Stewe Löfberg, Ingrid Linse, Kristina Palmström Schäder, Jonas Sjöberg
046-3597030
stewe.lofberg@lund.se

Utbildningsnämnden

Yttrande över: Kommunrevisionens granskning av behörighet till känsliga uppgifter samt interna kontroller

Sammanfattning

De förtroendevalda revisorerna har gett Ernst & Young (EY) i uppdrag att granska behörighet och åtkomst till IT-system med känsliga uppgifter samt interna kontroller. Syftet med granskningen har varit att bedöma om nämndernas arbete med behörigheter, åtkomster och loggkontroll i verksamhetssystemen hanteras på ett ändamålsenligt sätt och med tillräcklig intern kontroll.
Inom ramen för granskningen har vissa avvikelser noterats, framförallt i ett av systemen, Unikum.
Vidare har granskningen visat att barn- och skolnämnden och utbildningsnämnden behöver se över systemägarskapen i syfte att renodla ansvarsfördelningen.
Revisorerna önskar svar på vilka åtgärder som kommer att vidtas med anledning av vad som framkommit i granskningen och rekommendationer som lämnats senast den 18 december 2018.

Beslutsunderlag

Utbildningskansliets tjänsteskrivelse 2018-11-26
Missiv till revisionsrapport 2018-09-19
Revisionsrapport ”Granskning av behörighet till känsliga uppgifter samt interna kontroller”.

Barnets bästa

Ärendet påverkar barns och ungdomars bästa, då det gäller behörighet och åtkomst till IT-system med känsliga personuppgifter.

Ärendet

De förtroendevalda revisorerna har gett Ernst & Young (EY) i uppdrag att granska behörighet och åtkomst till IT-system med känsliga uppgifter samt interna kontroller. Syftet med granskningen har varit att bedöma om nämndernas arbete med behö-

righeter, åtkomster och loggkontroll i verksamhetssystemen hanteras på ett ändamålsenligt sätt och med tillräcklig intern kontroll.
Inom ramen för granskningen har vissa avvikelser noterats, framförallt i ett av systemen, Unikum.
Vidare har granskningen visat att barn- och skolnämnden och utbildningsnämnden behöver se över systemägarskapen i syfte att renodla ansvarsfördelningen.

Utifrån granskningsresultatet rekommenderas samtliga nämnder att:

- Se över rutiner för gallring av behörigheter.

Utifrån granskningsresultatet rekommenderas utbildningsnämnden och barn- och skolnämnden att:

- Se över och säkerställa att ansvarsfördelningen avseende ägarskap och förvaltning av granskade IT-system är tydlig
- Säkerställa att systematiska loggkontroller genomförs i samtliga system
- Tillse att det finns ändamålsenliga rutiner för behörighetstilldelning och roller.

Utbildningsförvaltningens synpunkter

Nedan följer svar på respektive punkt:

Översyn av rutiner för gallring av behörigheter

I förvaltningsplanen för Procapita BoU beskrivs rutinen i avsnitt 3.3.2.5 Avslut och borttagning av behörigheter. Rutinen fördelar ansvar på ett tydligt sätt.
Eftersom vi i dagsläget inte har personnummer eller andra unika identifikationsid kopplade till användarkontona, går det inte att samköra med andra register, t ex Personec.
När vi går över till Tieto Education, kommer alla användare kopplas till sitt personnummer. Detta möjliggör rutinmässiga kontroller på central nivå i en helt annan omfattning. Vi ser även möjlighet att koppla användarna genom att tilldela dem AD-grupper genom vilka behörigheterna styrs.

I förvaltningsplanen för PMO beskrivs rutiner i avsnitt 5.3.7 - Avslut och borttagning av behörigheter, där det står att: Ansvarig chef/ samordnare är ansvarig att rapportera till Servicedesk/systemförvaltare när användare inte längre ska vara behörig till systemet eller ha åtkomst till enheten. Systemförvaltare går utifrån detta månadsvis genom behörigheter och inaktiverar behörighet för skolsköterskor och årsvis inaktivering för övriga användare. Skolöverläkare och systemförvaltare går utöver detta

igenom vilka användare som ska vara aktiva samt vilka enheter de ska vara kopplade till i samband med läsårsstart.

I förvaltningsplanen för Unikum anges att behörighetstilldelning ska ske enligt Lunds kommuns informationssäkerhetsriktlinjer.
Användarkonton i Unikum tilldelas och tas bort i enlighet med registreringar i vårt elevregister Procapita. För elever följer detta läsårets tider och för personal anställningstider.
Det finns också s.k. priviligierade användarkonton med högre behörighet t ex administratörer och observatörer.
Dessa konton ska hållas till ett minimum eftersom det alltid finns risk att känslig information kan röjas. Tillgång till och avslut av priviligierade konton/behörigheter beslutas av behörig chef. Systemförvaltare administrerar detta och håller ett register över vem som ska ha vilken priviligierad behörighet på resp enhet.

Se över och säkerställa att ansvarsfördelningen avseende ägarskap och förvaltning av granskade IT-system är tydlig

Kommunrevisionen har påtalat att system som helt eller delvis avser barn- och skolnämnden hanteras av utbildningsförvaltningen, vilket gör att ett ansvarsutkrävande försvåras.
Vi kan konstatera att utbildningsnämnden har detta ansvar genom skrivelser i sitt reglemente. Det är utbildningsdirektören som är Systemägare, vilket beskrivs i Förvaltningsplanen. I densamma beskrivs förvaltningsfunktionen. Däremot saknas det forum där representanter för barn- och skolnämnden tillsammans med systemägare och systemförvaltare tillsammans tydliggör ansvarsfördelningen.
En möjlighet skulle kunna vara att upprätta överenskommelser i form av personuppgiftsbiträdesavtal för att säkerställa att ansvarsfördelningen avseende ägarskap och förvaltning av IT-system är tydlig mellan utbildningsnämnden och barn- och skolförvaltningen.

För Unikums del är ansvar och samarbete tydligt beskrivet i förvaltningsplanerna för våra digitala system. Det finns beskrivet hur en styrgrupp med bemanning från skolförvaltningar ska arbeta med styrning och utveckling. Denna styrgrupp har dessvärre inte återbemannats med personal i samband med organisations- och personalförändringar. I den situation som råder nu kan detta felaktigt uppfattas som att det inte finns något planerat strukturerat samarbete mellan förvaltningarna.

Säkerställa att systematiska loggkontroller genomförs i samtliga system

Ändamålsenliga funktioner så att systemförvaltare kan utföra systematiska kontrollerna saknas eller är otillräckliga i befintliga system. Vi behöver kommunicera med befintliga leverantörer så att de tar fram

fullgoda tjänster. I kommande upphandlingar måste krav ställas för att säkerställa att upphandlade system möter våra krav.

Tillse att det finns ändamålsenliga rutiner för behörighetstilldelning och roller

Procapita BoU och PMO uppfyller detta krav genom skrivelser i förvaltningsplanerna.
För Unikum finns ändamålsenliga rutiner för behörighetstilldelning i enlighet med förvaltningsplan och kommunens riktlinjer. Däremot behöver vi i samarbete med leverantören utveckla behörigheterna så att de blir mer ändamålsenliga och utformas efter nya och förändrade behov.

Förvaltningens förslag till beslut

Utbildningsnämnden föreslås besluta

att lämna svar till Lunds kommuns revisorer i enlighet med tjänsteskrivelse 2018-11-26.

Stefan Norrestam
Utbildningsdirektör

Stewe Löfberg
Nämndsekreterare

Beslut expedieras till:
Lunds kommuns revisorer
Akten