lösningar har lyfts upp till diskussion inom avdelningen.

Agresso
Vid internrevisionens test noterades att det finns ett flertal användare med höga behörigheter i systemet. Samtliga dessa behörigheter medför möjlighet att lägga till och ändra bland annat inställningar i systemet. Enligt uppgift är orsaken till många höga behörigheter att det vid granskningstillfället pågick en uppgradering av Agresso. Internrevisionen informerades om att flera av behörigheterna avslutats då arbetet slutförts.

Vidare identifierades att två användare fanns kvar med aktiva behörigheter i systemet fast de har avslutat sin anställning. En av användarna gick i pension 2017-07-31 den andra användaren avslutade sin anställning 2018-05-13.

Att det finns enskilda användare som har höga behörigheter i systemet kan vara befogat ur ett effektivitetsperspektiv men internrevisionen anser att det även ökar risken för att felaktigheter förblir oupptäckta. Tilldelning av alltför många höga behörigheter kan innebära risk för att obehöriga får åtkomst till information. Internrevisionen har inte noterat några orimligt höga behörigheter men anser att det är viktigt att det alltid sker en bedömning av om tilldelning av höga behörigheter är befogat.

Primula
Vid genomgång av behörigheter identifierades att två användare har kvar sina behörigheter i systemet fast de borde ha tagits bort. Vidare noterades att en användares behörighet var helt felaktig. Systemansvarig har åtgärdat detta under granskningens gång och behörigheten är korrekt nu.

Lins
I Lins har samtliga anställda tillgång till standardrapporter. Det finns också ett mer avancerat verktyg, Lins analyskub, där behörighet ansöks hos och bedöms av Linssupporten. För att få tillgång till Lins analyskub krävs obligatorisk utbildning.

Användare har endast åtkomst till information i systemet och har ingen möjlighet att lägga till, ändra eller ta bort information.

Internrevisionen anser att det föreligger låg risk avseende behörighetshantering i systemet Lins.

IR rekommenderar att universitetsledningen säkerställer

D. att det finns övergripande rutiner för regelbunden kontroll av behörigheter vid byte av arbetsuppgifter/arbetsplats inom SLU.

E. att behovet av höga behörigheter i de granskade systemen regelbundet kontrolleras och bedöms.

F. att samtliga anställdas och verksammas möjlighet att se alla leverantörsfakturor i Proceedo utvärderas och att säkerhetsrisken med tittbehörighet beaktas.

4.4 Attestflöden

Det är möjligt för slutattestant att attestera fakturor som rör egna inköp. Detta innebär risk för felaktigheter.

Proceedo
Systemet hanterar beställningar (inköp) och leverantörsfakturor. SLU:s ekonomihandbok anger att en faktura alltid ska handläggas av minst två personer

där en godkänner fakturan (fakturagranskare) och en fattar beslut om utbetalning (slutattestant). Vid e-beställning attesterar slutattestanten redan vid beställning. I systemet tillförsäkras dualitetsprincipen[5] genom automatiska spärrar som omöjliggör att fakturagranskning och beslutsattest utförs av samma person. Om utsedd slutattestant inte attesterar faktura inom sex arbetsdagar eskalerar den upp till prefektnivå. Fakturan kommer då att finnas hos den ursprungliga attestanten och den överordnade chefen samtidigt. I systemet markeras eskalerade fakturor med en symbol.

I Ekonomihandboken anges att *”Ingen anställd vid SLU får attestera fakturor/utlägg som rör dennes personliga inköp i tjänsten, dessa ska i regel attesteras av närmast överordnad chef.”*

Proceedo är uppbyggt så att attest styrs utifrån kostnadsställe och det kan därför inträffa att en faktura för personligt inköp hamnar för attest hos den slutattestant som det personliga inköpet avser. Systemet signalerar inte att det är en faktura som avser personligt inköp. Det krävs att användaren kryssar i eget köp i en ruta för att fakturan ska gå vidare till nästa nivå i attesthierarkin för slutattest. Information om detta finns i handbok för attestanter.

Internrevisionen anser att dualitetsprincipen och automatiska spärrar minskar risken för felaktig hantering. Däremot finns en risk att en anställd attesterar fakturor som rör egna inköp då detta ska markeras med ett kryss.

Primula
I Primula attesteras ledigheter, semestrar och ersättningar i ett flöde och reseräkningar i ett annat flöde.

Det normala flödet för ett ärende i Primula är att ärendet går från den anställde till attesterande chef, där den anställde har sin hemvist. Vid attest av ledigheter, semestrar och ersättningar eskaleras ärendet till nästa nivå om den attesterande chefen inte attesterat ärendet inom tio dagar. Reseräkningar granskas av personalregistrerarroll där den anställde har sin hemvist och går därefter vidare till attesterande chef/chefer som har ansvar för de kostnadsställen som reseräkningen ska belasta. För reseräkningar finns ingen eskalering vilket innebär att om attesterande chef inte attesterar ärendet så sker ingen utbetalning. Enligt uppgift är det inte möjligt att skapa eskalering i systemet.

En prefekt kan ha utlägg som avser den egna forskningen och inte prefektrollen. I Primula finns specialflöde för prefekter avseende egna kostnader som reseräkningar/motsvarande. Ärendena går då till dekan för slutattest oberoende av var prefekt/motsvarande har sin hemvist. Specialflöde har skapats för att bland annat minska risken att underställd chef attesterar en prefekts egna utlägg. Det är

[5] Dualitetsprincipen: principen om att ingen person ensam ska handlägga en transaktion genom hela betalningskedjan.

lönespecialister vid personalavdelningen som lägger in specialflöden efter begäran från institution/motsvarande.

Det går att ta ut olika rapporter ur Primula, bland annat behörigheter per institution. Det är dock inte möjligt att ta fram rapport i systemet över vilka användare som har specialflöden. Uppgifterna måste tas fram manuellt vilket enligt uppgift är tidskrävande och kräver mycket manuell hantering.

Vid ändring/byte av tjänst inom SLU finns en risk att specialflöde kan ligga kvar på personen som inte längre har behov av det. Systemet känner inte av byte av tjänst automatiskt utan en ändring måste ske manuellt. Detta är inte riktigt tydliggjort.

I Primula eskalerar inte slutattest av reseräkningar till nästa nivå i attesthierarkin. Det innebär att det finns risk att anställd inte får ersättning för utlägg, traktamenten etc. I Primula finns även en risk att specialflöden är felaktiga då det saknas kontroll över vilka som har/ska ha den attestbehörigheten.

IR rekommenderar att universitetsledningen säkerställer

G. att tilldelade specialflöden kontrolleras regelbundet.

IR rekommenderar att universitetsledningen överväger

H. att se över möjliga lösningar för att hantera risken att egna kostnader attesteras av den som har gjort inköp och för att hantera risken att reseräkningar inte blir attesterade inom rimlig tid.

4.5 Uppföljning

Det saknas dokumenterade rutiner för uppföljning/inventering av behörigheter och attester. Uppföljning av behörigheter sker inte regelbundet eller inte alls, vilket ökar risken för att personer har felaktig behörighet.

Uppföljning av behörigheter bör ske med viss regelbundenhet för att tillförsäkra att behörigheter är korrekta.

I de dokument som finns för respektive system saknas rutiner och ansvarsfördelning för uppföljning/inventering av behörigheter för såväl central nivå som för institution/motsvarande. Enligt uppgift sker viss uppföljning av behörigheter i enstaka fall, exempelvis attesträtter i Proceedo vid prefektbyte. Dock sker ingen systematisk uppföljning av behörigheter.

Det är inte tydligt att uppföljning av behörigheter och attester ska göras, vem som är ansvarig, på vilken nivå uppföljningen ska utföras samt hur ofta. Internrevisionen anser att det bland annat behövs en genomgång av aktuella behörigheter och attester vid prefektbyte så att ny prefekt har möjlighet att bedöma om behörigheter och attest är rimliga i förhållande till personernas arbetsuppgifter.

Regelbunden inventering av behörigheter lyfts även fram i SLU Säkerhets förslag på instruktion för åtkomsthantering där informationsägaren[6] anges som ansvarig för att säkerställa att inventering sker regelbundet.

Om behörigheter inte följs upp finns risk för felaktig tilldelning av behörigheter vilket kan innebära att obehörig får tillgång till information, uppgifter kan ändras och att personuppgifter kan spridas.

IR rekommenderar att universitetsledningen säkerställer

I. att regelbunden uppföljning av tilldelade behörigheter och attesträtter inom respektive system genomförs samt att rutiner och ansvarsfördelning för uppföljning införs för att säkerställa att registrerade behörigheter är aktuella och riktiga.

I rutinen bör det framgå att uppföljning av behörigheter ska ske regelbundet, vilka funktioner som ansvarar för och genomför uppföljning. Uppföljningen bör dokumenteras och kommuniceras till berörda chefer och administrativa roller på institutioner/motsvarande.

Inga Astorsdotter
Internrevisionschef

Lisbeth Sundkvist Johansson
Internrevisor

[6] ”Informationsägare är ofta den verksamhetsansvarige vars verksamhet har skapat informationen, fattat beslut om den alternativt tagit över ansvaret för den. Det kan vara prefekt eller motsvarande chef men det kan också vara delegerat.” (Riktlinjer för informationssäkerhet vid SLU, ua 2015.2.10-2118)

Sveriges lantbruksuniversitet
Swedish University of Agricultural Sciences

Rektor

ÅTGÄRDSPLAN SLU ID: SLU..ua 2019.1.1.2-963

2019-08-28

Rektors åtgärdsplan till internrevisionens rapport Behörighetshantering.

Nr	**Noterade brister** (internrevisionen fyller i)	**Rekommendation** (internrevisionen fyller i)	**Åtgärd** (ledning/verksamhet fyller i)
A	Enligt internvisionens bedömning finns brister i det interna regelverket då det saknas övergripande beskrivning av hur behörighetshantering ska ske inom SLU. Avsaknad av övergripande styrdokument kan medföra att behörighetshanteringen inte sker enhetligt inom myndigheten.	IR rekommenderar att universitetsledningen säkerställer att övergripande styrdokument för behörighetshantering upprättas och tillgängliggörs. Styrdokument för behörighetshantering bör bland annat definiera syfte, mål, inriktning, omfattning, roller och ansvarsfördelning.	**Ansvarig avdelning/enhet:** Avdelningen för service, säkerhet och miljö ☒ Åtgärdas enligt rekommendation ☐ Åtgärdas på annat sätt, ange vilket under kommentar nedan ☐ Åtgärdas inte, ange varför under kommentar nedan **Kommentar:** En instruktion för åtkomsthantering tas fram av Informationssäkerhet. **Åtgärdas senast:** 2019-12-31 **Dokumentation** (om det ej framgår ovan)**:**
B	Internrevisionen ser en risk med att det finns flera systemägare till Idis samt att deras ansvar inte finns angivet. Detta ökar	IR rekommenderar att universitetsledningen säkerställer att det enbart finns en utsedd systemägare för Idis.	**Ansvarig avdelning/enhet:** Udir m.h.a. IT-avdelningen

Nr	**Noterade brister** (internrevisionen fyller i)	**Rekommendation** (internrevisionen fyller i)	**Åtgärd** (ledning/verksamhet fyller i)
	risken för att systemet inte hanteras effektivt, säkert och ändamålsenligt. Däremot är det en fördel att det finns flera systemansvariga då Idis hanterar tre identitetsgrupper; anställd, verksam och student.		☒ Åtgärdas enligt rekommendation ☐ Åtgärdas på annat sätt, ange vilket under kommentar nedan ☐ Åtgärdas inte, ange varför under kommentar nedan **Kommentar:** **Åtgärdas senast:** 2019-12-31 **Dokumentation** (om det ej framgår ovan)**:**
C	Det finns behov av att uppdatera de administrativa rollerna med tydligare uppgifter om vilka roller som är involverade i behörighetshantering. Dokumenterade rollbeskrivningar är grundläggande förutsättningar för att veta vad som förväntas av rollerna samt vilket ansvar de har.	IR rekommenderar att universitetsledningen säkerställer att roller och ansvar formaliseras och tydliggörs för såväl systemägare/systemansvariga som för övriga roller som hanterar behörigheter.	**Ansvarig avdelning/enhet:** IT-avdelningen ☐ Åtgärdas enligt rekommendation ☒ Åtgärdas på annat sätt, ange vilket under kommentar nedan ☐ Åtgärdas inte, ange varför under kommentar nedan **Kommentar:** Utreda införande av en systemförvaltningsmodell med tillhörande roller och ansvar. **Åtgärdas senast:** 2019-12-31 **Dokumentation** (om det ej framgår ovan)**:**
D	Vid förändringar, t.ex. om en anställd eller verksam byter arbetsplats inom SLU behålls identiteten i Idis Vid intervjuer	IR rekommenderar att universitetsledningen säkerställer att det finns övergripande rutiner	**Ansvarig avdelning/enhet:** Avdelningen för service, säkerhet och miljö

Nr	Noterade brister (internrevisionen fyller i)	Rekommendation (internrevisionen fyller i)	Åtgärd (ledning/verksamhet fyller i)
	framkom att det är den gamla arbetsplatsen som ska avsluta behörigheter. Det saknas dock dokumenterade rutiner för de administrativa rollerna att sådan kontroll regelbundet ska ske vid byte av arbetsplats. Detta innebär enligt internrevisionen en risk för att personer kan ha kvar felaktiga behörigheter i systemen	för regelbunden kontroll av behörigheter vid byte av arbetsuppgifter/arbetsplats inom SLU.	☒ Åtgärdas enligt rekommendation ☐ Åtgärdas på annat sätt, ange vilket under kommentar nedan ☐ Åtgärdas inte, ange varför under kommentar nedan **Kommentar:** Rutinbeskrivning ingår i instruktionen för åtkomsthantering, se punkt A. Respektive systemägare ansvarar för regelbunden kontroll av behörigheter. **Åtgärdas senast:** 2019-12-31 **Dokumentation** (om det ej framgår ovan)**:**
E	Tilldelning av alltför många höga behörigheter kan innebära risk för att obehöriga får åtkomst till information. Internrevisionen har inte noterat några orimligt höga behörigheter men anser att det är viktigt att det alltid sker en bedömning av om tilldelning av höga behörigheter är befogat.	IR rekommenderar att universitetsledningen säkerställer att behovet av höga behörigheter i de granskade systemen regelbundet kontrolleras och bedöms.	**Ansvarig avdelning/enhet:** Berörda systemägare på resp. avdelning ☒ Åtgärdas enligt rekommendation ☐ Åtgärdas på annat sätt, ange vilket under kommentar nedan ☐ Åtgärdas inte, ange varför under kommentar nedan **Kommentar:** **Åtgärdas senast:** 2019-12-31 **Dokumentation** (om det ej framgår ovan)**:**
F	Internrevisionen anser att det är viktigt att bedöma behovet av åtkomst till leverantörsfakturor i Proceedo. Att samtliga anställda och verksamma kan se alla	IR rekommenderar att universitetsledningen säkerställer att samtliga anställdas och verksammas möjlighet att se alla	**Ansvarig avdelning/enhet:** Ekonomiavdelningen

Nr	Noterade brister (internrevisionen fyller i)	Rekommendation (internrevisionen fyller i)	Åtgärd (ledning/verksamhet fyller i)
	leverantörsfakturor i systemet innebär en säkerhetsrisk där känsliga uppgifter kan spridas till obehöriga.	leverantörsfakturor i Proceedo utvärderas och att säkerhetsrisken med tittbehörighet beaktas.	☒ Åtgärdas enligt rekommendation ☐ Åtgärdas på annat sätt, ange vilket under kommentar nedan ☐ Åtgärdas inte, ange varför under kommentar nedan **Kommentar:** **Åtgärdas senast:** 2020-06-30 **Dokumentation** (om det ej framgår ovan)**:**
G	Det är inte möjligt att ta fram rapport i systemet över vilka användare som har specialflöden. Uppgifterna måste tas fram manuellt vilket enligt uppgift är tidskrävande och kräver mycket manuell hantering.	IR rekommenderar att universitetsledningen säkerställer att tilldelade specialflöden kontrolleras regelbundet.	**Ansvarig avdelning/enhet:** Ekonomiavdelningen (Proceedo) Personalavdelningen (Primula) ☒ Åtgärdas enligt rekommendation ☐ Åtgärdas på annat sätt, ange vilket under kommentar nedan ☐ Åtgärdas inte, ange varför under kommentar nedan **Kommentar:** **Åtgärdas senast:** 2020-06-30 **Dokumentation** (om det ej framgår ovan)**:** Rutiner samt lathundar utarbetas för att säkerställa detta.
H	Internrevisionen anser att dualitetsprincipen och automatiska spärrar minskar risken för felaktig hantering. Däremot finns en risk att	IR rekommenderar att universitetsledningen överväger att se över möjliga lösningar för att hantera risken att egna kostnader attesteras av	**Ansvarig avdelning/enhet:**

Nr	Noterade brister (internrevisionen fyller i)	Rekommendation (internrevisionen fyller i)	Åtgärd (ledning/verksamhet fyller i)
	en anställd attesterar fakturor som rör egna inköp då detta ska markeras med ett kryss. För reseräkningar finns ingen eskalering vilket innebär att om attesterande chef inte attesterar ärendet så sker ingen utbetalning.	den som har gjort inköp och för att hantera risken att reseräkningar inte blir attesterade inom rimlig tid.	Ekonomiavdelning: Ansvarig fakturaprocessen/Proceedo: chef reskontraenheten. 2020-12-31 Personalavdelning: Ansvarig reseräkningsprocess/ Primula: 2020-06-30 ☒ Åtgärdas enligt rekommendation ☐ Åtgärdas på annat sätt, ange vilket under kommentar nedan ☐ Åtgärdas inte, ange varför under kommentar nedan **Kommentar:** Avser Primula: Tidigare försök har gjorts för att ändra detta men ytterligare kontakter bör tas med leverantören. **Åtgärdas senast:** **Dokumentation** (om det ej framgår ovan)**:**
I	I de dokument som finns för respektive system saknas rutiner och ansvarsfördelning för uppföljning/inventering av behörigheter för såväl central nivå som för institution/motsvarande. Det sker ingen systematisk uppföljning av behörigheter. Det är inte tydligt att uppföljning av behörigheter och attester ska göras, vem	IR rekommenderar att universitetsledningen säkerställer att regelbunden uppföljning av tilldelade behörigheter och attesträtter inom respektive system genomförs samt att rutiner och ansvarsfördelning för uppföljning införs för att säkerställa att registrerade behörigheter är aktuella och riktiga. I rutinen bör det framgå att uppföljning av behörigheter ska ske regelbundet, vilka funktioner som ansvarar för och genomför	**Ansvarig avdelning/enhet:** Stycke 1: berörd systemägare Stycke 2: Avdelningen för service, säkerhet och miljö ☒ Åtgärdas enligt rekommendation ☐ Åtgärdas på annat sätt, ange vilket under kommentar nedan ☐ Åtgärdas inte, ange varför under kommentar nedan **Kommentar:**

Nr	**Noterade brister** (internrevisionen fyller i)	**Rekommendation** (internrevisionen fyller i)	**Åtgärd** (ledning/verksamhet fyller i)
	som är ansvarig, på vilken nivå uppföljningen ska utföras samt hur ofta. Om behörigheter inte följs upp finns risk för felaktig tilldelning av behörigheter vilket kan innebära att obehörig får tillgång till information, uppgifter kan ändras och att personuppgifter kan spridas.	uppföljning. Uppföljningen bör dokumenteras och kommuniceras till berörda chefer och administrativa roller på institutioner/motsvarande.	**Åtgärdas senast:** Stycke 1: 2019-12-31 Stycke 2: 2019-12-31 **Dokumentation** (om det ej framgår ovan)**:**