Innehållsförteckning granskning av: Behörighetsfördelning i känsliga system och interna kontroller.

1 Missiv angående granskning av behörighetsfördelning i känsliga system och interna kontroller:

LESSEBO KOMMUN 2021-11-19
Kommunens revisorer

Till
Kommunstyrelsen, Barn- och utbildningsnämnden samt Socialnämnden för svar
Kommunfullmäktige och gemensamma nämnden för lönesamverkan för kännedom

Granskning av behörighetsfördelning i känsliga system och interna kontroller

EY har fått i uppdrag av de förtroendevalda revisorerna i Lessebo kommun att genomföra en granskning med syfte att bedöma om barn- och utbildningsnämnden, socialnämnden och kommunstyrelsens arbete med behörigheter, åtkomster och loggkontroller i verksamhetssystemen hanteras på ett ändamålsenligt sätt och med tillräcklig intern kontroll. Granskningen syftar även till att följa upp om den gemensamma nämnden för lönesamverkan har vidtagit åtgärder för att stärka kontroller, utifrån rekommendationen i 2019 års granskning.

Vår bedömning är att det på övergripande nivå finns ett behov av att arbeta vidare med informationssäkerhetspolicyn och hur dess intentioner ska översättas i grundläggande krav rörande behörigheter, gallring och loggkontroller. Vidare bör ansvarsfördelningen mellan centrala IT och förvaltningarna som har ansvar för verksamhetssystemen tydliggöras.

Granskningen visar att socialnämnden har riktlinjer gällande roller, ansvar och till viss del behörigheter och loggkontroller. Dessa efterlevs dock i flera delar inte alls och skulle behöva uppdateras.

Avseende utbildningsnämnden bedömer vi att det finns ett behov av att upprätta övergripande systemdokumentation samt upprätta riktlinjer och rutiner för såväl behörighetstilldelning som loggkontroller. Det är positivt att man inom nämnden genomför systemspecifik användarutbildning med alla nya användare.

Utifrån granskningsresultatet rekommenderar vi kommunstyrelsen att:

- Uppdra åt kommunledningsförvaltningen att utifrån informationssäkerhetspolicyn ta fram instruktioner för systemägarna, IT-driften och användarna av systemen. Vidare bör kommunledningsförvaltningen tydliggöra ansvaret mellan centrala IT och förvaltningarna där det tydliggörs på vilket sätt stöd ska ges t.ex. i form av utbildningar eller kommungemensamma rutiner.
- I egenskap av systemägare för Evolution uppdra åt kommunledningsförvaltningen att upprätta generell systemdokumentation samt generella riktlinjer och rutiner för verksamhetssystemet.

Vi rekommenderar socialnämnden att:

- Uppdra åt socialförvaltningen att uppdatera sin systemdokumentation, riktlinjer och rutiner

för verksamhetssystemet Procapita. Vidare rekommenderas nämnden ta del av de granskningsprotokoll för loggkontroller som upprättas som en del av sin interna kontroll.

Vi rekommenderar barn- och utbildningsnämnden att:

- Uppdra åt förvaltningen att i samråd med kommunledningskontoret upprätta systemdokumentation, riktlinjer och rutiner för behörigheter och loggning i sin hantering av elevakter.

Revisorerna bedömer att det krävs att åtgärder vidtas med anledning av rapportens iakttagelser och avser att genomföra en uppföljning längre fram.
Kommunens revisorer överlämnar härmed granskningsrapporten och önskar svar på rapportens rekommendationer samt vilka åtgärder som planeras att vidtas. Svar önskas senast 2021-01-30.
För kommunens revisorer

Örjan Davoust	Per-Anders Johansson
Ordförande	***Vice ordförande***

2 Socialnämndens svar på revisorernas missiv:
Lessebo kommuns revisorer har gett EY i uppdrag att genomföra en granskning med syfte att bedöma om Socialnämndens arbete med behörigheter, åtkomster och loggkontroller i verksamhetssystemen hanteras på ett ändamålsenligt sätt och med tillräcklig intern kontroll. Granskningen visar på behov av uppdatering av riktlinjer samt brister i följsamhet. Socialförvaltningen kommer att uppdatera systemdokumentation, riktlinjer och rutiner för verksamhetssystemet Procapita samt redovisa utförda loggkontroller om socialnämnden beslutar att detta kontrollmoment ska ingå i intern kontroll 2022.

3 Barn- och utbildningsnämndens svar revisorernas missiv.
Nämnden beslutar att uppdra åt förvaltningen att i samråd med kommunledningskontoret upprätta systemdokumentation, riktlinjer och rutiner för behörigheter och loggning i sin hantering av elevakter.
Arbete har påbörjats med gemensamma behörighetsrutiner för Evolution som ska kompletteras med förvaltningsspecifika rutiner. Nämndsekreterare på Barn- och utbildningsförvaltningen kommer att ansvara för att ta fram förvaltningsspecifika riktlinjer och rutiner för behörigheter och loggning gällande hantering av förvaltningens elevakter. Målet är att under första halvan av 2022 ta fram dessa riktlinjer och rutiner samt implementera dem som en del av förvaltningens årshjul. Det här för att säkerhetsställa att rutinen ingår i ett levande dokument som är en naturlig del av förvaltningens arbete. Systemdokumentation finns i den versionsbeskrivning som leverantören tillhandahåller, samt i det driftsavtal som tecknas med IT-avdelningen.

4 Kommunstyrelsens svar på revisorernas missiv.
Revisorerna i Lessebo kommun har gett EY i uppdrag att genomföra en granskning med syfte att bedöma om Barn- och utbildningsnämnden, Socialnämnden och Kommunstyrelsens arbete med behörigheter, åtkomster och loggkontroller i verksamhetssystemen hanteras på ett ändamålsenligt sätt och med tillräcklig intern kontroll. Utifrån granskningsresultatet rekommenderar revisorerna Kommunstyrelsen att: 1) Uppdra åt kommunledningsförvaltningen att utifrån informationssäkerhetspolicyn ta fram instruktioner för systemägarna, IT-driften och användarna av systemen. Vidare bör kommunledningsförvaltningen tydliggöra ansvaret mellan centrala IT och förvaltningarna där det tydliggörs på vilket sätt stöd ska ges t.ex. i form av utbildningar eller kommungemensamma rutiner. 2) I egenskap av systemägare för Evolution uppdra åt kommunledningsförvaltningen att upprätta generell systemdokumentation samt generella riktlinjer och rutiner för verksamhetssystemet.

5 Revisorernas ställningstagande: Revisorerna avslutar ärendet.

6 Granskningsrapport behörighetsfördelning i känsliga system och interna kontroller.
Rapporten finns som fristående dokument.

Granskningsrapport 2021
Genomförd på uppdrag av revisorerna
nov 2021

Lessebo kommun

Granskning av behörighetsfördelning i känsliga system samt interna kontroller

Building a better working world

Innehåll

1. Sammanfattning

EY har på uppdrag av de förtroendevalda revisorerna i Lessebo kommun granskat två verksamhetssystem hos socialnämnden och utbildningsnämnden samt kommunstyrelsens samordnande roll i syfte att bedöma om deras arbete med behörigheter, åtkomster och loggkontroller hanteras på ett ändamålsenligt sätt och med tillräcklig intern kontroll.

Vår bedömning är att det på övergripande nivå finns ett behov av att arbeta vidare med informationssäkerhetspolicyn och hur dess intentioner ska översättas i grundläggande krav rörande behörigheter, gallring och loggkontroller. Vidare bör ansvarsfördelningen mellan centrala IT och förvaltningarna som har ansvar för verksamhetssystemen tydliggöras. Det finns ett behov av att proaktivt samla och utbilda förvaltningarna kring gemensamma frågor såsom generell informationssäkerhet, behörighetstilldelning, gallring och kontroller.

Granskningen visar att socialnämnden har riktlinjer gällande roller, ansvar och till viss del behörigheter och loggkontroller. Dessa efterlevs dock i flera delar inte alls och skulle behöva uppdateras. En skriftlig systemförvaltningsorganisation med roller och ansvar, en tydlig rutin och dokumentation kring beställning av behörigheter och systemspecifik utbildning och information om loggning skulle skapa en robustare och mindre personberoende systemadministration med förbättrad kontrollmiljö.

Avseende utbildningsnämnden bedömer vi att det finns ett behov av att upprätta övergripande systemdokumentation samt upprätta riktlinjer och rutiner för såväl behörighetstilldelning som loggkontroller. Det är positivt att man inom nämnden genomför systemspecifik användarutbildning med alla nya användare.

Gällande nämnden för lönesamverkan är tydligt att granskningen 2019 resulterat i förbättringar i nämnden. Behörigheter är en punkt i internkontrollplan, tydliga rutiner finns avseende behörigheter och gallring. Tilldelning av behörighet sker numera kopplat till organisationen genom skriftlig (digital) ansökan av behörig chef.

Utifrån granskningsresultatet rekommenderar vi kommunstyrelsen att:

- Uppdra åt kommunledningsförvaltningen att utifrån informationssäkerhetspolicyn ta fram instruktioner för systemägarna, IT-driften och användarna av systemen. Vidare bör kommunledningsförvaltningen tydliggöra ansvaret mellan centrala IT och förvaltningarna där det tydliggörs på vilket sätt stöd ska ges t.ex. i form av utbildningar eller kommungemensamma rutiner.
- I egenskap av systemägare för Evolution uppdra åt kommunledningsförvaltningen att upprätta generell systemdokumentation samt generella riktlinjer och rutiner för verksamhetssystemet.

Vi rekommenderar socialnämnden att:

- Uppdra åt socialförvaltningen att uppdatera sin systemdokumentation, riktlinjer och rutiner för verksamhetssystemet Procapita. Vidare rekommenderas nämnden ta del av de granskningsprotokoll för loggkontroller som upprättas som en del av sin interna kontroll.

Vi rekommenderar barn- och utbildningsnämnden att:

- Uppdra åt förvaltningen att i samråd med kommunledningskontoret upprätta systemdokumentation, riktlinjer och rutiner för behörigheter och loggning i sin hantering av elevakter.

2. Inledning

2.1. Bakgrund

Behörigheter till kommunens verksamhetssystem som innehåller känsliga persondata regleras av olika lagar såsom dataskyddsförordningen. Det ska finnas en rättslig grund för de uppgifter som kommunen registrerar om personer. Uppgifterna ska också skyddas så att ingen obehörig kan få del av uppgifterna.

Socialnämndens och utbildningsnämndens verksamheter har med åren blivit alltmer beroende av IT-stöd, vilket innebär nya former av hot och risker. Behörighetsstyrning och interna kontroller är en viktig del i arbetet för att skydda uppgifterna och möta lagkrav. I detta ligger att upprätta och upprätthålla rättigheter för användare i de IT-system som brukas, så att användarna enbart får och har åtkomst till den information som behövs i det dagliga arbetet. En bristfällig styrning och kontroll inom området kan riskera att verksamheten inte bedrivs på ett ändamålsenligt sätt samt att känslig information sprids till icke behöriga.

I 2019 års granskning av löneprocessen konstaterades att det inte genomfördes några kontroller kopplat till de aktiviteter/åtgärder som utförs av personer med höga behörigheter i lönesystemet (systemförvaltarna) samt om behörigheter för anställda i kommunen överensstämde med gällande organisationsstruktur. Den gemensamma nämnden för lönesamverkan rekommenderades därför att genomföra systematiska och dokumenterade kontroller av behörigheter.

De förtroendevalda revisorerna har med utgångspunkt i ovanstående beslutat genomföra en granskning avseende hanteringen av behörigheter i relation till känslig persondata samt följa upp om nämnden för lönesamverkan har vidtagit åtgärder för att stärka kontroller av behörigheter.

2.2. Syfte och revisionsfrågor

Syftet med granskningen är att bedöma om barn- och utbildningsnämnden, socialnämnden och kommunstyrelsens arbete med behörigheter, åtkomster och loggkontroller i verksamhetssystemen hanteras på ett ändamålsenligt sätt och med tillräcklig intern kontroll. Granskningen syftar även till att följa upp om den gemensamma nämnden för lönesamverkan har vidtagit åtgärder för att stärka kontroller, utifrån rekommendationen i 2019 års granskning.

I granskningen besvaras följande revisionsfrågor:

- Är ansvars- och arbetsfördelningen inom organisationen tillräckligt tydlig?
- Är uppföljning och utvärdering inom området ändamålsenlig?
- Sker en tillräcklig styrning av behörigheter till känsliga verksamhetssystem?
- Säkerställer nämnderna att tillräcklig intern kontroll inom området har upprättats för att hindra otillåten åtkomst till och spridning av känslig information?

Avseende den gemensamma nämnden för lönesamverkan besvaras följande fråga:

- Genomför nämnden systematiska och dokumenterade kontroller av behörigheter såsom aktiviteter som utförts av personer med höga behörigheter i lönesystemet, att registrerade behörigheter för anställda överensstämmer med gällande organisationsstruktur och attestförteckning samt om behörig chef har undertecknat blanketten vid förändring av behörigheter?

2.3. Genomförande

Granskningen omfattar två verksamhetssystem inom socialnämndens och utbildningsnämndens ansvarsområde. Följande verksamhetssystem omfattas av granskningen:

- Procapita/Lifecare inom individ- och familjeomsorgen
- Evolution

Granskningen har skett genom dokumentstudier och intervjuer med ansvariga tjänstepersoner (se bilaga 1). Verifiering av den interna kontrollen har skett genom loggkontroller i ett verksamhetssystem inom utbildningsnämndens verksamhetsområde och ett inom socialnämndens verksamhetsområde. Samtliga intervjuade har beretts tillfälle att sakgranska rapporten. Sakgranskningen är genomförd 11 oktober 2021 – 15 oktober 2021.

Kommunstyrelsen granskas utifrån sitt lednings- och samordningsansvar.

2.4. Revisionskriterier

2.4.1. Kommunallagen (2017:725)

Kommunallagens 6 kapitel redogör för kommunstyrelsens och nämndernas uppgifter. 1 § fastställer att kommunstyrelsen ska leda och samordna kommunens angelägenheter och ha uppsikt över övriga nämnder.

Nämnderna ska enligt 6 § inom sitt ansvarsområde se till att verksamheten bedrivs i enlighet med kommunfullmäktiges mål och riktlinjer. Därtill ska nämnderna se till att den interna kontrollen är tillräcklig.

2.4.2. Dataskyddsförordningen (GDPR)

Den 25 maj 2018 trädde dataskyddsförordningen (GDPR) i kraft och ersatte personuppgiftslagen (PUL). Förordningen innebär stärkta rättigheter och skydd för individen vad gäller information och samtycke samt ett ökat ansvar för personuppgiftsansvariga. Ett sätt att säkerställa att personuppgiftsbehandlingen är i överensstämmelse med lagstiftningen kan vara att anta uppförandekoder, interna riktlinjer och förfaranden.

2.4.3. Informationssäkerhetspolicy

Kommunfullmäktige beslutade om policyn 2020-03-01. Policyn gäller för samtliga nämnder och kommunala bolag.

I policyn anges att informationssäkerhet handlar om att upprätthålla rutiner och skydd av information utifrån följande nivåer:

- Tillgänglighet
- Riktighet
- Konfidentialitet
- Spårbarhet

3. Granskningsresultat

3.1. Ansvarsfördelning och övergripande styrning

Enligt kommunens informationssäkerhetspolicy ska varje verksamhet ansvara för sina informationstillgångar och att det är upp till förvaltningarna att bestämma hur detta skall göras.

Av informationssäkerhetspolicy tydliggörs vilka roller som har ansvar för verksamhetssystemens förvaltning:

- Alla – följer policy och instruktioner, delar kunskap, deltar i utbildning och rapporterar incidenter
- Chef – ser till att informationstillgångar statas, hanteras och avslutas korrekt
- Beredskap- och säkerhetssamordnare – ansvarar för informationssäkerhet och ger stöd
- IT chef – ansvarar för operativ drift och ger stöd till systemägare
- Systemägare/förvaltningschef – ansvarar för informationstillgångar och utser
- Systemansvarig – ansvarar för den dagliga användningen.

Inom kommunledningskontoret finns IT-chef och en IT-enhet med tre anställda. IT-enhetens primära uppgift är att säkra driften av kommunens olika verksamhetssystem. Ett arbete pågår centralt med att göra en systeminventering, en klassificering av informationstillgångarna och skapa rutiner för behörigheter, detta i syfte att ta fram instruktioner för förvaltningar och bolag där tydliggör ansvar och gällande riktlinjer.

Man arbetar också med att teckna avtal mellan IT-enheten och förvaltningarna för att klargöra sina respektive ansvarsområden med t.ex. behörighetstilldelning. Grundläggande behörighet ges idag av IT-enheten per automatik när nya medarbetare läggs in i personalsystemet. Active Directory (AD) som styr detta delas med flera kommuner och kommunala bolag. Grundläggande behörighet ges vid tex. nyanställning vilket är en förutsättning för att sedan kunna ges behörighet till verksamhetssystem. Detta finns dokumenterat i tjänstebeskrivning – behörighet och konton.

I intervju framkommer att inga utbildningar planeras eller samordnas via centrala IT-enheten. Enheten finns som stöd för driften av systemen till förvaltningarna och det är upp till verksamheterna att anmäla behov av stöd.

3.1.1. Bedömning

Vi bedömer att informationssäkerhetspolicyn i stort ger en tydlig bild av tänkt ansvarsfördelning och att policyn uttrycker VAD som ska göras.

Vi ser däremot ett behov av att arbeta vidare med policyn och skapandet av instruktioner för såväl förvaltningarna (systemägarna), IT-driften och användare för HUR detta ska ske.

Ansvarsfördelningen mellan centrala IT och förvaltningarna kan med fördel klargöras.

IT-enheten kan också ta ett större ansvar i att proaktivt samla och utbilda förvaltningarna kring gemensamma frågor såsom generell informationssäkerhet, behörighetstilldelning,

gallring och kontroller. Detta för att säkerställa en tillräcklig informationssäkerhet enligt beslutad policy.

3.2. Procapita/Lifecare

Procapita/Lifecare är individ och familjeomsorgens verksamhetssystem (IFO). Systemet används i huvudsak av handläggare och ekonomiadministratörer på IFO.

På förvaltningen finns två systemansvariga, en inom IFO och en inom omsorgen. Dessa tillsammans med en verksamhetsutvecklare som sitter centralt på socialförvaltningen har full behörighet i verksamhetssystemet.

Därutöver finns inom IFO ett 30-tal användare däribland ett antal externa användare från familjerätten i Växjö. Dessa användare har handläggarroller i systemet där behörigheterna är anpassade efter arbetsuppgifterna. Mallar finns för de olika handläggarrollerna och de behörigheter de ska tilldelas. Systemansvarig kan lägga till nya roller och lägga till eller ta bort specifika behörigheter.

3.2.1. Behörigheter

Tillgång till och behörighet i systemet ges till nyanställda av systemansvarig efter muntlig beställning normalt sett via telefon från anställande chef. Det samma gäller för familjerätten i Växjö. Ingen dokumentation sker vid tilldelning. Skulle systemansvarig vara frånvarande ersätts denne av motsvarande funktion inom omsorgen.

Vid förändringar av arbetsuppgifter för en anställd eller att denne slutar ska anmälan ske av ansvarig chef. Den intervjuade uppger dock att detta ofta brister.

I dokumentet, rutin för loggkontroll för informationshantering och dokumentation i akter på individ och familjeomsorgen upprättad 15 nov 2015 framgår att det är verksamhetschefen som är övergripande ansvarig för hantering av akter inom sitt verksamhetsområde.

Senaste gallring av akter i systemet genomfördes 7 maj 2018 med hjälp av Sydarkivera. Intervjuad är osäker på om rutin finns för hur ofta detta ska ske och hur det ska gå till. Systemansvarig försöker gallra behörigheter löpande då denne får kännedom om att medarbetare slutar eller byter tjänst. Handläggare från familjerätten i Växjö som inte varit inloggade i systemet på ett år tas bort ut systemet av systemansvarig. Enligt uppgift meddelar inte alltid familjerätten i Växjö när anställningar avslutas eller förändras. Då Växjö och Lessebo delar AD (tilldelning av grundläggande behörighet) kan inte medarbetare som slutar sin anställning logga in i systemet. Användare som inte kontinuerligt är inloggade uppmanas efter 90 dagar byta lösenord, görs inte detta upphör deras behörighet. Behörigheter kan dock behållas vid byte av tjänst inom respektive kommun.

Då systemansvarig är centralt placerad och har arbetat länge i kommunen har hon god kännedom om de anställda och ansvariga chefer. Den intervjuade uppger att hon som ett stöd i sitt arbete skulle vilja se uppdaterade skriftliga rutiner inom alla delar av systemansvaret och en större delaktighet från cheferna på förvaltningen.

3.2.2. Loggkontroller

I rutin för loggkontroll för informationshantering och dokumentation i akter på individ och familjeomsorgen upprättad 2015 framgår att det är verksamhetschefen som ansvarar för att det finns en lokal rutin för systematisk loggning. Det framgår vidare i rutinen att det är verksamhetschefen som tillsammans med systemansvarig som ska genomföra loggkontroller. Det är vidare verksamhetschefens ansvar att informera systemansvarig om personalförändringar, att varje användare informeras om loggning och loggkontroll samt tillse att nyanställda får denna information.

Av rutinen från 2015 framgår vidare att systematiska loggkontroller ska genomföras en gång per månad. Urvalet ska utgöras av 5 % av användarna och omfatta 10 % av akterna som granskas under en vecka. Ett granskningsprotokoll ska upprättas för loggkontrollen som arkiveras i 10 år. Av dokumentation framgår att dessa ska överlämnas till nämnd i oktober varje år.

Rutinen fastställer också att kontroller kan genomföras vid klients begäran om loggutdrag, vid misstanke om otillbörlig åtkomst (verksamhetschefs ansvar) samt andra riktade loggkontroller då främst avseende användare med behörighet i flera verksamhetssystem.

I intervju framkommer att loggkontroller genomförs en gång per kvartal, att dessa genomförs av systemansvarig själv och att protokollen lämnas till verksamhetschef. Den intervjuade vet inte hur protokollen hanteras sedan. Den intervjuade har hunnit genomföra två loggkontroller sedan hon tog över systemansvaret och har inte stött på någon avvikelse i sin kontroll. Såvitt den intervjuade känner till har det inte genomförts några riktade kontroller, inte heller har chefer kontrollerats. Loggkontroller gällande akter och användare genomförs samtidigt. Den intervjuade uppger att förvaltningen håller nu på att se över sina rutiner på detta område.

Systemansvarig tror inte att någon utbildning genomförs gällande verksamhetssystemet specifikt, nyanställda får viss information om loggning och loggkontroller i och med att de får skriva på informationssäkerhetsinstruktioner.

3.2.3. Bedömning

Vi bedömer att det finns brister i hur förvaltningens rutiner efterlevs avseende verksamhetssystemet.

Gällande behörigheter sker ingen dokumentation i samband med att nya användare läggs till i systemet. Det brister också i att chefer ska anmäla förändringar i anställningar till systemansvarig såväl inom IFO som inom familjerätten i Växjö. Denna risk är störst vid byte av tjänst inom kommunen då risk finns för att behörigheter ligger kvar på anställda som inte längre behöver dessa i sin tjänsteutövning. Riskerna avseende behörighet bedöms trots detta som låg då verksamheten är förhållandevis liten och att grundläggande behörigheter upphör i samband med att anställningar upphör, detta förhindrar inloggning i verksamhetssystemet.

Det sker såvitt framkommit ingen utbildning eller information om att loggning och loggkontroller kommer ske till befintliga eller nya användare i verksamhetssystemet. Detta är enligt rutinerna ett chefsansvar. Endast generell information ges till nyanställda. Detta bedömer vi kan förbättras och bidra till en bättre kontrollmiljö.

Avseende loggkontroller bedömer vi att tydliga rutiner finns men att dessa inte efterlevs. Det gör att samtliga funktioner inte granskas under året i tillräcklig omfattning. Enligt gällande rutin ska verksamhetschefen vara involverad i loggkontrollerna vilket inte heller skett.

Vi bedömer att rutinerna som finns idag, från 2015 skulle behöva uppdateras och bättre anpassas efter IFOs verksamhet. Uppdateringen skulle troligen bidra till att fler kände till dem och en bättre efterlevnad.

Vi noterar att socialnämnden påbörjat ett arbete med dataskyddsefterlevnad och informationssäkerhet vilket bland annat behandlades på nämnden i maj 2021. Vi kan dock inte i protokoll utläsa om nämnden tagit del av granskningsprotokollen från loggkontrollerna i verksamhetssystemen vilket ska ske enligt rutin.

3.3. Evolution

Systemet används av alla nämnder som postdiarie, ärendehanteringssystem samt för att förvara handläggares personliga eller delade dokument. Inom barn- och utbildningsnämnden används systemet som postdiarie, ärendehanteringssystem, för hantering av elevakter men även dokumentförvaring och delning av dokument via en mappstruktur. Totalt finns 55 användare på barn- och utbildningsnämnden. Av dokumentation från förvaltningen framgår när systemet ska användas. Elevakterna som finns i den ”allmänna” delen av diariet kan innehålla känslig information i form av anteckningar från kuratorer och elevhälsoprotokoll. I samband med införandet av Office 365 har användandet av Evolution ökat då verksamheterna behöver kunna hantera känslig personinformation i ett skyddat system. Icke-känslig information hanteras i andra system.

Inom kommunen finns tre systemansvariga som kan lägga upp nya användare och tilldela behörigheter.

3.3.1. Behörigheter

Behörighetstilldelning sker genom att chef kontaktar systemansvarig och beställer behörigheter för nya användare. Ibland kan även andra medarbetare göra denna beställning. Hur detta ska gå till finns beskrivet i en kort rutin på kommunens intranät. Systemansvarig sparar ingen dokumentation i samband med att nya användare läggs upp i systemet.

Systemansvarig kontaktar nya användare och bokar tid för användarutbildning antingen enskilt eller i grupp. I samband med övergången till Office 365 genomfördes utbildning för alla användare i verksamhetssystemet.

När systemet införskaffades skapades ett antal standardbehörigheter för t.ex. handläggare, registrator, nämndssekreterare osv. Dessa reglerar vad som kan göras i systemet t.ex. bara läsa eller skapa nya handlingar. Systemansvarig kan skräddarsy behörigheter om detta skulle behövas. De funktioner som har tillgång till elevakterna idag är rektor, skoladministratör, elevhälsan, nämndssekreterare, utbildningschef och samordnare.

Enskilda användare kan också begränsa informationstillgången ytterligare genom att skapa en mappstruktur där användaren kan bestämma vilka som kan se skapade dokument eller arbetsmaterial och vad som bara kan ses av användaren själv. Detta gäller framförallt material som inte ska finnas i elevakten eller är under framtagande.

Vid intervju framkommer att det inte finns någon skriftlig vägledning kring tilldelning av behörigheter. Det är upp till beställande chef att avgöra vilket behov av behörigheter som finns och det är systemansvarigs roll att tilldela detta. Dokumentation finns kring klassning av information och vilka system som ska användas men inkommen dokumentation har ingen koppling till behörigheter i systemen.

Gallring sker löpande och på initiativ av systemansvarig då denne får kännedom om förändringar i verksamheten eller genom att generella behörigheter upphör genom s.k. AD:t. Någon systematisk gallring vid särskilda tidpunkter eller avstämningar mot listor över användare/anställda görs inte.

3.3.2. Loggkontroller

Det saknas skriftliga rutiner kring detta för verksamhetssystemet. I intervju bekräftas att inga systematiska loggkontroller görs. Punkten tas dock upp i användarutbildningen där systemansvarig informerar om loggning och loggkontroller.

3.3.3. Bedömning

Granskningen visar att det finns möjligheter i verksamhetssystemet för att skydda information i form av arbetsmaterial och tydligt avgränsa vem som kan se information genom dess mappstruktur, vilket vi ser som positivt. Det är vidare positivt att användarutbildning sker med alla nya och vid behov även för befintliga användare i systemet. Riskerna för otillbörlig åtkomst bedöms som relativt små tack vare god utbildningsstatus hos användarna, användande av mappstruktur samt kännedom om att loggning sker vilket skapar en god kontrollmiljö.

Vi bedömer dock att utbildningsnämnden bör upprätta rutiner för behörighetstilldelning, dokumentera när nya användare läggs till i systemet samt skapa rutiner för gallring och loggkontroller.

3.4. Gemensamma nämnden för lönesamverkan

Systemförvaltningsorganisationen finns tydligt dokumenterad med roller och ansvar. Momentet behörigheter finns med dokumentet samt i nämndens internkontrollplan för 2020 såväl som 2021. Med anledning av detta har en översyn och gallring av behörigheter skett i verksamhetssystemet (Personec) under 2020.

All behörighet utöver den som är styrkt med underskrift av ansvarig chef och dokumenterad på behörighetsblanketter har rensats ur systemet. Behörighetsblanketterna har digitaliserats under 2021 för en snabbare hantering och dessa rullas ut i samverkanskommunerna under hösten. Blanketterna kan bara skapas av lönesättande chef med särskild inloggning eventuellt kommer detta ske med Band-ID framöver.. Blanketten innehåller förutom detta en koppling till AD:t (generell behörighet) vilket gör att chef bara kan välja egen personal och inga uppgifter ändras. Till detta tillkommer en kontroll av tjänsteperson innan behörigheten slutligt ges till ny användare.

I internkontrollplanen för 2021 framgår att samtliga behörigheter kommer att kontrolleras under året.

3.4.1. Bedömning

Bedömningen är att behörighetstilldelning fungerar tillfredsställande i gemensamma nämnden för lönesamverkan. Skriftliga rutiner kring behörighetstilldelning finns, gallring och översyn av behörigheterna har gjorts i närtid för att spegla respektive kommuns organisation och behörighetsblanketterna (snart digitala) skapar en tydlig spårbarhet mellan organisation, behörig chef och behörighetstilldelning. Till detta kommer att nämnden kommer att genomföra kontroller av samtliga behörigheter under året vilket är positivt.

4. Stickprovskontroll av loggar

För Procapita har ett slumpmässigt urval av användare genomförts av EY. Systemansvarig har bistått med listor över användare. Totalt omfattade stickprovet 9 användare vars aktivitet i systemet granskades under 5 dagar (v. 21 2021).

Respektive chef har ombetts gå igenom loggarna för respektive användare under perioden. Vid genomgång har inga avvikelser rapporterats.

Under året har IFO-verksamheten genomfört egna loggkontroller vid två tillfällen, inga avvikelser har rapporterats vid dessa tillfällen.

För Evolution har ett slumpmässigt urval av användare genomförts av EY. Systemansvarig har bistått med listor över användare. Totalt omfattade stickprovet 10 användare vars aktivitet i systemet granskades under 5 dagar (v.21 2021).

Respektive chef har ombetts gå igenom loggarna för respektive användare under perioden. Vid genomgång har inga avvikelser rapporterats.

Barn- och utbildningsnämnden har inte genomfört egna loggkontroller.

5. Bedömning

På övergripande nivå finns ett behov av att arbeta vidare med informationssäkerhetspolicyn och skapandet av instruktioner för såväl systemägarna, IT-driften och användarna för hur policyns intentioner ska översättas i grundläggande krav rörande behörigheter, gallring och loggkontroller. Vidare bör ansvarsfördelningen mellan centrala IT, som ska ge stöd och förvaltningarna som har ansvar för verksamhetssystemen tydliggöras. Det finns ett behov av att proaktivt samla och utbilda förvaltningarna kring gemensamma frågor såsom generell informationssäkerhet, behörighetstilldelning, gallring och kontroller. Detta för att säkerställa en tillräcklig informationssäkerhet enligt beslutad policy.

Granskningen visar att socialnämnden har riktlinjer gällande roller, ansvar och till viss del behörigheter och loggkontroller. Dessa efterlevs dock i flera delar inte alls och skulle behöva förtydligas/uppdateras. En skriftlig systemförvaltningsorganisation med roller och ansvar, en tydlig rutin och dokumentation kring beställning av behörigheter och systemspecifik utbildning och information om loggning skulle skapa en robustare och mindre personberoende systemadministration med förbättrad kontrollmiljö.

Avseende utbildningsnämnden bedömer vi att det finns ett behov av att upprätta övergripande systemdokumentation samt upprätta riktlinjer och rutiner för såväl behörighetstilldelning som loggkontroller. Det är positivt att man inom nämnden genomför systemspecifik användarutbildning med alla nya användare.

Gällande nämnden för lönesamverkan är tydligt att granskningen 2019 resulterat i förbättringar i nämnden. Behörigheter är en punkt i internkontrollplan, tydliga rutiner finns avseende behörigheter och gallring. Tilldelning av behörighet sker numer kopplat till organisationen genom skriftlig (digital) ansökan av behörig chef.

Revisionsfrågor	Svar
Är ansvars- och arbetsfördelningen inom organisationen tillräckligt tydlig?	Delvis. Det finns ett behov av att förtydliga ansvaret mellan kommunstyrelse och nämnder.
Är uppföljning och utvärdering inom området ändamålsenlig?	Delvis.
Sker en tillräcklig styrning av behörigheter till känsliga verksamhetssystem?	Delvis. Systemdokumentation med roller och ansvar samt skriftliga riktlinjer och rutiner för behörigheter och dokumentation vid tilldelning av behörighet behöver skapas/uppdateras.
Säkerställer nämnderna att tillräcklig intern kontroll inom området har upprättats för att hindra otillåten åtkomst till och spridning av känslig information?	Delvis. Skriftliga riktlinjer och rutiner kring loggning och loggkontroller bör upprättas.
Genomför gemensamma nämnden systematiska och dokumenterade kontroller av behörigheter såsom	Ja. En tydlig ansvarsfördelning för systemförvaltningen finns. Tydliga rutiner finns för behörighetstilldelning och gallring. Kontroller

aktiviteter som utförts av personer med höga behörigheter i lönesystemet, att registrerade behörigheter för anställda överensstämmer med gällande organisationsstruktur och attestförteckning samt om behörig chef har undertecknat blanketten vid förändring av behörigheter?	av behörigheter sker. Behörigheter är tydligt låsta till organisationen och närmsta chef som skriftligen ansöker om behörigheter för sina medarbetare.

Utifrån granskningsresultatet rekommenderar vi kommunstyrelsen att:

- Uppdra åt kommunledningsförvaltningen att utifrån informationssäkerhetspolicyn ta fram instruktioner för systemägarna, IT-driften och användarna av systemen. Vidare bör kommunledningsförvaltningen tydliggöra ansvaret mellan centrala IT och förvaltningarna där det tydliggörs på vilket sätt stöd ska ges t.ex. i form av utbildningar eller kommungemensamma rutiner.
- I egenskap av systemägare för Evolution uppdra åt kommunledningsförvaltningen att upprätta generell systemdokumentation samt generella riktlinjer och rutiner för verksamhetssystemet.

Vi rekommenderar socialnämnden att:

- Uppdra åt socialförvaltningen att uppdatera sin systemdokumentation, riktlinjer och rutiner för verksamhetssystemet Procapita. Vidare rekommenderas nämnden ta del av de granskningsprotokoll för loggkontroller som upprättas som en del av sin interna kontroll.

Vi rekommenderar barn- och utbildningsnämnden att:

- Uppdra åt förvaltningen att i samråd med kommunledningskontoret upprätta systemdokumentation, riktlinjer och rutiner för behörigheter och loggning i sin hantering av elevakter.

Ort den 19 november 2021

Carl-Henrik Sölvinger Jakob Smith

Bilaga 1: **Källförteckning**

Intervjuade funktioner:

- IT-chef
- Systemansvarig Procapita/Lifecare
- Systemansvarig Evolution

Dokument:

- Informationssäkerhetspolicy, beslutad mars 2020
- Rutin för loggkontroll för informationshantering och dokumentation i akter på IFO upprättad 2015
- Mallar för behörighet – IFO
- Mall granskningsprotokoll – loggkontroll IFO
- Tjänstebeskrivning behörighet och konto - AD
- Patientsäkerhetsberättelse 2020, socialnämnden
- Lessebo kommuns skolors IT-tjänster och vad de används till

Gemensamma nämnden för lönesamverkan

- Samverkansavtal
- Systemförvaltningsorganisation PersonecP 2020
- Rutiner för behörighetshantering
- Internkontrollplan 2020 och 2021