Sveriges lantbruksuniversitet
Swedish University of Agricultural Sciences

**Styrelsen**

**BESLUT**

SLU ID: SLU.ua.2018.1.1.2-3887

2019-06-19

# Ladok

## Beslut

Styrelsen beslutar

att fastställa internrevisionens rapport Ladok, samt

att fastställa rektors åtgärdsplan med anledning av rapporten.

## Ärendet

Internrevisionen har i enlighet med revisionsplanen för 2018 granskat hanteringen av systemet Ladok centralt vid Ladokkonsortiet och lokalt vid SLU. Syftet med denna granskning var att bedöma i vilken utsträckning Ladokkonsortiets och SLU:s interna styrning avseende Ladok är effektiv, ändamålsenlig och att systemet har en tillfredsställande säkerhet.

Internrevisionens sammanfattande bedömning är att hanteringen av Ladok kan förbättras såväl centralt som lokalt vid SLU. Med anledning av detta rekommenderar internrevisionen ett antal åtgärder.

Beslut i detta ärende har fattats av styrelsen efter föredragning av biträdande universitetsdirektör Birgitta Wikmark Carlsson. Ärendet har i huvudsak beretts av Roger Pettersson, avdelningschef för avdelningen för lärande och digitalisering.

Rolf Brennerfelt

Birgitta Wikmark Carlsson

## Kopia för kännedom

Prorektor
Dekanerna
Avdelningschefer (motsv.) inom universitetsadministrationen
Universitetdjursjukhusdirektör
Överbibliotekarie

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

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

Sveriges lantbruksuniversitet
Swedish University of Agricultural Sciences

**Internrevisionen**

SLU ID: SLU.ua 2018.1.1.2-3887

2019-06-19

# Ladok

## Rapport från internrevisionen

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

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

# Innehåll

# 1 Sammanfattning

Internrevisionen har i enlighet med revisionsplanen för 2018 granskat hanteringen av systemet Ladok centralt vid Ladokkonsortiet och lokalt vid SLU. Syftet med granskning var att bedöma i vilken utsträckning den interna styrning avseende Ladok är effektiv, ändamålsenlig och innehar tillfredsställande säkerhet.

Internrevisionens sammanfattande bedömning är att hanteringen av Ladok kan förbättras såväl centralt som lokalt vid SLU. Det finns brister som riskerar att påverka styrning och säkerhet vilket kan innebära att obehöriga får tillgång till information samt att det kan ske felaktiga utbetalningar av studiemedel från CSN. Internrevisionens bedömning grundar sig i huvudsak på följande;

1. Ladok centralt saknar styrdokument för informationssäkerhet, backuphantering samt förändringshantering.
2. SLU saknar eller det förekommer brister i styrande dokument för Ladok inom behörighetshantering, informationssäkerhet, backuphantering och förändringshantering.
3. SLU saknar dokumenterad riskanalys, kontinuitet- och katastrofplan som inkluderar Ladok.
4. SLU saknar viktiga moment för att säkerställa en tillförlitlig behörighetshantering av Ladok.

De väsentligaste rekommendationerna är följande;

- Att universitetsledningen säkerställer att Ladokkonsortiet tar fram styrande dokument inom området för informationssäkerhet, backuphantering samt förändringshantering för att fastställa och tydliggöra konsortiets viljeinriktning och styrning inom respektive område.
- Att befintliga styrande dokument utvecklas inom SLU för att säkerställa en adekvat styrning av behörigheter. Dessa bör inkludera förändring och borttagande av behörigheter samt regelbunden kontroll av behörigheter och priviligierade användaraktiviteter.
- Att SLU genomför en riskanalys av Ladok i syfte att identifiera risker och utvärdera hur dessa kan hanteras samt att en dokumenterad kontinuitetsplan/katastrofplan etableras för återställning av Ladok proxy[1] inom SLU.
- Att det vid SLU finns kontrollmoment i behörighetsprocessen för Ladok som säkerställer att behörigheter och priviligierade användaraktiviteter granskas regelbundet samt att förändring/borttagande av behörigheter hanteras ändamålsenligt.

[1] Ladok proxy är namnet på SLU:s lokala kopia av konsortiets Ladokdatabas.

## 2 Bakgrund och motiv

Ladok är ett nationellt system för studieadministration och hanterar information om studenter, kursregistrering, resultat och examen. Information som registreras i systemet ligger till grund för utbetalning av studiemedel från Centrala studiestödsnämnden (CSN). Exempel på andra informationsmottagare är SCB, Migrationsverket och universitetskanslersämbetet. Ladok lämnar även uppgifter om bland annat helårsstudenter och helårsprestationer till årsredovisningen. För Linneuniversitetet och Karlstads universitet är uppgifter i Ladok även underlag för redovisning av intäkter.

Ladok ägs gemensamt av 37 högskolor och universitet samt CSN genom Ladokkonsortiet. Systemet har under senare år genomgått en omfattande uppgradering till version 3. Arbetet med att forma ett utvecklingsprojekt startade 2007 och fastställdes 2010. Efter omfattande förseningar och fördyringar infördes nya Ladok succesivt vid lärosätena mellan hösten 2017 och december 2018. Vid SLU driftsattes systemet i maj 2018.

Under 2017 identifierade Ladokkonsortiet att det saknades separat strömförsörjning av den sekundära datorhallen, samt att backup av Ladok inte förvarades på annan plats. Vidare visar en rapport från Riksrevisionen[2] att det förekommer brister inom behörighetsadministration samt hanteringen av säkerhetskopior av produktionsdata. Om Ladok inte uppfyller högt ställda krav på säkerhet föreligger bland annat risk för att felaktig information lämnas i årsredovisningen och till olika informationsmottagare samt att studenternas rättssäkerhet och försörjning hotas.

## 3 Syfte

Syftet med denna granskning är att bedöma i vilken utsträckning SLU:s och Ladokkonsortiets interna styrning avseende Ladok är effektiv, ändamålsenlig och att systemet har en tillfredsställande säkerhet. Granskningen ska besvara följande revisionsfrågor:

- Finns det tillräcklig och tillfredställande styrande dokument?
- Finns det en tillfredställande kris- och kontinuitetshantering av drift och hantering?
- Hanteras behörigheter på ett tillfredställande sätt i Ladok?
- Hanteras rapportering, uppföljning och utvärdering av inträffade incidenter på ett ändamålsenligt sätt?
- Finns det tydligt ansvar och ägandeskap av information som registreras i Ladok?

Brister i intern styrning och kontroll avseende Ladok kan leda till:

[2] Riksrevisionen IT-granskning av Ladok 3, Dnr 2.3.3-2017-1250

- Felaktiga behörigheter i systemet, vilket kan innebära att obehöriga personer får tillgång till information.
- Felaktig registrering av information och bristande säkerhet vid drift av systemet, vilket kan innebära risk för felaktiga eller obefintliga utbetalning av studiemedel från CSN.
- Spridning av känslig information till obehöriga personer.
- en bristande kris- och kontinuitetshantering av Ladok, vilket kan innebära förlust av information samt driftstopp av systemet.

## 4 Metod och inriktning

Då Ladoksystemet och en stor del av riskerna som är knutna till det är gemensamma för lärosätena så har granskningen genomförts i samarbete med internrevisionen vid Linnéuniversitetet och Karlstads universitet. Granskningen har genomförts av internrevisionen vid SLU tillsammans med Transcendent Group. Granskningen har i huvudsak genomförts genom intervjuer med ett urval av nyckelpersoner vid Ladokkonsortiet samt inom SLU. Internrevisionen har även varit i kontakt med CSN. Utöver intervjuer har relevant styrdokumentation granskats.

Rapporten är uppdelad i två delar där första delen avser iakttagelser av hanteringen inom Ladokkonsortiet och den andra delen avser iakttagelser inom SLU.

Eftersom internrevisionen är underställd och rapporterar till SLU:s styrelse har enheten valt att ställa rekommendationerna som avser Ladokkonsortiets hanteringen av systemet (avsnitt 5) till SLU:s universitetsledning som brukligt vid andra granskningar. Internrevisionen bedömer att ledningen via sin roll i konsortiets stämma och via övriga kontakter kan verka för att åtgärder vidtas.

Granskningen har genomförts av Viktor Bergvall, IT-revisor (CISA) från Transcendent Group och Lisbeth Sundkvist Johansson, internrevisor vid SLU.

# 5 Ladok centralt

Ladokkonsortiet ägs och används av 37 lärosäten samt CSN. Konsortiets stämma, där företrädare för alla lärosäten och CSN deltar, utser en styrelse som har det övergripande ansvaret för verksamheten. Ladokkonsortiet ansvarar för drift och utveckling av Ladok. För att genomföra detta köper konsortiet infrastruktur och personalresurser avseende drift, utveckling och support från Umeå universitet. Det finns en uppdragsöverenskommelse mellan konsortiet och universitetet som avser teknisk förvaltning och drift av systemet för perioden 2018-01-01 – 2018-12-31. Överenskommelsen är under omarbetning.

Konsortiechefen är anställd av styrelsen och ansvarar tillsammans med en ledningsgrupp för systemutveckling, drift, support och verksamhetsstöd till lärosätena. Konsortiechefen rapporterar budgetutfall till styrelsen fyra gånger per år. Vid eventuellt budgetöverskridande beslutar styrelsen om åtgärder. Om avgifterna behöver höjas krävs stämmobeslut. Ladokkonsortiet har som ambition att inte höja avgifterna för förvaltningen av Ladok.

Varje lärosäte äger och har ansvar för sin information i Ladok. Det finns ett personuppgiftsbiträdesavtal upprättat mellan Ladokkonsortiet och respektive lärosäte, som bland annat beskriver krav för behandling av personuppgifter samt vilket ansvar respektive part har vid en eventuell skada. Internrevisionen har noterat att det förekommer viss oklarhet om konsortieformen, är den mest lämpliga ägandeformen. Det pågår en utredning för att se över organisationsformen.

Arbetet med att forma ett utvecklingsprojekt för Ladok startade 2007 och fastställdes med projektstart 2010 i form av ett förprojekt. Som tidigare nämnts var projektet behäftat med kraftiga förseningar och fördyringar, dessutom var budgetstyrningen bristfällig. I början av 2012 fattades ett beslut som innebar att det fanns tillräckligt med underlag för vidareutveckling av Ladok. Projektplan och budget togs fram där ett uppdaterat budgetförslag om 314 mnkr presenterades och godkändes. Projektets slutgiltiga budget blev 384 mnkr[3], vilket i huvudsak möttes vid slutrapportering.

## *5.1 Styrande dokument*

**Det saknas styrande dokument för informationssäkerhet, backuphantering samt förändringshantering inom Ladokkonsortiet, vilket bland annat ökar risken för felaktig hantering av information.**

Avsaknad av styrande dokument kan medföra att det finns oklarheter kring rutiner och arbetssätt samt att anställda inte arbetar mot gemensamma mål. Bristfällig central styrning leder även till ökad risk för personberoenden.

Då Umeå universitet genomför arbetet med drift och utveckling av Ladok gäller deras styrande dokument även för Ladok. Dock kvarstår ansvaret hos

[3] Inklusive kostnader för förprojekt och förstudier om ca 30 mnkr.

Ladokkonsortiet att ställa krav på säkerhet och hantering av Ladok i form av exempelvis styrande dokument. Umeå universitet har en informationssäkerhetspolicy från 2017, men saknar policydokument för backuphantering och förändringshantering.

Internrevisionens granskning visar att Ladokkonsortiet saknar en informationssäkerhetspolicy samt styrande dokument inom området för backuphantering och förändringshantering. Inom Ladokkonsortiet har det gjorts en översyn[4] inom områdena system, drift och hantering av Ladok. Baserat på resultatet av översynen ska beslut tas om policydokument inom informationssäkerhetsområdet, vilket internrevisionen ser positivt på.

Det finns dokumenterade rutiner för hur backup av Ladok ska hanteras, men det saknas underliggande analys som ställer krav på intervall och typ av backup. Detta medför att de backuper som görs av Ladok riskerar att vara otillräckliga avseende högskolornas/universitetens krav på tillgänglighet samt hur mycket data som kan förloras utan att påverka användandet av Ladok.

Det finns dokumenterade underlag som visar beslutspunkter för produktionssättning av utförda förändringar. Det saknas styrande dokument som beskriver förhållningsätt till förändringar av Ladok, innehållande exempelvis krav på testning, godkännande och prioritering av förändringar innan produktionssättning. Detta kan medföra att förändringar inte hanteras på ett korrekt, tydligt och konsekvent sätt.

Det finns styrande dokument för behörighetsprocessen vid Umeås universitet. Dokumentet beskriver i korthet hantering av priviligierade[5] behörigheter och granskning av användares behörigheter. Det saknas dock ett tydligt stöd i styrdokumentet för hur regelbunden granskning av priviligierade behörigheter och användaraktiviteter ska genomföras och dokumenteras.

**Internrevisionen rekommenderar att universitetsledningen säkerställer**

**A.** att Ladokkonsortiet tar fram styrande dokument inom området för informationssäkerhet, backuphantering samt förändringshantering för att fastställa och tydliggöra Ladokkonsortiets viljeinriktning och styrning inom respektive område.

Styrdokument för backuphantering bör baserat på underliggande behovsanalys av typ av backup och nödvändiga intervaller. Styrdokument för åtkomsthantering bör inkludera ett tydligt stöd i hur regelbunden granskning av priviligierade behörigheter och användaraktiviteter genomförs och dokumenteras.

[4] IS/IT – översyn System, IS/IT – översyn Drift, IS/IT – översyn Hantering
[5] Behörighet med kraftfulla rättigheter

**B.** att Ladokkonsortiet förankrar styrdokument i verksamheten samt att de följs upp för att säkerställa efterlevnad.

### *5.2 Hantering, rapportering och dokumentation av incidenter*

Det finns en dokumenterad incidenthantering av Ladok som är framtagen 23 januari 2018. Dokumentet syftar till att beskriva hur kritiska incidenter i systemet ska hanteras inom Ladokkonsortiet, bland annat beskrivs hur bedömning av incidenter ska göras, hur kommunikation ska ske, hur beslut om åtgärder ska tas samt hur eskalering till kriskommitté ska hanteras.

I augusti 2018 inträffade en omfattande incident som bidrog till att Ladok blev otillgängligt för användarna. Det var orsakat av ett planerat strömavbrott i samband med ett elarbete vid Umeå universitet. Reservkraftförsörjningen som normalt ska träda in kom inte igång vilket resulterade i att den primära serverhallen slogs ut. Samtidigt inträffade ytterligare ett fel som slog ut den sekundära serverhallen. Detta medförde att system stängdes ner okontrollerat samt att Ladok blev otillgängligt. Händelseförloppet under driftstoppet dokumenterades i en rapport som även innehöll förslag på förbättringsåtgärder. I rapportens summering bedöms hanteringen av incidenten ha fungerat bra. Genom intervjuer kan internrevisionen konstatera att incidenten hanterats bra i sin helhet.

Två oberoende utredningar om incidenten har tillsats. En genomförs av Umeå universitet och är inriktad på den fysiska infrastrukturen av datorhallarna. Ladokkonsortiet genomför en utredning som är inriktad på den logiska infrastrukturen av Ladok. Konsortiestyrelsens utredning ska även utreda behovet av att utöver den primära och sekundära serverhallen på Umeå universitet lagra backup av Ladok på ytterligare en ort. Tidigare version av Ladok driftades på flera ställen i landet och de backup som togs speglades till driftställen på andra orter.

### *5.3 CSN och LADOK*

CSN beslutar om och betalar ut studiestöd baserat på den information som registrerats i Ladok av lärosätena. Informationen hanteras via en tjänst med gränssnitt mot myndigheter som behöver åtkomst till information i Ladok. CSN hämtar information en gång per dygn. Om systemet är otillgängligt en längre period kan inte CSN få information om studenters registreringar och ett längre avbrott skulle medföra att informationen skulle behöva skickas manuellt från respektive lärosäte till CSN.

Enligt uppgift finns det manuella rutiner hos CSN att tillgå vid en sådan händelse. Incidenten i augusti 2018 inträffade inte under terminstid och påverkade inte CSN:s hantering av studiemedel. Internrevisionen anser dock att manuell hantering ökar risken för brister vid utbetalning av studiemedel, inte minst då CSN hanterar studiestöd till mellan 400 000- 500 000 studenter.

### *5.4 Riskanalys, kontinuitet- och katastrofhantering*

I samband med projektstarten av Ladok 3 genomfördes en riskanalys för att identifiera och värdera risker inom projektet samt för att skapa en vägledning för vilken ordning riskerna skulle hanteras. Riskanalysen resulterade i en lista innehållande risker och åtgärder med ansvarig person för respektive risk och åtgärd. Uppföljning av åtgärderna rapporterades i samband med projektledningsmötena samt vid styrgruppsmötena under projektets gång.

En kontinuitetsplan syftar till att vägleda, samla åtgärder och aktiviteter för att ge en god överblick över oväntade händelser samt stärka förmågan till fortsatt verksamhet vid olika typer av störningar. Ladokkonsortiet har sedan 2015 en dokumenterad kontinuitetsplan. Kontinuitetsplanen testades i april 2018 och aktiverades vid incidenten i augusti. Planen har reviderats efter driftstoppet och efterföljande utvärdering.

En bidragande orsak till internrevisionens granskning av Ladok är tidigare identifierad avsaknad av alternativ strömförsörjning till de datorhallar som driftar Ladok, samt att backup lagrades i samma hus där driften hanterades. Internrevisionen har genom fysisk granskning av datorhall samt intervju med driftansvarig vid Umeå universitet kunnat konstatera att det finns separat strömförsörjning av datorhallarna. Backup tas varje natt och lagras i både den primära och sekundära datorhallen. Den sekundära finns i en annan byggnad ca 600 meter från den primära datorhallen. Det finns en dieselgenerator till den primära datorhallen som testas en gång i månaden, vilket dokumenteras enligt etablerad underhållsplan. Åtkomst till datorhallen är begränsad då det krävs kort och personlig kod för att öppna dörren till datorhallen. Det finns en UPS[6] som ser till att strömförsörjningen fortgår en begränsad tid tills dieselgeneratorn startar, i händelse av ett strömavbrott. Det finns även brandlarm och larm för fukt i datorhallen. Golvet är upphöjt för att undvika vattenskador på utrustningen i händelse av översvämning.

[6] Uninterruptible power source

# 6 Ladok vid SLU

## *6.1 Styrande dokument*

**Det saknas eller förekommer brister i styrande dokument vid SLU för behörighetshantering, informationssäkerhet, backuphantering och förändringshantering avseende Ladok. Detta ökar bland annat risken för felaktig hantering av information.**

Granskningen har visat att det finns styrande dokument inom området för behörighetshantering, informationssäkerhet och backuphantering men att det förekommer brister och förbättringsområden i dokumenten.

I dokumentet Riktlinjer för behörigheter i Ladok beskrivs översiktligt hur man får behörighet i Ladok vid SLU. Det saknas beskrivning av hur behörigheter i systemet ska hanteras i samband med att en person ändrar anställning, institution eller avdelning samt om en person avslutar sin anställning. Vidare saknas beskrivning av hur regelbunden granskning av behörigheter ska ske samt hur priviligierade behörigheter ska hanteras.

I dokumentet Riktlinjer för informationssäkerhet (ua 2015.2.10-2118) vid SLU beskrivs övergripande arbetssätt inom informationssäkerhet samt vilka roller och ansvar som finns kopplat till informationssäkerhetsarbetet. Dokumentet är framtaget 2014-05-06 och det saknas uppgifter om när uppdatering ska ske. Internrevisionen har noterat att riktlinjen hänvisar till en av MSB:s föreskrifter, MSBFS 2009:10[7] som har ersatts med MSBFS 2016:1.

I dokumentet Riktlinjer för god drift och förvaltning av system beskrivs delvis hur systembackup ska hanteras. Det saknas en underliggande analys som syftar till att kravställa vilken typ av backup som genomförs av Ladokkonsortiet som är adekvat för SLU. Som myndighet är SLU ansvarig för att all information hanteras enligt gällande föreskrifter oavsett om informationen förvaras i universitetets lokaler, vid annat lärosäten, myndighet eller företag.

Det saknas styrande dokument för förändringshantering av Ladok inom SLU som beskriver förhållningsätt till förändringar, exempelvis krav på testning och godkännande av förändringar innan produktionssättning.

**Internrevisionen rekommenderar att universitetsledningen säkerställer**

**C.** att befintliga styrande dokument utvecklas inom SLU för att säkerställa en adekvat styrning av behörigheter. Dessa bör inkludera förändring och borttagande av behörigheter samt regelbunden kontroll av behörigheter och priviligierade användaraktiviteter.

[7] MSBFS 2009:10 föreskrifter och allmänna råd om statliga myndigheters informationssäkerhet

**D.** att beslut fattas om hur förändringshantering inom SLU ska bedrivas i Ladok.

**Internrevisionen rekommenderar att universitetsledningen överväger**

**E.** att genomföra analys för SLU:s behov av backuper som genomförs av Ladok centralt.

**F.** att etablera en process för att regelbundet revidera SLU:s styrande dokument rörande Ladok och hålla dem uppdaterade.

### *6.2 Hantering, rapportering och dokumentation av incidenter*

Det finns styrande dokument, i form av riktlinjer och processdokumentation, som beskriver rapportering av incidenter. Det finns fem sätt att rapportera incidenter generellt; anmälan via e-mail, webbformulär, telefon, fysiskt besök eller genom ett systemlarm. Gäller incidenten Ladok så finns det en supportsida på intranätet med kontaktuppgifter till systemansvarig, både via telefon och e-mail.

När en incident har rapporterats hamnar den hos en central funktion vid SLU som har till uppgift att samordna, analysera samt bedöma inrapporterade incidenter. I de fall incidenterna bedöms som allvarliga kan den centrala funktionen rapportera vidare till MSB.

### *6.3 Riskanalys, kontinuitet- och katastrofhantering*

**Det saknas dokumenterad riskanalys, kontinuitet- och katastrofplan som inkluderar Ladok proxy[8].**

Det finns en instruktion för riskhantering som beskriver syfte och genomförande av riskanalys, men det saknas en dokumenterad riskanalys för Ladok. Det har genomförts en informationssäkerhetsklassning av Ladok, men resultat har inte kommunicerats till Ladokkonsortiet i syfte att kravställa hanteringen av Ladok centralt utifrån arbetet med konfidentialitet, riktighet och tillgänglighet.

Det finns styrdokument som beskriver kontinuitetsplanering ur ett informationssäkerhetsperspektiv. Internrevisionen har genom intervjuer konstaterat att det saknas en dokumenterad kontinuitetsplan som inkluderar Ladok vid SLU.

Det finns en riktlinje för krishantering och krisorganisation vid SLU (ua 2015.1.1.1-2460) samt en dokumenterad process som översiktligt beskriver aktörer och aktiviteter för att hantera stora störningar i IT-miljön. Det saknas dock en dokumenterad katastrofplan som syftar till att i detalj beskriva vilka steg som ska vidtas i händelse av ett större avbrott vid SLU som inkluderar Ladok. Det kan exempelvis vara beskrivning av vilken ordning servrar ska prioriteras när de ska startas efter ett avbrott eller hur backup ska återläsas för att minska risken för dataförlust.

[8] Ladok proxy är namnet på SLU:s lokala kopia av Konsortiets Ladokdatabas.

**Internrevisionen rekommenderar att universitetsledningen säkerställer**

**G.** att SLU genomför en riskanalys av Ladok i syfte att identifiera risker och utvärdera hur dessa kan hanteras.

**H.** att en dokumenterad kontinuitetsplan/katastrofplan etableras för återställning av Ladok proxy inom SLU.

### *6.4 Behörighetsprocessen*

**Det saknas viktiga moment för att säkerställa en tillförlitlig behörighetshantering av Ladok, vilket ökar risken för felaktiga behörigheter och obehörig tillgång till information.**

En behörighetsprocess bör innehålla kontrollmoment för att säkerställa att åtkomst i system och underliggande infrastruktur endast tilldelas behöriga personer. Kontrollmomenten bör även hantera förändringar och borttagande av behörigheter. Priviligierade behörigheter, vilket innebär att behörigheten är mer kritisk och medför en högre risk, bör hanteras extra varsamt och regelbundet granskas, dels avseende vem som innehar en sådan behörighet dels vilka aktiviteter som utförs med behörigheten.

Hanteringen av Ladok sker inom avdelningen för lärande och digitalisering där avdelningschefen är systemägare för Ladok. Vid avdelningen finns även systemansvarig som delegerats visst ansvar för hanteringen av Ladok.

Behörighet beställs via Ladok och behörighetskontroll sker i kombination med systemet Idis. Idis är SLU:s identitets- och informationssystem samt katalog över studenter, anställda och verksamma. För att få behörighet till Ladok måste personen finnas i Idis. Det finns ett dokument som beskriver att tilldelning av behörigheter i Ladok endast ska ske efter godkännande av prefekt. För att få möjlighet att attestera i Ladok måste personen ha rollen ”Examinator” i Idis, vilken kataloganvarig i Idis på varje institution ansvarar för att hantera. För att få rollen ”Examinator” måste personen uppfylla angivna kompetenskrav som finns beskrivna i utbildningshandboken.

Det finns 17 olika typer av behörigheter i Ladok vid SLU. Samtliga behörigheter är skapade och administreras av systemansvarig för Ladok. Ett aktivt val har gjorts att dela upp åtkomsträttigheter i flera olika behörigheter för att undvika behörigheter som innehåller många olika åtkomsträttigheter. Internrevisionen har dock noterat att det är möjligt att inneha flera olika behörigheter som i kombination kan medföra ökad risk för obehörig åtkomst till funktioner och information i Ladok. Enligt uppgift går det dock inte att få en kombination av behörigheter som gör att du kan attestera en kurs som du själv går. Granskningen har visat att det saknas en underliggande analys för vilka risker som finns vid innehav av respektive behörighet samt risker vid olika kombinationer av behörigheter. Detta medför ökad risk att felaktig information registreras i Ladok.

SLU använder den lokala kopian, Ladok proxy, för att hantera integrationer med andra system på ett effektivt sätt. Ladok proxy uppdateras från Ladok centralt en gång per dygn. Det finns fem personer som har behörighet att logga in på den lokala Ladokdatabasen. Dessa personer arbetar som It-tekniker och kan i enlighet med sin arbetsroll logga in lokalt för att utföra sina arbetsuppgifter. Det sker viss loggning av deras aktiviteter men loggarna följs inte upp på en regelbunden basis, vilket medför en ökad risk för att obehörig hantering av information kan ske i den lokala Ladokdatabasen.

Det har under granskningen framkommit att det finns en informell process för att regelbundet granska användarkonton som inte varit aktiva de senaste sex månaderna. Dock är kontrollerna inte dokumenterade. Enligt internrevisionens bedömning saknas en formell process för att hantera förändringar, borttagande och regelbunden uppföljning av behörigheter. Det saknas även en formell process för regelbundet kontrollera priviligierade användaraktiviteter i Ladok. Därtill saknas beskrivning över vilka kontrollmoment som ska genomföras för att säkerställa att tilldelning, förändring och borttagande av behörigheter hanteras på ett ändamålsenligt sätt. Avseende borttagande och förändring av behörigheter i Ladok ansvarar respektive institution för att meddela Ladokansvarig att en behörighet ska tas bort. Sker inte denna kommunikation riskerar behörigheten att finnas kvar i Ladok och utgör då en säkerhetsrisk. Detta tillsammans med en avsaknad av analys för vilka risker som finns vid innehav av olika kombinationer av behörigheter ökar risken för obehörig åtkomst till funktioner och information i Ladok.

**Internrevisionen rekommenderar att universitetsledningen säkerställer att**

**I.** det finns kontrollmoment i behörighetsprocessen för Ladok som säkerställer att behörigheter och priviligierade användaraktiviteter granskas regelbundet samt att förändring och borttagande av behörigheter hanteras på ett ändamålsenligt sätt.

**Internrevisionen rekommenderar att universitetsledningen överväger att**

**J.** genomföra en analys för vilka risker som finns för innehav av respektive behörighet i Ladok, samt vilka risker som kan uppstå vid olika kombinationer av behörigheter.

Inga Astorsdotter
Internrevisionschef

Lisbeth Sundkvist Johansson
Internrevisor

Sveriges lantbruksuniversitet
Swedish University of Agricultural Sciences

**Rektor** | 2019-06-03 | SLU ID: SLU.ua 2018.1.1.2-3887

# Åtgärdsplan med anledning av internrevisionens rapport angående Ladok

Nedan refereras till punkterna i internrevisionens rekommendationer:

*Sammanfattning*

*Internrevisionen har i enlighet med revisionsplanen för 2018 granskat hanteringen av systemet Ladok centralt vid Ladokkonsortiet och lokalt vid SLU. Syftet med granskning var att bedöma i vilken utsträckning den interna styrning avseende Ladok är effektiv, ändamålsenlig och innehar tillfredsställande säkerhet.*

*Internrevisionens sammanfattande bedömning är att hanteringen av Ladok kan förbättras såväl centralt som lokalt vid SLU. Det finns brister som riskerar att påverka styrning och säkerhet vilket kan innebära att obehöriga får tillgång till information samt att det kan ske felaktiga utbetalningar av studiemedel från CSN. Internrevisionens bedömning grundar sig i huvudsak på följande;*

1. *Ladok centralt saknas styrdokument för informationssäkerhet, backuphantering samt förändringshantering.*
2. *SLU saknar eller det förekommer brister i styrande dokument för Ladok inom behörighetshantering, informationssäkerhet, backuphantering och förändringshantering.*
3. *SLU saknar dokumenterad riskanalys, kontinuitet- och katastrofplan som inkluderar Ladok.*
4. *SLU saknar viktiga moment för att säkerställa en tillförlitlig behörighetshantering av Ladok.*

*De väsentligaste rekommendationerna är följande;*

*• Att universitetsledningen säkerställer att Ladokkonsortiet tar fram styrande dokument inom området för informationssäkerhet, backuphantering samt förändringshantering för att fastställa och tydliggöra konsortiets viljeinriktning och styrning inom respektive område.*

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

Tel: 018-67 10 00 (vx)
Mobilnr: XXX-XXX
fornamn.efternamn@slu.se

*• Att befintliga styrande dokument utvecklas inom SLU för att säkerställa en adekvat styrning av behörigheter. Dessa bör inkludera förändring och borttagande av behörigheter samt regelbunden kontroll av behörigheter och priviligierade användaraktiviteter.*

*• Att SLU genomför en riskanalys av Ladok i syfte att identifiera risker och utvärdera hur dessa kan hanteras samt att en dokumenterad kontinuitetsplan/katastrofplan etableras för återställning av Ladok proxy inom SLU.*

*• Att det vid SLU finns kontrollmoment i behörighetsprocessen för Ladok som säkerställer att behörigheter och priviligierade användaraktiviteter granskas regelbundet samt att förändring/borttagande av behörigheter hanteras ändamålsenligt.*

*Rekommendationerna är följande:*

**A.** att Ladokkonsortiet tar fram styrande dokument inom området för informationssäkerhet, backuphantering samt förändringshantering för att fastställa och tydliggöra Ladokkonsortiets viljeinriktning och styrning inom respektive område. Styrdokument för backuphantering bör baserat på underliggande behovsanalys avseende typ av backup och nödvändiga intervaller. Styrdokument för åtkomsthantering bör inkludera tydligt stöd i hur regelbunden granskning av priviligierade behörigheter och användaraktiviteter genomförs och dokumenteras.

**B.** att Ladokkonsortiet förankrar styrdokument i verksamheten samt att de följs upp för att säkerställa efterlevnad.

**C.** att befintliga styrande dokument utvecklas inom SLU för att säkerställa en adekvat styrning av behörigheter. Dessa bör inkludera förändring och borttagande av behörigheter samt regelbunden kontroll av behörigheter och priviligierade användaraktiviteter.

**D.** att beslut fattas om hur förändringshantering inom SLU ska bedrivas i Ladok.

**E.** Internrevisionen rekommenderar att universitetsledningen överväger att genomföra analys för SLU:s behov av backuper som genomförs av Ladok centralt.

**F.** att etablera en process för att regelbundet revidera SLU:s styrande dokument rörande Ladok och hålla dem uppdaterade.

**G.** att SLU genomför en riskanalys av Ladok i syfte att identifiera risker och utvärdera hur dessa kan hanteras.

**H.** att en dokumenterad kontinuitetsplan/katastrofplan etableras för återställning av Ladok proxy inom SLU.

**I.** att det finns kontrollmoment i behörighetsprocessen för Ladok som säkerställer att behörigheter och priviligierade användaraktiviteter granskas

regelbundet samt att förändring och borttagande av behörigheter hanteras på ett ändamålsenligt sätt.

J. **Internrevisionen rekommenderar att universitetsledningen överväger** att genomföra en analys för vilka risker som finns för innehav av respektive behörighet i Ladok, samt vilka risker som kan uppstå vid olika kombinationer av behörigheter.

## Åtgärder

**Punkt A.** Som internrevisionen skriver ägs Ladok gemensamt och universitetsledningen vet att Ladokkonsortiet redan ser redan över relevanta styrande dokument inom området för informationssäkerhet, backuphantering samt förändringshantering. Ladokstyrelsen har också redan genomfört en extern granskning(HP och Atea) av bland annat den logiska infrastrukturen, en utredning som visade att Umeå universitet följer best praxis inom området.

Universitetsledningen kommer givetvis även i fortsättningen via sin roll i konsortiets stämma och via övriga kontakter kontinuerligt bevaka och verka för att adekvata åtgärder hela tiden vidtas.

**Punkt B.** Universitetsledningen är trygg med att Ladokkonsortiet som tidigare förankrar styrdokument i verksamheten samt att de följs upp för att säkerställa efterlevnad.

Universitetsledningen kommer givetvis även i fortsättningen via sin roll i konsortiets stämma och via övriga kontakter kontinuerligt bevaka denna fråga.

**Punkt C och D.** Dokumentet ”Riktlinjer för behörigheter i Ladok” finns redan klart och andra relevanta dokumentet kommer att ses över.

**Ansvarig:** Avd. för lärande och digitalisering

**Klart:** 2019-12-31

**Punkt E.** Som internrevisionen skriver ägs Ladok gemensamt och behov av backuper som genomförs av Ladok centralt bestäms gemensamt av medlemmarna efter enkäter mm där vi kan framföra synpunkter. SLU kan inte kräva någon avvikande backuppfrekvens.

**Punkt F.** En process för att se över och revidera nödvändiga dokumentet kommer att etableras och ske på årlig basis.

**Ansvarig:** Avd. för lärande och digitalisering

**Klart:** 2019-12-31

**Punkt G.** Riskanalyser och hur dessa kan hanteras genomförs just nu av Ladok centralt vilket under 2019 kommer att resultera i rekommendationer även till lärosätena. Universitetsledningen anser att det räcker.

**Ingen åtgärd**.

**Punkt H.** Ladok Proxy har SLU byggt som en extra säkerhet vilket inte alla universitet har. Återställning av data är inget problem då den uppdateras en gång per dygn från Ladok centralt. Däremot kommer vi att se över återställning av Ladok proxy servrarna inom SLU.

**Ansvarig:** Avd. för lärande och digitalisering och IT-avdelningen

Klart: 2019-12-31

**Punkt I.** Dokumentet ”Riktlinjer för behörigheter i Ladok” finns redan klart (se punkt C och D).

**Punkt J.** Behörighet söks via Ladok och en kontroll sker i Idis att prefekten på institutionen godkänt behörigheten. Universitetsledningen anser att risker kopplade till behörigheter är små vid SLU då behörighetskontrollen vid SLU hanteras av prefekters medgivande, Idis-systemet och nu med de nya ”Riktlinjer för behörigheter i Ladok” bör riskerna minimeras ytterligare.

**Ingen åtgärd**.