www.pwc.se

Revisionsrapport

Behörighetshantering

Söderköpings kommun 2018

Niklas Ljung
Johan Jonsson

Maj 2018

pwc

Innehåll

Sammanfattande revisionell bedömning

PwC har på uppdrag av Söderköping kommuns revisorer genomfört en granskning gällande behörighetshanteringen inom IT. Här konstateras brister gällande styrning, uppföljning och kontroll. Vår samlade revisionella bedömning grundar sig på de iakttagelser med efterföljande bedömningar som gjorts i följande kontrollfrågor:

	Kontrollfråga	Bedömning
1	Finns det styrande dokument, såsom policy och riktlinjer för informations och IT-säkerhet och är de kontinuerligt reviderade?	
2	Finns roller och ansvar tydligt definierad i dokumentation enligt befintlig sysselsättning för att skapa en god intern kontrollmiljö och för att säkerhetsställa en effektiv IT- och informationssäkerhet?	
3	Finns styrande dokument och rutiner kring ändringar av roller och ansvar i behörighetsstrukturen för IT-systemen?	
4	Finns det styrande dokument och rutiner kring hantering av användarkonton?	
5	Finns det väl förankrade rutiner för behörighetstilldelning till nya, förändrade och borttagna användare för att försäkra sig att användaren har rätt (auktoriserad) behörighet?	
6	Säkerställs att den behöriga till viss tilldelning är medveten om rättigheter och skyldigheter som följer?	
7	Finns det periodiska granskningar av användares behörigheter för att säkerhetsställa intern kontroll och riktighet?	
8	Finns det en tydlig dokumentation som hanterar uppdelningen av behörigheter för personal som arbetar inom IT-verksamheten gentemot de som jobbar inom övrig verksamhet?	
9	Finns det en tydlig rutin kring hanteringen av generiska systemkonton med högre behörigheter, såsom servicekonton?	

 - Uppfyllt kontrollmål

 - Delvis uppfyllt kontrollmål

 - Ej uppfyllt kontrollmål

Sammanfattning

1. **Finns det styrande dokument, såsom policy och riktlinjer för informations och IT-säkerhet och är de kontinuerligt reviderade?**

Kontrollmålet bedöms som *delvis uppnått*. Med utgångspunkt från den nyligen antagna IT-planen och förutsatt att informationssäkerhetsplanen för Söderköpings kommun antas av Kommunfullmäktige med tillhörande tjänstemannainstruktioner för drift, förvaltning och användare anses relativt erforderliga styrande dokument kopplade till IT- och informationssäkerhet finnas på plats. Däremot noterades att ingen förankrad versionshanteringsrutin existerar och att revidering av de styrande dokumenten för IT- och informationssäkerhet sker vid behov.

2. **Finns roller och ansvar tydligt definierad i dokumentation enligt befintlig sysselsättning för att skapa en god intern kontrollmiljö och för att säkerhetsställa en effektiv IT- och informationssäkerhet?**

Kontrollmålet bedöms som *delvis uppfyllt*. Det framgår i granskningen att roller och ansvar är tydligt definierade i dokumentation kring informationssäkerhet men att den är bristfällig för IT-säkerhetsområdet.

3. **Finns styrande dokument och rutiner kring ändringar av roller och ansvar i behörighetsstrukturen för IT-systemen?**

Kontrollmålet bedöms som *uppfyllt*. Det framgår av granskningen att det finns tydliga dokument och rutiner kring hanteringen av ändringar i behörighetsstrukturen.

4. **Finns det styrande dokument och rutiner kring hantering av användarkonton? Exempel på styrande dokument; lösenordspolicy, unika användarkonton, systemloggning och utgångsdatum för konto. Exempel på rutiner; Onboarding och offboarding (när en person påbörjar och avslutar sitt uppdrag).**

Kontrollmålet bedöms som *delvis uppfyllt*. Det framkommer att loggning genomförs av system och nätverk men att ingen löpande granskning görs. Vidare anses lösenordshanteringen vara god som har ett tillräckligt starkt säkerhetskrav. Konsult- och praktikantkonton tidsbegränsas. Det framkommer att det finnas en relativt erforderlig onboardingprocess och att arbete med tilltänkt implementering av off- och preboarding sker. Vidare anses det, baserat på granskningen, vara en god hantering av konton med priviligierade behörigheter.

5. **Finns det väl förankrade rutiner för behörighetstilldelning till nya, förändrade och borttagna användare för att försäkra sig att användaren har rätt (auktoriserad) behörighet?**

Kontrollmålet bedöms som *delvis uppfyllt*. Det anses finnas relativt erforderliga rutiner för tilldelning av behörigheter till nya användare och för borttagning av behörigheter för avslutade konton. Däremot noterades bristfälliga rutiner kring hantering av förändring av behörigheter vid exempelvis intern förflyttning och att behörigheter till mailkontot och därmed innehållet i mailboxen, inte går att särskilja beroende på uppdrag i kommunen.

6. **Säkerställs att den behöriga till viss tilldelning är medveten om rättigheter och skyldigheter som följer?**

Kontrollmål bedöms som *uppfyllt*. Baserat på granskningen anses tilldelning av behörighet vara medvetna om rättigheter och skyldigheter som följer.

7. Finns det periodiska granskningar av användares behörigheter för att säkerhetsställa intern kontroll och riktighet?

Kontrollmålet bedöms som *ej uppfyllt*. Det noterades en avsaknad av periodisk manuell granskning av användares behörigheter vilket resulterar att intern kontroll och riktighet kring behörighetshantering inte kan säkerställas. Vidare noterades att hanteringen av användares behörighetsbeställning och borttagande är tydligt, varför en implementation av en periodisk granskning inte bör vara komplicerat att förankra.

8. Finns det en tydlig dokumentation som hanterar uppdelningen av behörigheter för personal som arbetar inom IT-verksamheten gentemot de som jobbar inom övrig verksamhet?

Kontrollmålet bedöms som uppfyllt. Det finns tydlig dokumentation som hanterar uppdelning av behörigheter kring arbetsfördelning.

9. Finns det en tydlig rutin kring hanteringen av generiska systemkonton med högre behörigheter, såsom servicekonton?

Kontrollmålet bedöms som *delvis uppfyllt*. Det noterades att generiska systemkonton hanteras av en begränsad skara men att lösenordsskyddet till dessa konton är bristfälliga.

Rekommendationer

- Ansvaret för kommunens kontohantering bör ligga under HR-chefen eftersom att ett konto startas och avslutas här.

- Utbildningar inom kommunen bör kopplas till kommunens vision och övergripande strategi. Kompetensen bör säkerställas utifrån kommunens behov. Att kompetensutveckla personalen är en viktig del i att säkerställa att kommunen kan dra nytta av den snabba utveckling som sker inom digitalisering och IT. Det bidrar också till en roligare och mer utvecklande arbetsmiljö. Den nyligen införskaffade e-learningsplattformen är ett bra sätt att uppnå ökad mognad och medvetenhet hos kommunens anställda och invånare.

- Kommunen bör införa en periodiserad granskning över användares kontobehörigheter på årsbasis för att öka den interna kontrollen.

- Kommunen bör förankra en rutin kring hanteringen av behörigheter då anställd byter förvaltning för att öka den interna kontrollen.

- Kommunen bör implementera versionshantering och datumstämpel i styrande dokument samt att revidering av styrande dokument sker periodiskt och inte endast efter behov, för att säkerställa korrekthet och riktighet i dokumenten.

- IT-säkerhetsansvarig bör vara dokumenterad i roll- och arbetsbeskrivning.

- Informationssäkerhetssamordnaren bör verka som kravställare mot IT och bör då inte organisatoriskt ligga under IT-avdelningen.

- Kommunen bör arbeta vidare med utveckling samt implementering av onboarding/preboarding/offboarding då det är uttryckt i kommunens strategi att stärka varumärket för nuvarande och kommande medarbetare.

- Det noterades i styrande dokument att kommunen minst ska följa standarden ISO 27001 och kommande ISO 27002. Kommunen bör omformulera målsättning till att ha ISO 27001 och 27002 som riktmärke då det endast finns några få enstaka kommuner i Sverige som innehar certifiering från ovannämnda standard. Exempel på omformulering: *”… ska sträva efter att använda ISO 27001 och ISO 27002 som riktmärke i vårt informationssäkerhetsarbete”*.

1. Inledning

1.1. Bakgrund

Kommunstyrelse och facknämnder ska förvalta och genomföra verksamheten i enlighet med fullmäktiges uppdrag, lagar och föreskrifter. För att fullgöra uppdraget måste respektive organ bygga upp system och verktyg för ledning, styrning, uppföljning, kontroll och rapportering samt säkerställa att dessa verktyg tillämpas på avsätt sätt. En bristfällig styrning och kontroll kan riskera att verksamheten inte bedrivs och utvecklas på avsett sätt.

PwC genomförde under slutet av 2017 en förstudie som bland annat undersökt huruvida IT-säkerhets- och sekretessfrågor har behandlats på ett ändamålsenligt sätt vad gäller samarbetet med IP-Only Networks AB. Förstudien kom fram till att det kan finnas anledning att genomföra en uppföljande granskning av IT-behörighetshantering under 2018.

1.2. Syfte och revisionsfråga

Granskningen syftar till att besvara följande revisionsfråga:

- *Har kommunstyrelsen säkerställt att Söderköpings kommun har en ändamålsenlig behörighetshantering samt att organisation och rutiner är väl förankrade.*

1.3. Kontrollfrågor

- Finns det styrande dokument, såsom policy och riktlinjer för informations och IT-säkerhet och är de kontinuerligt reviderade?
- Finns roller och ansvar tydligt definierad i dokumentation enligt befintlig sysselsättning för att skapa en god intern kontrollmiljö och för att säkerhetsställa en effektiv IT- och informationssäkerhet?
- Finns styrande dokument och rutiner kring ändringar av roller och ansvar i behörighetsstrukturen för IT-systemen?
- Finns det styrande dokument och rutiner kring hantering av användarkonton? Exempel på styrande dokument; lösenordspolicy, unika användarkon-ton, systemloggning och utgångsdatum för konto. Exempel på rutiner; Onboarding och offboarding (när en person påbörjar och avslutar sitt uppdrag).
- Finns det väl förankrade rutiner för behörighetstilldelning till nya, förändrade och borttagna användare för att försäkra sig att användaren har rätt (auktoriserad) behörighet?
- Säkerställs att den behöriga till viss tilldelning är medveten om rättigheter och skyldigheter som följer?
- Finns det periodiska granskningar av användares behörigheter för att säkerhetsställa intern kontroll och riktighet?
- Finns det en tydlig dokumentation som hanterar uppdelningen av behörig-heter för personal som arbetar inom IT-verksamheten gentemot de som jobbar inom övrig verksamhet?
- Finns det en tydlig rutin kring hanteringen av generiska systemkonton med högre behörigheter, såsom servicekonton?

1.4. Metod

Granskningen genomförs i form av intervjuer med identifierade nyckelpersoner i kommunen, (se intervjulista, bilaga 1) samt inläsning och genomgång av de dokumentation och styrande dokument som tillgängliggjorts för oss. Erhållet material har granskats på en övergripande nivå.

Granskningen avgränsas till att omfatta Söderköping kommuns IT-enhet, personalavdelning och servicenämnden.

Rapporten är sakavstämd hos de intervjuade och kvalitetssäkrad internt inom PwC.

1.5. Revisionskriterier

Revisionskriterier i denna granskning är:

- Kommunallagen
- IT-styrdokument

2. Iakttagelser och bedömningar

2.1. Finns det styrande dokument, såsom policy och riktlinjer för informations och IT-säkerhet och är de kontinuerligt reviderade?

På övergripande nivå konstaterades att det finns erforderliga styrande dokument relaterade till informationssäkerhet med varierande aktualitet, exempelvis ”Informationssäkerhetspolicy för Söderköpings kommun” daterad till 2010 samt nyligen utformade tjänstemannadokument under 2018 ”Informationssäkerhetsinstruktion förvaltning och drift 2018-2022” och ”Informationssäkerhetsinstruktion användare 2018-2022”. Vidare konstaterades att en dragning för kommunfullmäktige gällande ”Informationssäkerhetsplan för Söderköpings kommun 2018-2022” genomförs i närtid.

Det noterades att det nyligen antagits en IT-plan i syfte att tydliggöra övergripande principer och förhållningssätt avseende IT inom kommunen framöver. Här framförs utpekade områden inom IT att jobba med, ansvarsfördelning kring IT-säkerhet och kommunstyrelsens och organisationens ansvar.

Vidare framkommer det under granskningen att det finns styrande dokument som förtydligar rutin och process vid anskaffning och implementering av informationssystem för att säkerställa ett visst mått av IT- och informationssäkerhet genom integrations- och acceptanskrav samt inledande systemsäkerhetsanalys utifrån KLASSA.

Bedömning

Kontrollmålet bedöms som ***delvis uppnått***.

Med utgångspunkt från den nyligen antagna IT-planen och förutsatt att informationssäkerhetsplanen för Söderköpings kommun antas av Kommunfullmäktige med tillhörande tjänstemannainstruktioner för drift, förvaltning och användare anses relativt erforderliga styrande dokument kopplade till IT- och informationssäkerhet finnas på plats. Däremot noterades att ingen förankrad versionshanteringsrutin existerar och att revidering av de styrande dokumenten för IT- och informationssäkerhet sker vid behov.

2.2. Finns roller och ansvar tydligt definierad i dokumentation enligt befintlig sysselsättning för att skapa en god intern kontrollmiljö och för att säkerhetsställa en effektiv IT- och informationssäkerhet?

IT-säkerhet

Efter genomgång av den nyligen antagna IT-planen fastställs att kommunstyrelsen innehar det övergripande och strategiska ansvaret för IT-säkerheten. Vidare följer säkerhetsansvaret linjeorganisationen som innebär att var och en som är ansvarig för en del i verksamheten även är ansvarig för att IT-säkerheten efterlevs inom sitt område.

Granskningen indikerar att det generellt sett finns angivna roller inom kommunen med fokus på koncernstöd inom IT- och informationsverksamheten men att roller och ansvarsfördelningen kring IT-säkerhet anses vara övergripande definierad och att det saknas befintlig dokumentation som tydliggör detta. Vidare anses det operativt löpande IT-säkerhetsarbetet vara otydligt och att organisationen anses verka mer reaktivt än proaktivt med IT-säkerhet.

Informationssäkerhet

Baserad på genomförd granskning noterades att roller och fördelning av ansvar kring informationssäkerheten finns tydligt dokumenterade i informationssäkerhetsinstruktionerna förvaltning, drift och användare i syfte att understödja den övergripande IT-planen och informationssäkerhetsplanen. Ansvaret hos rollerna systemägare och systemansvariga är tydligt definierade där systemägaren står som ansvarig för informationen i respektive förvaltningssystem. IT-chefen är systemägare för det interna IT-nätverket samt gemensamma servrar medan Kommunstyrelsen är systemägare för övriga gemensamma och underliggande system i kommunen. Systemägarna är ansvarig för att systemsäkerhetsanalyser för de egna informationssystemen genomförs med stöd av KLASSA (SKLs verktyg för att förenkla genomförandet av informationsklassning). Informationssystem inom Söderköpings kommun klassas utifrån de information som hanteras i systemet. Klassning görs från aspekterna sekretess (konfidentiellt), riktighet och tillgänglighet.

Vidare noterades att det finns en roll benämnd informationssäkerhetssamordnare på plats inom kommunen som stödjer arbetet med att uppnå informationssäkerhetsplanens mål samt analyser av de delar av IT-stödet som är gemensamma för hela verksamheten utifrån KLASSA.

Bedömning

Kontrollmålet bedöms som ***delvis uppfyllt***.

Det framgår i granskningen att roller och ansvar är tydligt definierade i dokumentation kring informationssäkerhet men den är bristfällig för området IT-säkerhet.

2.3. Finns styrande dokument och rutiner kring ändringar av roller och ansvar i behörighets-strukturen för IT-systemen?

I systemdokumentationen för Microsofts metakatalogprodukt, FIM (Microsoft Forefront Identity Manager) framgår en utförlig beskrivning av befintliga rutiner för identitetshantering av de system som är beroende av Active Directory. Regelverket i FIM säkerställer att konton skapas och underhålls i berörda system och att de tilldelas rätt inställningar, exempelvis att konton får rätt behörighet och rätt placering kopplat till organisationsstrukturen i Active Directory. Personalsystemet Personec är det system som ligger till grund för kontohanteringen för all personal och är därmed styrande. Granskningen visar även att versionshantering och datumstämpel för systemdokumentationen finns på plats vilket tydliggör riktigheten i dokumentet.

Det noterades i granskningen av mottagna informationssäkerhetsinstruktioner att IT-chefen för respektive roll och ansvar inom IT-avdelningen beslutar om tilldelning av behörigheter, samtidigt som åtkomst till verksamhetssystem hanteras av systemförvaltare.

Vidare sker en manuell hantering av behörigheter i samråd med IT-chef och medarbetares närmast överordnande chef vid specifika fall, exempelvis vid övergång till annan förvaltning alternativt vid avslut av anställning där personen också har ett politiskt uppdrag i kommunen.

Bedömning

Kontrollmålet bedöms som ***uppfyllt***.

Det framgår av granskningen att det finns tydliga dokument och rutiner kring hanteringen av ändringar i behörighetsstrukturen.

2.4. Finns det styrande dokument och rutiner kring hantering av användarkonton? Exempel på styrande dokument; lösenordspolicy, unika användarkonton, systemloggning och utgångsdatum för konto. Exempel på rutiner; Onboarding och offboarding (när en person påbörjar och avslutar sitt upp-drag).

Systemloggning

Det framgår av styrande dokument att rutin för genomgång av loggar ska dokumenteras i respektive systems förvaltningsplan.

Vidare framkommer det under granskningen att loggning för system och nätverk är påslagen men att ingen kontinuerlig uppföljning av loggarna genomförs förutom vid incidenter.

Det framkommer också att beslut om övervakning av informationssystems loggar tas av systemägaren rörande:

- Hur ofta de ska analyseras
- Vem som ansvarar för analyser av dem
- Hur länge de ska sparas
- Hur de ska förvaras

Lösenord

Det noterades under granskningen att styrande dokument kring hantering av lösenord till användarkonton finns tydligt dokumenterade i styrande dokument. ID och lösenord tilldelas användare som inte tidigare loggat in i systemet av överordnad chef där det är systemtvingande för användaren att byta lösenordet till något som är minst åtta tecken långt, består av en blandning av stora och små bokstäver, siffror och specialtecken. Lösenordsbyte sker tvingande var 90:e dag och det går inte byta till ett lösenord användaren tidigare haft.

On- och offboarding

Det noterades att en nyanställd genomgår en datorstödd informationssäkerhetsutbildning för användare (DISA) som ges ut av Myndigheten för samhällsskydd och beredskap för att höja medarbetarens medvetenhet om, och grunderna i, en god informationssäkerhetshantering. Vidare ligger det i överordnad chefs ansvar att tjänstemannainstruktioner tillgodoses så att medarbetaren är införstådd med rättigheter och skyldigheter kring hanteringen av sina användarkonton.

Vidare framkommer det under granskningen att ett arbete med att utveckla onboardingen samt införa preboarding (innan anställning) och offboarding.

Högre behörigheter

Under intervju framkommer det att tekniker har två uppsättningar av konton, ett vanligt användarkonto för dagliga sysslor och ett adminkonto med mer privilegierande behörigheter som används vid exempelvis driftarbeten av server, nätverk eller system. Kontona är individuella och loggning sker på adminkonto. Teknikerna är säkerhetsklassade enligt

nivå 3 och IT-chef enligt nivå 2. Som tidigare noterats sker ingen löpande uppföljning av loggar utan endast vid incident.

Bedömning

Kontrollmålet bedöms som ***delvis uppfyllt***.

Det framkommer att loggning genomförs av system och nätverk men att ingen löpande granskning görs. Vidare anses lösenordshanteringen vara god som har ett tillräckligt starkt säkerhetskrav. Konsult- och praktikantkonton tidsbegränsas. Det framkommer att det finnas en relativt erforderlig onboardingprocess och att arbete med tilltänkt implementering av off- och preboarding sker. Vidare anses det, baserat på granskningen, vara en god hantering av konton med priviligierade behörigheter.

2.5. Finns det väl förankrade rutiner för behörighetstilldelning till nya, förändrade och borttagna användare för att försäkra sig att användaren har rätt (auktoriserad) behörighet?

Det noterades under granskningen att det finns relativt erforderliga rutiner för tilldelning, förändring och borttagning av behörigheter inom IT-avdelningen.

Då nyanställd signerat sitt anställningsavtal läggs personen upp i personalsystemet Personec. Personec är sammankopplat med Active Directory som skapar en användare automatiskt. Användaren tilldelas en uppsättning behörigheter utifrån anställningsplats till gemensamma ytor, hemkatalog, mailbox och närmsta chef tilldelas ID och lösenord till användarens konto. Specifika behörigheter beställs i ServiceDesk av rekryterande chef. Då en beställning görs av en person som inte har behörighet att beställa behörigheter så genereras ett automatiskt mail till överordnad chef som behöver attestera beställningen.

Vid ändring av behörigheter, exempelvis vid en intern förflyttning och då person redan är upplagd i Active Directory, beställs nya behörigheter av den tilltänkta personalansvarige. Det noterades att det i nuläget inte finns en förankrad rutin kring radering av ursprungliga behörigheter på kontot men att en utarbetning av sådant sker.

Vid fall då flera uppdrag finns kopplade till kontot (exempelvis anställd och förtroendevald) fortskrider behörigheterna till kontot även om personen avslutar sin anställning. En manuell hantering av sådana konton har implementerats för att säkerställa att personens behörigheter överensstämmer med respektive uppdrag. Däremot finns det i nuläget ingen utarbetad rutin kring hanteringen av personens mailkonto då mailboxen är generell för personen och inte frånskilt beroende på respektive uppdrag.

Bedömning

Kontrollmålet bedöms som ***delvis uppfyllt***.

Det anses finnas relativt erforderliga rutiner för tilldelning av behörigheter till nya användare och för borttagning av behörigheter för avslutade konton. Däremot noterades bristfälliga rutiner kring hantering av förändring av behörigheter vid exempelvis intern förflyttning och att behörigheter till mailkontot och därmed innehållet i mailboxen, inte går att särskilja beroende på uppdrag i kommunen.

2.6. Säkerställs att den behöriga till viss tilldelning är medveten om rättigheter och skyldigheter som följer?

Det noterades under granskningen att verksamhetschefen är ansvarig för att informera den anställde om:

- Informationssäkerhetens betydelse för verksamheten
- Innehållet i Informationssäkerhetsplanen
- Innehållet i IT-planen
- Informationssäkerhetsinstruktionen för användare

Vidare framgår det under intervjuerna att nya användare ska ges ”Datorstödd informationssäkerhetsutbildning för användare” (DISA) i samband med tilldelning av behörighet i nätverket.

Under granskningen framkommer det också att systemägare ansvarar för att användarhandledning för aktuellt system finns och att medarbetare har tillräckliga kunskaper om säkerhetsreglerna för de informationssystem de behöver för de egna arbetsuppgifterna.

Bedömning

Kontrollmål bedöms som ***uppfyllt.*** Baserat på granskningen anses tilldelning av behörighet vara medvetna om rättigheter och skyldigheter som följer.

2.7. Finns det periodiska granskningar av användares behörigheter för att säkerhetsställa intern kontroll och riktighet?

Det noterades under granskningen att det inte sker några periodiska granskningar kopplade till användares behörigheter för att säkerställa intern kontroll och riktighet.

Under granskningen förekommer dock att det anses finnas andra kontroller som minskar risken av oriktiga användarkonton. Det utförs nattliga körningar av inventariesystemet mot attribut i Active Directory, i syfte att kontrollera status på kontot (aktivt/inaktivt). Ifall statusattributet är inaktivt (vilket det blir då en persons anställning avslutas) noteras ServiceDesk genom ärendehanteringssystemet EasIT och har då möjlighet att låsa inventarier med åtkomst till Active Directory för personen.

En annan kontroll som anses som mildrande är den interna faktureringen av kostnaden för kontohantering hos IT-avdelningen till förvaltningarna. Förutsatt att en strävan för kostnadsminimerande åtgärder finns hos förvaltningarna anses det förekomma incitament att kontinuerligt revidera vilka konton som är aktiva respektive inaktiva.

Bedömning

Kontrollmålet bedöms som ***ej uppfyllt***.

Det noterades en avsaknad av periodisk manuell granskning av användares behörigheter vilket resulterar att intern kontroll och riktighet kring behörighetshantering inte kan säkerställas. Vidare noterades att hanteringen av användares behörighetsbeställning och borttagande är tydligt, varför en implementation av en periodisk granskning inte bör vara komplicerat att förankra.

2.8. Finns det en tydlig dokumentation som hanterar uppdelningen av behörigheter för personal som arbetar inom IT-verksamheten gentemot de som jobbar inom övrig verksamhet?

Det framkommer under granskningen av dokumentet ”instruktioner för informationssäkerhetsinstruktion” att dokumentation för målgruppen IT-driftansvariga, ledning, systemägare och systemförvaltare samt en instruktion för samtliga medarbetare finns.

Bedömning

Kontrollmålet bedöms som **uppfyllt.**

Det finns tydlig dokumentation som hanterar uppdelning av behörigheter kring arbetsfördelning.

2.9. Finns det en tydlig rutin kring hanteringen av generiska systemkonton med högre behörigheter, såsom service konton?

Det noterades under granskningen att IT-enhetens personal har vanliga användarkonton samt personliga systemkonton med priviligierade behörigheter. Det är IT-chefen som beslutar om behörigheter för respektive roll utöver standard rättigheter. Som standard arbetar alltid tekniker som vanlig användare**.** Administratörsrättigheter (priviligierad behörighet) nyttjas endast vid åtkomst till servrar och nätverksutrustning.

Under granskningen förekommer det att loggning är påslagen för personliga systemkonto men att ingen kontinuerlig uppföljning av loggarna genomförs förutom vid uppdagade incidenter.

Vidare noterades att det finns ett fåtal generiska systemkonton som tillhandahavs av IT-avdelningens drifttekniker vid exempelvis backuphanteringen. Under granskningen framkommer relativt erforderlig hantering med utrymme för förbättring.

Bedömning

Kontrollmålet bedöms som ***delvis uppfyllt***. Det noterades att generiska systemkonton hanteras av en begränsad skara men att lösenordsskyddet till dessa konton är bristfälliga.

2018-06-13

Lena Brönnert, uppdragsledare	*Niklas ljung, projektledare*

3. Bilaga

Intervjulista

Namn	Roll	Verksamhet
Bärbel Elenius	HR-chef	Personalavdelningen
Anneli Lindblom	IT- och kommunikationschef	IT-enheten
Yvonne Persson	Första vice ordförande, del av presidium	Kommunfullmäktige
Rickard Bardun	Chef för Servicenämnden	Serviceförvaltningen
Christian Valgren	Chef för ServiceDesk	IT-enheten