För kännedom till:

Kommunstyrelsen
Kommunfullmäktige

Kungälvs kommun

Granskningsrapport "Granskning av kommunens införande av digital välfärdsteknik”

De förtroendevalda revisorerna i Kungälvs kommun har givit KPMG i uppdrag att genomföra en granskning av kommunens införande av digital välfärdsteknik.

Uppdraget ingår i revisionsplanen för år 2024.

Syftet med granskningen var att bedöma om kommunstyrelsen har säkerställt att införandet av digital teknik inom vård- och omsorg sker på ett ändamålsenligt sätt.

KPMG:s samlade bedömning utifrån granskningens syfte är att kommunstyrelsen delvis har säkerställt att införandet av digital teknik inom vård- och omsorg sker på ett ändamålsenligt sätt.

Mot bakgrund av granskningen rekommenderar vi kommunstyrelsen att:

- Säkerställa att samtliga styrdokument är aktuella.
- Säkerställa tydliga ansvar och roller i projektarbeten på området genom följsamhet till beslutade anvisningar.
- Fastställ rutiner för arbetet inför upphandling av nya system, som tydliggör ansvar och roller i arbetet med beaktandet av säkerhetsfrågor.
- Tillse att det finns ett systematiserat arbete för att säkerställa att behörigheter i samtliga system är korrekta och uppdaterade.
- Säkerställa att tekniska säkerhetsåtgärder såsom två faktorsinloggning implementeras i samtliga system.

Vi önskar, senast den 9 maj 2025, kommunstyrelsens skriftliga kommentarer till KPMG:s granskningsrapport och våra synpunkter enligt ovan.

Kungälv den 22 januari 2025
För kommunrevisionen

Göran Johansson
Göran Johansson (22 jan. 2025 11:11 GMT+1)
Göran Johansson
Ordförande

KOMMUNREVISIONEN

KUNGÄLVS KOMMUN

ADRESS Stadshuset · 442 81 Kungälv
TELEFON 0303-23 80 00 vx
FAX 0303-182 59
E-POST kommun@kungalv.se
HEMSIDA www.kungalv.se

Missiv - Granskningsrapport Granskning av kommunens införande av digital välfärdsteknik

Slutgiltig revideringsrapport 2025-01-22

Skapad:	2025-01-22
Av:	Sophie Nygren (sophie.nygren@kungalv.se)
Status:	Signerat
Transaktions-ID:	CBJCHBCAABAAGczt0Lb5OEzfmqEDKCO066K77ORV4IUV

”Missiv - Granskningsrapport Granskning av kommunens införan de av digital välfärdsteknik” – historik

Dokumentet skapades av Sophie Nygren (sophie.nygren@kungalv.se)
2025-01-22 - 10:05:08 GMT

Dokumentet skickades med e-post till goran.johansson@kungalv.se för signering
2025-01-22 - 10:05:11 GMT

E-postmeddelandet har visats av goran.johansson@kungalv.se
2025-01-22 - 10:11:03 GMT

Signerare goran.johansson@kungalv.se angav namnet Göran Johansson vid signering
2025-01-22 - 10:11:55 GMT

Dokumentet har e-signerats av Göran Johansson (goran.johansson@kungalv.se)
Signaturdatum: 2025-01-22 - 10:11:57 GMT – Tidskälla: server

Avtal har slutförts.
2025-01-22 - 10:11:57 GMT

Granskning av kommunens införande av digital välfärdsteknik

Rapport

Kungälvs kommun

KPMG AB

2025-01-10

Antal sidor 21

Kungälvs kommun
Granskning av kommunens införande av digital välfärdsteknik

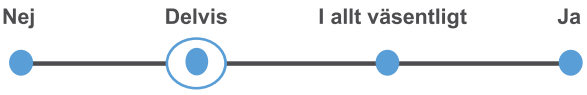
2025-01-10

Innehållsförteckning

1 Sammanfattning

KPMG har av Kungälvs kommuns revisorer fått i uppdrag att granska kommunens införande av digital välfärdsteknik.

Syftet med granskningen har varit att bedöma om kommunstyrelsen säkerställt att införandet av digital teknik inom vård- och omsorg sker på ett ändamålsenligt sätt.



Vår samlade bedömning utifrån granskningens syfte är att kommunstyrelsen delvis säkerställt att införande av digital teknik inom vård- och omsorg sker på ett ändamålsenligt sätt.

Bakgrunden till vår samlade bedömning är att granskningen visat att kommunen har antagit styrdokument som visar mål och syfte med digitaliseringen i kommunen. Utöver det noterar vi att sektor trygghet och stöd har tagit fram en digitaliseringsplan för införande av digitalisering. Vidare framgår att sektor trygghet och stöd upplever den övergripande organisationen med digitalisering som tydlig, men att det finns brister i projektstyrning och att mallen för projektdirektiv inte används i stor utsträckning.

Avseende säkerhet och behörigheter noterar vi att det genomförs riskanalyser vid införande av nya system. Vi noterar dock att det saknas en tydlig dokumenterad process inför upphandlingar av nya system. Vid tidpunkten för granskningen arbetar upphandlingsenheten med att ta fram en checklista som en del i arbetet med den dokumenterade processen, vilket vi anser är positivt.

Avseende rutiner för behörighet noterar vi att det finns dokumenterade regler för medarbetarnas åtkomst till känslig information. Vi konstaterar dock brister i arbetet med behörigheter i granskat system samt att alla system inte har implementerat tvåfaktorsautentisering.

I det följande redovisas våra samlade bedömningar av respektive revisionsfråga.

Revisionsfråga	Bedömning
Finns beslutade styrdokument som tydliggör uppdrag och ansvar för digitaliseringsarbetet inom vård- och omsorg?	I allt väsentligt
Finns en ändamålsenlig organisation för digitaliseringsarbetet?	I allt väsentligt
Har kommunstyrelsen säkerställt att verksamheterna beaktar säkerhet i sitt digitaliseringsarbete?	Delvis

Finns dokumenterade regler för medarbetares åtkomst till känslig information?	I allt väsentligt
Finns en tillräcklig intern kontroll för att säkerställa att endast behöriga får åtkomst till information och utrymmen som de har behov av utifrån organisationstillhörighet och roll?	Delvis
Har tekniska säkerhetsåtgärder vidtagits för att säkerställa att inte känsliga uppgifter röjs till obehöriga?	Delvis

För närmare beskrivning av bakgrunden till våra bedömningar hänvisar vi till respektive avsnitt i revisionsrapporten.

Utifrån resultatet av vår granskning rekommenderar vi kommunstyrelsen att:

- Säkerställa att samtliga styrdokument är aktuella.
- Säkerställa tydliga ansvar och roller i projektarbeten på området genom följsamhet till beslutade anvisningar.
- Fastställ rutiner för arbetet inför upphandling av nya system, som tydliggör ansvar och roller i arbetet med beaktandet av säkerhetsfrågor.
- Tillse att det finns ett systematiserat arbete för att säkerställa att behörigheter i samtliga system är korrekta och uppdaterade.
- Säkerställ att tekniska säkerhetsåtgärder såsom två faktorsinloggning implementeras i samtliga system.

2 Bakgrund

Vi har av Kungälvs kommuns förtroendevalda revisorer fått i uppdrag att granska kommunens införande av digital välfärdsteknik. Uppdraget ingår i revisionsplanen för år 2024.

Den offentliga förvaltningen investerar årligen miljardbelopp i verksamhetsutveckling med hjälp av IT för att följa lagar, effektivisera processer och höja servicenivån för de som efterfrågar verksamhetens tjänster. De omfattande projekten kräver ofta stora insatser från verksamheten, både i form av tid och ekonomiska resurser.

Inom kommunernas vård- och omsorgsverksamhet är implementeringen av välfärdsteknik en väsentlig del av verksamhetsutvecklingen, ofta syftande till att förbättra och effektivisera. Samtidigt är det avgörande att teknikens användning följer etiska riktlinjer och lagkrav kring integritet och dataskydd för att skydda användarnas rättigheter och värdighet.

Välfärdsteknik är digital teknik som ska bidra till ökad livskvalitet för äldre personer och personer med funktionsnedsättning. Välfärdstekniken ska utgå från kriterierna för ”God vård och omsorg” vilket innebär att vården och omsorgen ska vara kunskapsbaserad, säker, tillgänglig, effektiv och jämlik samt utgå från individens behov. Exempel på välfärdsteknik är olika former av hjälpmedel för det dagliga livet som innehåller digital teknik som digitala trygghetslarm, tillsyn via kamera, sensorer för påminnelser, robotar och datorprogram.

Att införa välfärdsteknik i kommunens verksamheter ställer krav på att kommunens styr- och ledningsprocess har sett till att det finns kunskap, processer och en tydlig ansvarsfördelning för att genomföra digitaliseringsprojekt på ett säkert sätt.

Revisorerna bedömer att det finns en risk för att digitaliseringsarbetet genomförs utan att säkerhetsfrågorna beaktas tillräckligt, vilket kan leda till att sårbarheter finns som inte identifieras.

Med anledning av ovanstående drar kommunens revisorer slutsatsen i sin riskanalys, att kommunens införande av digital välfärdsteknik behöver granskas.

2.1 Syfte, revisionsfrågor och avgränsning

Syftet med granskningen har varit att bedöma om kommunstyrelsen har säkerställt att införandet av digital teknik inom vård- och omsorg sker på ett ändamålsenligt sätt.

Granskningen har omfattat följande revisionsfrågor:

- Finns beslutade styrdokument som tydliggör uppdrag och ansvar för digitaliseringsarbetet inom vård- och omsorg?
- Finns en ändamålsenlig organisation för digitaliseringsarbetet?

- Har kommunstyrelsen säkerställt att verksamheterna beaktar säkerhet i sitt digitaliseringsarbete?
- Finns dokumenterade regler för medarbetares åtkomst till känslig information?
- Finns en tillräcklig intern kontroll för att säkerställa att endast behöriga får åtkomst till information och utrymmen som de har behov av utifrån organisationstillhörighet och roll?
- Har tekniska säkerhetsåtgärder vidtagits för att säkerställa att inte känsliga uppgifter röjs till obehöriga?

Granskningen har avgränsats till att avse digital välfärdsteknik inom vård- och omsorg. Granskningen avser kommunstyrelsen.

2.2 Revisionskriterier

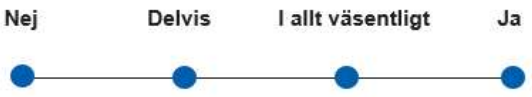
I granskningen har revisionskriterierna utgjorts av:

- Kommunallagen 6 kap § 6
- Dataskyddsförordningen artikel 32
- Offentlighets och sekretesslagen 26 kap § 1
- Digitaliseringsprogram
- Informationssäkerhetspolicy

2.3 Metod

Granskningen har genomförts genom dokumentstudier, intervjuer och stickprov. En förteckning över intervjupersoner och granskade dokument finns i bilaga A. Vidare har stickprov genomförts. Stickproven har omfattat kontroll av behörigheter och loggar inom systemet för nyckelfria lås. Stickprovet har omfattat tre enheter inom verksamhetsområdet, både inom ordinärt och särskilt boende.

De bedömningar som avlämnas i granskningen har utgått ifrån följande bedömningsnivåer.



Rapporten är faktakontrollerad av samtliga intervjuade.

3 Resultat av granskningen

3.1 Styrdokument

Digitaliseringsprogram

Kommunfullmäktige i Kungälvs kommun har antagit ett digitaliseringsprogram[1], med syfte att styra digitaliseringen och skapa en gemensam riktning för området inom kommunen. Av programmet framgår ytterligare att syftet är att:

- Öka omställningsförmågan genom innovation och automatisering för att öka effektiviteten och förbättra kvalitén inom välfärden.
- Bidra till att verksamheternas mål inom vård, skola och omsorg uppnås.

Av programmet framgår att syftet ska uppnås genom nya arbetssätt, öppen och serviceinriktad förvaltning och smarta tjänster.

I digitaliseringsprogrammet beskrivs mål och viljeriktning inom digitalisering. Till målen finns även fastställda delmål. Mål och delmålen är:

Smartare förvaltning

- Ökad tillgänglig service
- Ökad samverkan på fler nivåer och områden
- Effektivisera och skapa värde genom att nyttja digitaliseringens möjligheter. Förbättra interna samarbetet genom nya digitala arbetssätt.

Förenkla vardagen

- Digitala tjänster ska utformas efter kundens behov.
- Digitala tjänster ska vara enkla och säkra att använda.
- Våra tjänster upplevs som en sammanhållen digital service.

Ökad digital förmåga

- Förbättra styrning, kontroll och nyttorealisering så att digitaliseringen främjas.
- Ökad kompetens kring digitala satsningar och utveckling för att accelerera digitaliseringen.
- Kommunicera tydligt och enkelt för att sprida lärdomar.

Vidare framförs strategier för hur målen ska uppnås. Ytterligare framgår hur styrdokumenten ska levandegöras och hur uppföljning ska ske. Uppföljning av

[1] Beslutades av kommunfullmäktige 2023-11-02

digitaliseringsarbetet ska årligen ske i kommunstyrelsen och vid behov i kommunstyrelsens utskott.

I relation till digitaliseringsprogrammet finns andra styrande dokument, exempelvis informationssäkerhetspolicy och riktlinjer för informationssäkerhet. Av informationssäkerhetspolicyn framgår kommunens inriktning avseende arbetet med informationssäkerhet. Av policyn framgår strategiska mål med informations-säkerhetsarbetet. De strategiska målen är:

- Systematisk uppföljning av laglighet i behandling av kommunens information och informationstillgångar.
- Kommuninvånare, företag och föreningar ska känna sig trygga i kommunens behandling av deras uppgifter.
- Informationssäkerhet ska vara en integrerad del av kommunens hantering av handlingar, uppgifter och information.
- Robusthet i kommunens informationshantering vid normalläge, kris eller höjd beredskap.
- Baserade på kravställningen i SS-EN ISO/IEC 27002:2022

Av riktlinjer för informationssäkerhet framgår ansvar och roller inom informationssäkerhetsarbetet.

Mål, strategi och plan - digitalisering Trygghet och stöd

Av digitaliseringsprogrammet framgår att förutom den kommunövergripande strategin ska förvaltningens olika sektorer inom ramen för sitt samhällsuppdrag konkretisera denna i sina respektive verksamhetsplaner. Sektor Trygghet och stöd har tagit fram en plan[2] kopplad till digitaliseringsprogrammet. Planen omfattar åren 2022 – 2024. Av planen framgår tre övergripande mål avseende digitalisering inom sektor trygghet och stöd:

- Öka individens delaktighet och självständighet
- Minska det digitala utanförskapet
- Förbättra arbetsprocesser med hjälp av digitalisering

Av styrdokumenten framgår ytterligare mål kopplade till områdena; vård och omsorgsboende, sociala resurser, myndighet, hemsjukvård, LSS-boende, hälsofrämjande och stöd i ordinärt boende.

Utifrån de olika målen framgår olika strategier/aktiviteter för hur målen ska uppnås. I planen specificeras även en handlingsplan för 2022–2024 som utgår från de

[2] Mål, strategi och plan digitalisering, sektor trygghet och stöd, 2022-09-09

aktiviteterna som är specificerade. Av planen framgår aktiviteterna, verksamheterna som ska genomföra aktiviteten samt hur status är avseende aktiviteten. Statusen är uppdelad i klar, påbörjad eller ej påbörjad.

Systemförvaltarhandbok

Av systemförvaltarhandbok[3] framgår att kommunen har etablerat en systemförvaltningsmodell. Systemförvaltning avser förvaltning av alla system som används. System kan delas in i IT-system och verksamhetssystem. Vidare beskrivs ett antal roller inom systemförvaltningsarbetet, däribland systemägare och systemförvaltare. I handboken beskrivs att systemägare och systemförvaltare ska vara obligatoriska för alla system i Kungälvs kommun. Systemägare ansvarar för verksamhetsspecifika system och är vanligen sektorchefer. Systemägarna delegerar delar av det tekniska ansvaret till systemförvaltare och enligt intervjuade finns ett nära samarbete i arbetet. Av intervjuer framgår att systemförvaltarhandboken är känd och etablerad i kommunen. Giltighetstiden för systemförvaltarhandboken var mars 2024. Av intervjuer framgår att handboken är under revidering.

3.1.1 Bedömning

Vår bedömning är att det i allt väsentligt finns beslutade styrdokument som tydliggör uppdrag och ansvar för digitaliseringsarbetet inom vård- och omsorg.

Vi noterar att det finns kommunövergripande styrdokument gällande digitaliseringsarbetet där både mål och strategier för att uppnå målen presenteras. Som en del av arbetet har sektor trygghet och stöd tagit fram plan för digitaliseringsarbetet som framhäver mål och aktiviteter för att utveckla arbetet inom sektorn. Vi noterar att systemförvaltarhandboken inte längre är formellt giltig då det framgår att giltighetstiden var till mars 2024. Av intervjuer framgår att den är under revidering.

3.2 Organisation och ansvarsfördelning

Övergripande

Av riktlinjer för informationssäkerhet[4] beskrivs ansvar och roller inom informationssäkerhetsarbetet. Av riktlinjen framgår att kommunstyrelsen ansvarar ytterst för informationssäkerhetsarbetet. Vidare framgår att systemägare ansvarar för säkerheten i informationstillgångar, klassning av informationstillgångar samt för genomförande av

[3] Systemförvaltarhandbok, Kommundirektör, 2022-04-01
[4] Beslutad av kommunstyrelsen 2023-12-13 §353/2023

riskåtgärder. Systemförvaltaren ska i sin tur stödja systemägaren i arbetet. Enligt riktlinjen ansvarar informationssäkerhetssamordaren för att leda och samordna informationssäkerhetsarbetet med stöd av en informationssäkerhetsgrupp. Gruppen ska bestå av informationssäkerhetssamordnaren, IT-strateg, dataskyddsombud och kontaktpersoner ifrån de olika sektorerna och staben. Av intervjuer framgår att gruppen sammanträder månatligen. Av riktlinjen tydliggörs även att enskilda medarbetare ansvarar för att följa rutiner, policys, riktlinjer och tillämpningar.

Av digitaliseringsprogrammet framgår att det strategiska arbetet koordineras och drivs centralt av IT-strateg, i samarbete med sektors ledningsgrupp och av utsedda representanter från sektorerna.

Sektor trygghet och stöd

Sektor trygghet och stöd är den sektor som arbetar med digitalisering inom vård- och omsorg. I organisationsskiss gällande digitaliseringsarbetet inom sektorn framgår att ansvar och roller finns på alla nivåer. På övergripande nivå finns systemförvaltare[5], dataskyddsombud, digitaliseringsansvarig samt IT-strateg. På sektornivå finns en digitaliseringsledare som enligt intervjuer leder det digitala utvecklingsarbetet inom sektorn. På verksamhetsnivå finns en digitaliseringssamordnare och på enhetsnivå finns digitaliseringsombud. Av intervjuer framgår att digitaliseringssamordnare har nätverksträffar månatligen. Digitaliseringsombuden har nätverksträffar 2 gånger per termin.

Av intervjuer framgår att digitaliseringsombuden i samarbete med personal identifierar och samlar in behov kopplade till digitalisering. Digitaliseringsledaren sammanställer och för vid behov vidare till systemförvaltare, IT-strateg eller andra relevanta aktörer. Digitaliseringsledaren håller även ihop digitaliseringsplanen för sektor trygghet och stöd (se avsnitt 3.1).

Av intervjuer framgår att det finns vissa utpekade personer enligt ovan som arbetar med digitaliseringsfrågan. Vid projekt som avser digitalisering, exempelvis införandet av ett nytt system, kompletteras denna organisation med tillfälliga resurser beroende på område och art. Det kan exempelvis vara verksamhets eller enhetschefer eller ytterligare representanter som blir involverade i arbetet.

Det finns en anvisning för styrning och ledning av projekt[6] inom kommunen som enligt intervjuade inte har följts i sektorn. När detta har uppmärksammats har ett arbete påbörjats med att säkerställa att detta följs. Av anvisningen framgår att en beställare initierar projektet genom ett projektdirektiv som definierar vad som ska utföras. Därefter ska en styrgrupp utses. Styrgruppen ska utgöra ett stöd till beställaren och utpekad projektledare, och ska säkerställa att projektet ligger i linje med förvaltningens

[5] Systemförvaltare finns både centralt placerat och under trygghet och stöd
[6] Styrning och ledning av program, projekt och uppdrag, Beslutad 2023-12-12 av Förvaltningsledningen

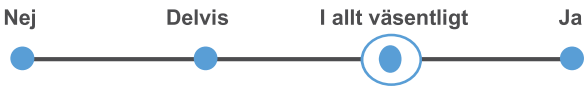
övergripande mål. Vidare framgår att det finns framtagna mallar för att underlätta arbetet, exempelvis mall för projektdirektiv.

Förutom arbetet med att skapa följsamhet till de kommunövergripande anvisningarna gällande projektstyrning framgår även av intervjuer att det har skapats en ny kommunövergripande styrgrupp för digitaliseringsarbetet generellt i kommunen.

Soltak

Kommunen har genom avtal outsourcat sin IT-drift till det gemensamt ägda bolaget Soltak AB[7]. Av intervjuer framgår att samtliga systemförvaltare har veckovisa möten med Soltak, där redovisningar av uppdateringar med mera tas upp. IT-strateg har det sammanhållande ansvaret för kommunens IT och för att tillse en så bra helhet som möjligt för IT-systemen. IT-strateg arbetar enligt intervjuade nära informations-säkerhetssamordnare och de systemförvaltare som finns inom staben. IT-strategens främsta uppgift uppges vara att utgöra språkrör och ha en aktiv dialog med bolaget för att säkerställa en så bra beställning och kravställning som möjligt inom IT.

3.2.1 Bedömning



Vår bedömning är att det i allt väsentligt finns en ändamålsenlig organisation för digitaliseringsarbetet.

Vår bedömning baseras på att det finns riktlinjer som specificerar ansvarsfördelning inom informationssäkerhetsarbetet över hela kommunen. Vidare har sektor trygghet och stöd tagit fram en organisation inom digitaliseringen, med exempelvis digitaliseringsledare, digitaliseringssamordnare och digitaliseringsombud. Detta bedömer vi skapar dels tydliggjorda roller, dels inkludering hela vägen ut i verksamheten.

Vi konstaterar dock att det inte har funnits styrgrupper för respektive projekt, där ansvar och roller varit tydliggjorda. Här ser vi det som positivt att ett arbete pågår med att skapa tydligare styrning i projektarbeten i enlighet med beslutade anvisningar.

3.3 Säkerhet och riskanalyser

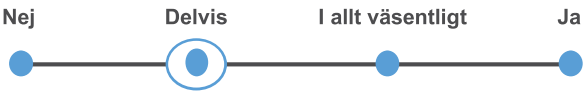
Vi har tagit del av ett utkast gällande checklista[8] för dataskyddsfrågor och informationssäkerhet som ska användas inför upphandling för att säkerställa att verksamheten får med alla krav när det gäller integritetsskydd, personuppgifter och

[7] Soltak AB är ett kommunalt bolag ägt av kommunerna Stenungssund, Orust, Lilla Edet, Tjörn, Ale, Kungälv och Öckerö. Bolaget erbjuder tjänster inom ekonomi, lön, IT och projekt.
[8] Beslutsdatum saknas

informationssäkerhet i förfrågningsunderlaget. Av checklistan framgår att dataskyddssamordnare och dataskyddsombud alltid ska kontaktas inför och under en upphandling som involverar personuppgifter. Vidare framgår att informationssäkerhetssamordnare kan kontaktas inför och under en upphandling för att få stöd i att ta fram ska- och bör-krav. Av checklistan framgår punkter som ska hanteras, besvaras och tas i beaktande inför en upphandling gällande dataskyddsfrågor. Exempelvis framgår av checklistan att riskanalyser och konsekvensbedömningar ska göras om kriterierna för detta är uppfyllda. Av intervjuer framgår att målsättningen är att det alltid ska genomföras riskanalyser samt konsekvensbedömningar vid införande av nya system inom trygghet och stöd. Detta hjälper dataskyddssamordnaren till med inom sektor trygghet och stöd, som även är utsedd kontaktperson för informationssäkerhet från sektorn tillsammans med digitaliseringsledare. Av intervjuer framgår även att det vid konsekvensbedömningar och riskanalyser finns representanter från verksamheterna med. Vi har tagit del av riskanalyser och konsekvensbedömningar. Av riskanalyserna beskrivs riskvärde, sannolikhet att risken inträffar, åtgärd samt vem som ansvarar för respektive åtgärd. Av intervjuer framgick ytterligare att en revidering genomförs efter att ett nytt system är på plats.

Av intervjuer framkom att det i nuläget pågår ytterligare ett arbete med att utveckla en omfattande och tydlig checklista som täcker hela processen inför upphandling av nya system. Enligt uppgift pågår ett arbete vid upphandlingsenheten med att utarbeta denna checklista.

3.3.1 Bedömning



Vår bedömning är att kommunstyrelsen endast delvis säkerställt att verksamheterna beaktar säkerhet i sitt digitaliseringsarbete.

Vi noterar att det finns ett färdigställt utkast till en checklista gällande dataskyddsfrågor vid upphandling, för att beakta integritetsskydd och personuppgifter. Intervjupersoner uppger att sektor trygghet och stöd redan har börjat arbeta utefter denna. Exempelvis framkom att målsättningen är att riskanalyser samt konsekvensbedömningar alltid görs vid införande av nytt system. Vi konstaterar dock att det i övrigt saknas en tydligt dokumenterad process för arbetet inför upphandling av nya system. Vi menar att det är väsentligt att det finns beslutade dokument som tydliggör ansvar och roller för att säkerställa att samtliga berörda beaktar säkerhet i sitt digitaliseringsarbete. Av bland annat gällande informationssäkerhetspolicy framgår att informationssäkerhet ska vara en integrerad del i arbetet.

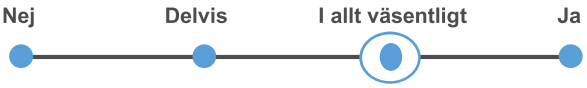
3.4 Behörigheter

Inom sektor trygghet och stöd finns en rutin[9], med syfte att säkerställa att behörigheter tilldelas på ett kontrollerat och spårbart sätt som begränsar möjlighet att data sprids, förändras eller på annat sätt används för ändamål som inte är godkända. Rutinen är framtagen för att tydliggöra ansvarsfördelning vid hantering av behörigheter i verksamhetssystem inom sektor trygghet och stöd.

Av en förteckning[10] framgår hur behörighetsstrukturen är uppdelad för varje verksamhetssystem inom sektor trygghet och stöd, som anses vara samhällsviktiga enligt Nis-direktivet[11]. Syftet med förteckningen är att uppnå en hög gemensam nivå på säkerhet i nätverket och informationssystem. Av förteckningen framgår olika system samt vilken typ av behörighet samtliga medarbetare bör ha utifrån medarbetarens roll. Utifrån samtliga roller framgår en behovsanalys, vad det är för risk vid liten åtkomst, risk vid stor åtkomst, vilken behörighetsnivå medarbetaren bör ha samt hur egenkontroll ska genomföras.

Av rutinen framgår att administration av behörigheter endast ska utföras av systemförvaltare och utsedda spetsanvändare. Spetsanvändare har ansvar för administration av användare på sin enhet. Dock har ansvarig chef det yttersta ansvaret för beslut om behörigheter. Respektive chef har det direkta ansvaret för att se till att behörigheter tilldelas, avslutas och kontrolleras. Beställning av nya eller avslutade behörigheter ska skickas av ansvarig chef till respektive spetsanvändare.

3.4.1 Bedömning



Vår bedömning är att det i allt väsentligt finns dokumenterade regler för medarbetares åtkomst till känslig information.

Bedömningen baseras på att det finns rutiner för hur behörigheter ska utdelas och vilka roller som ska ha åtkomst till vilken information. Av förteckningen framgår behovsanalys, vad det är för risk vid liten åtkomst, risk vid stor åtkomst, vilken behörighetsnivå medarbetaren bör ha samt hur egenkontroll ska genomföras. Av rutinen framgår även vem som är ansvarig för att tillse medarbetarnas åtkomst till känslig information. Vi bedömer att detta på ett tydligt sätt visar hur kommunstyrelsen arbetar för att säkerställa ett ansvarsfullt hanterade av uppgifter rörande enskildas

[9] Hantering av behörigheter i verksamhetssystem, upprättad 2023-10-27 av sektor trygghet och stöd
[10] Behörighetsstruktur verksamhetssystem, upprättad 2023-11-13 av sektor trygghet och stöd
[11] NIS-direktivet syftar till att uppnå en hög gemensam nivå på säkerhet i nätverk och informationssystem inom EU.

personliga förhållanden inom verksamheten utifrån offentlighet- och sekretesslagens bestämmelser.

3.5 Internkontroll och tekniska säkerhetsåtgärder

3.5.1 Verksamhetssystemet

Av rutinen[12] för hantering av behörigheter i verksamhetssystemet som används inom vård- och omsorg, framgår att kontroll av händelselogg ska ske enligt gällande rutin för att kontrollera och säkerställa att användaren inte är inne i ärende som faller utanför ramen för sitt arbete. Av rutinen framgår ytterligare att systemförvaltaren på begäran av chef kan ta fram en lista över aktuella användare. En genomgång/kontroll av samtliga användare för varje verksamhetssystem ska göras av respektive ansvarig chef minst en gång per år. Syftet är att se till att anställda som har bytt arbetsuppgifter eller arbetsplats i kommunen inte har felaktig behörighet. Av intervjuer framgår även att kontroll av händelseloggar görs varje tertial. Resultatet av kontrollerna registreras i verksamhetens systemstöd för kvalitetsuppföljning. Vid intervjuer framgår att inga ytterligare kontroller görs.

Av dokumenten för hantering av behörigheter beskrivs även att i de fall användare inte varit inloggad i verksamhetssystemet under en sammanhängande period om 99 dagar spärras behörigheten automatiskt som en säkerhetsåtgärd mot obehörig åtkomst. För uppföljning av övriga system som används i verksamheten finns ingen automatisk spärrfunktion vid inaktivitet.

3.5.2 Övriga system

Vidare framgår av intervjuer att vissa interna system är kopplade till det övergripande användarkontot[13]. I de fallen spärras användaren automatiskt när användarkontot inaktiveras, vilket görs automatiskt av chef via personalsystemet när anställningen avslutas. Alla system är dock inte uppkopplade mot det övergripande användarkontot, vilket intervjupersoner framhäver är ambitionen i framtiden. Av intervjuer framgår att i de system som saknar ovan nämnd koppling åligger ett ansvar hos varje enhetschef att avsluta behörigheterna vid avslut av anställning vid respektive enhet. Det saknas enligt de intervjuade dokumenterat systematiskt arbete eller kontroller för att säkerställa att behörigheternas omfång är korrekt vid flytt inom enheter.

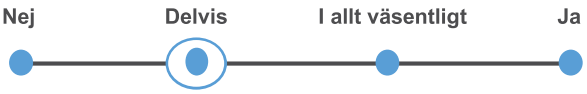
Exempel på system som inte har någon integration från något annat system är systemet för nyckelfria lås. Enligt de intervjuade är det därför upp till enhetscheferna att begära att den som ansvarar för behörigheterna vidtar åtgärder vi förändring. Vid intervjuer framhålls dock att man behöver ha tillgång till en mobil som är kopplad till

[13] Azure Activate Directory konto (AAD-konto)

enheten, för att kunna använda systemet även om man har en användare i systemet. Vid upplåsning framgår även att man behöver vara nära dörren och kan således inte öppna upp på distans.

Av digitaliseringsplanen 2022–2024[14] framgår att tvåfaktorsautentisering ska införas på samtliga system. De verksamheter som omfattas är särskilt stöd i ordinärt boende, boendestöd och hemsjukvård. Av planen framgår att aktiviteten är påbörjad. Vid intervjuer framgår att exempelvis verksamhetssystemet, system för nyckelfria lås och system för trygghetslarm kräver tvåstegsfaktorsinlogg för åtkomst till systemen.

3.5.3 Bedömning



Vår bedömning är att det delvis finns en tillräcklig intern kontroll för att säkerställa att endast behöriga får åtkomst till information och utrymmen som de har behov av utifrån organisationstillhörighet och roll.

Vi noterar att det finns ett flertal system med koppling till övergripande kommunkonto samt rutiner för årliga kontroller av behörigheter. Dock ser vi brister i de system som idag saknar koppling till övergripande kommunkonto.

Vi ser att det finns en risk i att behörigheter inte uppdateras i systemen. Processen som avser att respektive enhetschef ansvarar för att meddela administratör vid avslut bedöms således vara bristfällig. Vid vår stickprovskontroll (se avsnitt 4) bedöms systematiska brister föreligga i den interna kontrollen av behörigheter. Även om granskat system kräver en särskild mobil enhet och/ eller inloggning med ett övergripande kommunkonto för att få åtkomst till systemet finns betydande risker. Dels med utgångspunkt i kvarglömda, borttappade och redan inloggade enheter, dels med utgångspunkt i att det finns flertal gamla användare i systemen som inte uppdaterar lösenord. Detta minskar enligt vår bedömning systemens robusthet mot intrång. Vi ser även risker i behörigheter inom organisationen där personer som byter enhet och verksamhet fortsatt har tillgång till information och utrymmen som de inte har behov av, vilket inte enligt gällande lagstiftning är att anse är förenligt med offentlighets och sekretslagen samt kommunens informationssäkerhetspolicy. Av policyn framgår bland annat att informationssäkerhet ska vara en integrerad del av kommunens hantering av handlingar, uppgifter och information.

Vidare ser vi brister i stickprovskontrollen gällande exempelvis att namn inte uppdateras i systemen som saknar koppling till övergripande användarkonto, detta har noterats särskilt problematiskt vid vår stickprovskontroll då det saknas en tydlig

[14] Mål, strategi och plan digitalisering, sektor trygghet och stöd, 2022-09-09

spårbarhet och kontroll när personer inte fullt ut kan identifieras. Vidare identifierades användare som inte finns i personalsystem.

Vår bedömning är vidare att kommunstyrelsen delvis har vidtagit tekniska säkerhetsåtgärder för att säkerställa att inte känsliga uppgifter röjs till obehöriga.

Vi baserar vår bedömning på att det finns automatiska spärrar som inaktiverar användare vid avslut av anställning. Ytterligare framgår av intervjuer att system som är kopplade till kommunkonton spärras automatiskt när kommunkontot avslutas, exempelvis när en medarbetare slutar på kommunen. Planen är att fler system ska kopplas till kommunkonton, vilket vi anser är positivt. Vidare framgår att tvåfaktorsautentisering inte funnits i samtliga system under granskad period. Vi menar att det är av vikt att kommunstyrelsen har tekniska och organisatoriska säkerhetsåtgärder som är lämpliga i förhållande till risk i enlighet med dataskyddsförordningen artikel 32.

4 Stickprov

Som en del av denna granskning har vi genomfört stickprov i system för nyckelfria lås vid tre av kommunens enheter inom verksamhetsområdet. Med anledning av att arbete sker över flera enheter har stickprov även omfattat en stor mängd medarbetare från andra enheter samt centrala enheter och stödfunktioner.

4.1 Behörighetskontroll

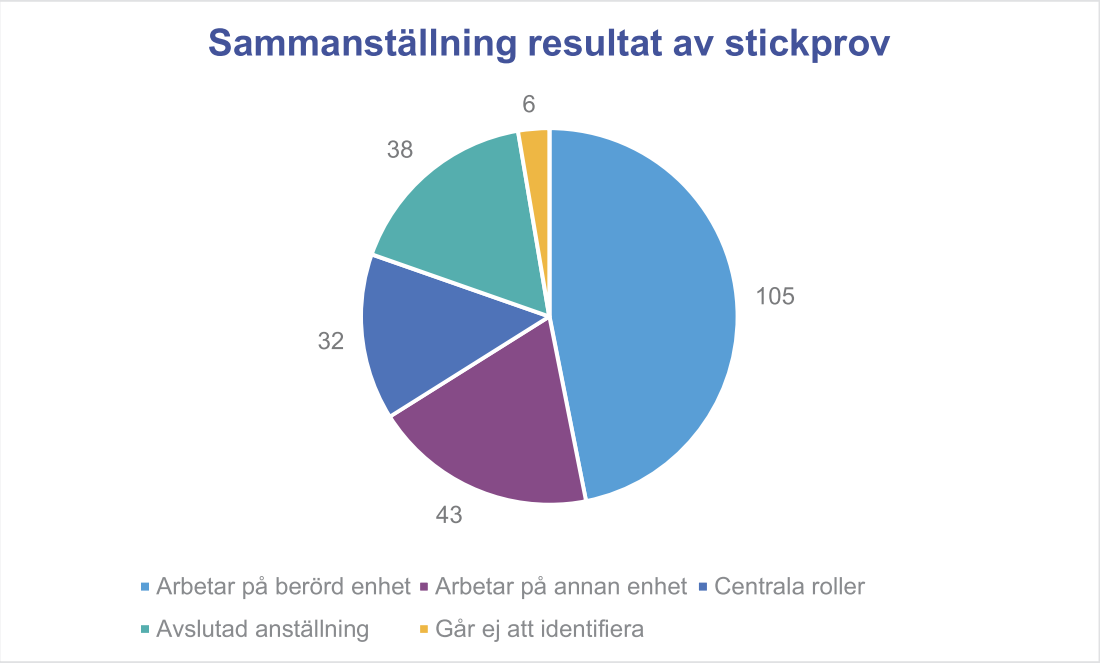
I ett första skede har kontroller genomförts av behörigheter i systemet för nyckelfria lås. Samtliga behörigheter har granskats vid två av kommunens enheter inom såväl ordinärt som särskilt boende. Totalt har 224 behörigheter granskats. Avstämning har gjorts en bestämd dag mitt i en månad, i detta fall 15 maj 2024.

Vid granskningen har förteckning över samtliga med behörighet användare, användare med delegering, administratör och administratör med delegeringsrätt granskats. Detta har i sin tur stämts av mot förteckning över samtliga med en anställning vid enheten vid aktuellt datum.

Av totalt 224 behörigheter konstateras att:

105 behörigheter var för personal anställda på enheten (4 av dessa hade dock sitt tidigare namn i systemet trots namnbyte), 32 behörigheter var för personal på centrala roller såsom sjuksköterska, koordinator, administratör eller trygghetslarm. 43 arbetade på annan enhet i organisationen, 38 behörigheter avsåg personal som avslutat anställning och 6 gick ej att bedöma då användarna inte kunde hittas i personalsystem.

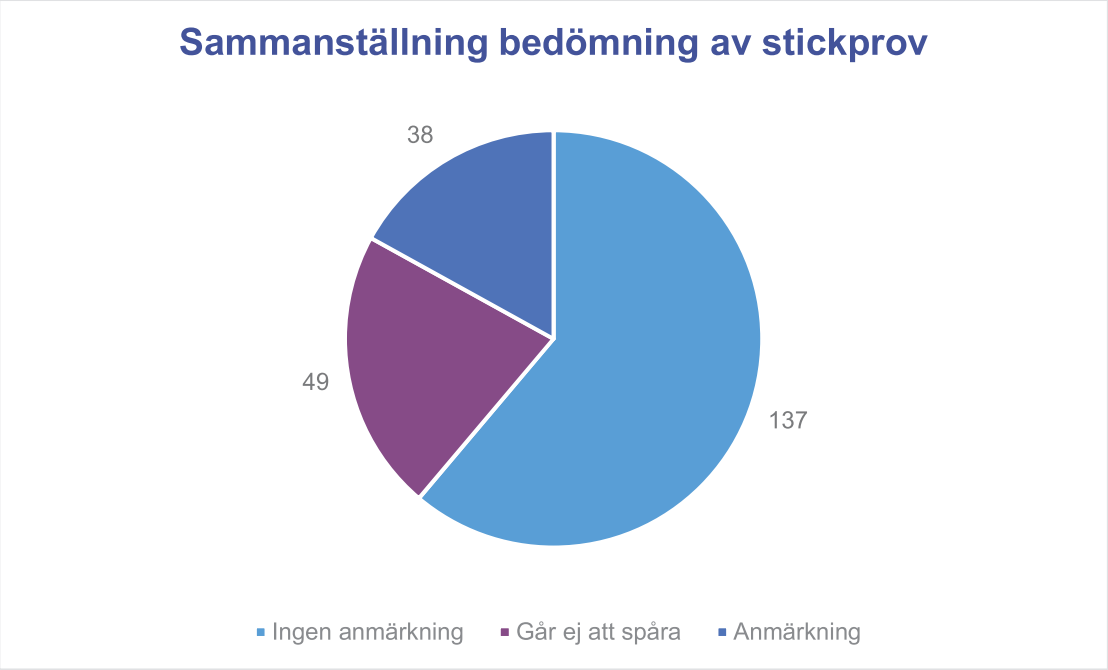
Se sammanställning i nedanstående figur.



Figur 1, sammanställning resultat av stickprov. Totalt 224 behörigheter.

4.1.1 Bedömning behörighetskontroll

Enligt vår bedömning är medarbetare med central roll samt medarbetare på berörd enhet utan anmärkning, totalt 137 behörigheter. Vad gäller de medarbetare som har behörigheter men arbetar på annan enhet, totalt 49, kan det finnas skäl för detta. Exempelvis vad gäller arbete över flera enheter vid behov. Dock saknas tydlig dokumentation om skälen till dessa behörigheter och vi kan således inte spåra detta i dokumentation. Vad gäller de 39 behörigheter som avser personer som avslutat anställning menar vi att det är en direkt brist då det saknas skäl till behörigheterna. Se sammanställning av vår bedömning i figur på kommande sida.



Figur 2, sammanställning bedömning av stickprov. Totalt 224 behörigheter.

Enligt vår bedömning ger detta en samlad bild av att det finns brister i form av att ett flertal personer som inte ska ha behörighet, har behörighet, samt att flera personer har behörighet utan att det tydligt går att spåra om personer ska ha behörighet (detta i form av personer vid andra enheter i organisationen och/ eller personer som inte finns i personalsystemet). Vi är dock medvetna om att enstaka fall kan avse personer med skyddade personuppgifter, bytt namn som vi ej kan spåra, inhyrd personal eller liknande. Detta stickprov syftar dock inte till att ge en uttömmande helhetsbild för arbetet utan syftar till att kartlägga om det finns systematiska brister, vilket vi menar att detta stickprov påvisar.

4.2 Loggkontroll

I ett andra skede har kontroller genomförts av loggar i system för nyckelfria lås, där samtliga händelser under en dag vid en enhet har granskats. Totalt har 60 händelser granskats. Granskning har gjorts en bestämd dag mitt i en månad, i detta fall, 15 maj 2024.

Vid granskningen har underlag utgjorts av förteckning över samtliga händelser under dagen (upplåsningar/ låsningar i såväl portar som dörrar och medicinskåp). Vidare har underlag utgjorts av dagsplanering från planeringssystem. Genom detta har kontroll kunnat göras på om varje händelse i respektive medarbetares logg har överensstämt med dagsplanering för respektive medarbetare.

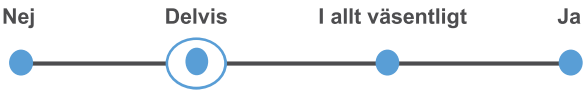
Inga avvikelser har identifierats vid stickprov enligt ovan. Samtliga händelser gällande portar och dörrar går att koppla till insats i dagsplaneringen. Samtliga händelser gällande medicinskåp går att koppla till insats som avser läkemedelshantering.

4.2.1 Bedömning loggkontroll

Samlat bedömer vi att genomfört stickprov inte påvisar några systematiska brister i arbetet vid granskade enheter. Vi vill dock framhålla att detta stickprov inte kan tas som helhetsbild för arbetet utan syftar enbart till att identifiera brister som kan tyda på systematiska brister.

5 Samlad bedömning och rekommendationer

Syftet med granskningen har varit att bedöma om kommunstyrelsen säkerställt att införandet av digital teknik inom vård- och omsorg sker på ett ändamålsenligt sätt.



Vår samlade bedömning utifrån granskningens syfte är att kommunstyrelsen delvis säkerställt att införande av digital teknik inom vård- och omsorg sker på ett ändamålsenligt sätt.

Detta med hänvisning till att det finns styrdokument och en organisation för digitaliseringsarbetet, men det finns brister i projektstyrning och uppdatering av styrdokumenten. Vi noterar att säkerhet beaktas och riskanalyser genomförs vid införandet av nya system, men att det saknas en tydligt dokumenterad process inför upphandlingar av nya system. Internkontroll och tekniska säkerhetsåtgärder är delvis tillräckliga. Dels konstaterar vi brister i arbetet med behörigheter i granskat system, dels har inte alla system implementerat tvåfaktorsautentisering.

Se inledning samt respektive rapportkapitel för en mer detaljerad beskrivning.

Utifrån resultatet av vår granskning rekommenderar vi kommunstyrelsen att:

- Säkerställa att samtliga styrdokument är aktuella.
- Säkerställa tydliga ansvar och roller i projektarbeten på området genom följsamhet till beslutade anvisningar.
- Fastställ rutiner för arbetet inför upphandling av nya system, som tydliggör ansvar och roller i arbetet med beaktandet av säkerhetsfrågor.
- Tillse att det finns ett systematiserat arbete för att säkerställa att behörigheter i samtliga är korrekta och uppdaterade.
- Säkerställ att tekniska säkerhetsåtgärder såsom tvåfaktorsautentisering implementeras i samtliga system.

Kungälvs kommun
Granskning av kommunens införande av digital välfärdsteknik

2025-01-10

Datum som ovan

KPMG AB

Joakim Hackström-Larsson
Verksamhetsrevisor

Amalie Christensen
Verksamhetsrevisor

Erik Söderberg
Certifierad kommunal yrkesrevisor

Bilaga A

Intervjuer har genomförts med:

- Sektorchef trygghet och stöd
- Verksamhetschef äldreomsorg
- Digitaliseringsledare trygghet och stöd
- Dataskyddsamordnare
- Informationssäkerhetssamordnare
- Systemförvaltare – centralt
- Systemförvaltare – trygghet och stöd

Följande dokument har granskats (omfattar inte stickprovet)

- Kommunstyrelsens reglemente
- Digitaliseringsprogram Kungälv
- Mål, strategi och plan digitalisering, sektor trygghet och stöd
- Informationssäkerhetspolicy
- Riktlinjer för informationssäkerhet
- Systemförvaltarhandbok (under revidering)
- Behörighetsstruktur verksamhetssystem (förteckning)
- Hantering av behörigheter i verksamhetssystem (rutin)
- Konsekvensbedömningar och riskanalyser
- Internkontrollplan kommunstyrelsen 2024
- Internkontrollplan sektor trygghet och stöd 2024
- Checklista - dataskyddsfrågor och informationssäkerhet tidigt i upphandlingsprocessen
- Styrning och ledning av program, projekt och uppdrag

PENNEO

Signaturerna i detta dokument är juridiskt bindande. Dokumentet är signerat genom Penneo™ för säker digital signering. Tecknarnas identitet har lagrats, och visas nedan.

"Med min signatur bekräftar jag innehållet och alla datum i detta dokumentet."

ERIK SÖDERBERG
Undertecknare
Serienummer: ea0c4c51fd4317[…]0e62741725d51
IP: 212.37.xxx.xxx
2025-01-21 08:22:30 UTC

Joakim Hackström Larsson
Undertecknare
Serienummer: 285ca3512a48bf[…]7db8136a1b3f1
IP: 93.92.xxx.xxx
2025-01-21 09:01:07 UTC

AMALIE CHRISTENSEN
Undertecknare
Serienummer: e411f64facbedb[…]c6bdb5451e7ab
IP: 83.191.xxx.xxx
2025-01-21 09:06:56 UTC

Penneo dokumentnyckel: YVYE3-KN0K0-V28NJ-AYGVU-1MW6K-GFTF0