BORÅS STAD

Instans
Kommunstyrelsen

Kc2

BESLUTSFÖRSLAG

Revisionsrapport - Informationssäkerhet

Kommunstyrelsen föreslås besluta:

Kommunstyrelsen lämnar upprättat svar på revisionsrapporten om Informationssäkerhet till Revisionskontoret.

Datum
2017-11-28 Ulf Olsson
Kommunalråd

Datum
2017-11-29 Annette Carlson
Kommunalråd

☐ Tillstyrkes

☐ Alternativt förslag

Diarienummer: KS 2017-00679 Programområde: 001
Handläggare: Magnus Widén

Datum
2017-11-20 Magnus Widén
Ekonomichef

Magnus Widén
Handläggare
033 357142

Datum
2017-12-18

Instans
Kommunstyrelsen
Dnr KS 2017-00679
007

Revisionsrapport - Informationssäkerhet

Förslag till beslut

Kommunstyrelsen lämnar upprättat svar på revisionsrapporten om Informationssäkerhet till Revisionskontoret.

Sammanfattning

Stadsrevisionen har 2017-10-09 översänt en revisionsrapport angående ”Informationssäkerhet” till Kommunstyrelsen.

Kommunstyrelsen instämmer i stort i de påpekanden som finns i revisionsrapporten, men pekar också på att en rad åtgärder vidtagits och kommer att vidtas.

Kommunstyrelsen har i budget för 2018, äskat medel för att anställa en Informationssäkerhetsansvarig som skall arbeta med de frågor som beskrivs i rapporten.

Utbildningar i informationssäkerhet både har genomförts och planeras, t.ex. i SKLs metod KLASSA.

Efterfrågade rutiner och styrdokument i informationssäkerhet kommer att tas fram.

Ärendet i sin helhet

Stadsrevisionen har 2017-10-09 översänt en revisionsrapport angående ”Informationssäkerhet” till Kommunstyrelsen, Servicenamnden samt Vård- och äldrenämnden, där man granskat in-formationssäkerheten i Borås Stad. Då såväl Servicenamnden som Vård- och äldrenämnden tillskrivits avser detta svar endast de punkter som rör Kommunstyrelsen.

Kommunstyrelsen instämmer i stort i de påpekanden som finns i revisionsrapporten, men pekar också på att en rad åtgärder vidtagits och kommer att vidtas, vilket redovisas nedan.

Revisionskontoret skriver ”De brister som har identifierats i granskningen bedöms främst bero på att Borås Stad till stor del saknar uppdaterade policys och rutiner för informationssäkerhet. De dokument som finns har i flertalet fall inte beslutats i enlighet med delegationsordningen.”. Man påpekar vidare att ”det inte finns någon särskilt utsedd person som arbetar med övergripande informationssäkerhetsfrågor.”.

Postadress
501 80 Borås

Besöksadress
Kungsgatan 55

Hemsida
boras.se

E-post
boras.stad@boras.se

Telefon
033-35 70 00 vxl

Kommunstyrelsen har i budget för 2018, äskat medel för att anställa en Informationssäkerhetsansvarig. Dennes primära uppgift blir att ta fram ett koncernövergripande LIS (Ledningsinformationssystem) för Informationssäkerhet. Själva Informationssäkerhetspolicyn avses ta fram till politiskt beslut, medan de underliggande dokumenten beslutas på tjänstemannanivå, då de rör verkställighet. Därmed åtgärdas de brister som idag finns vad gäller styrdokument för Informationssäkerhet. Den uppdaterade versionen av ”Informationssäkerhetsinstruktion användare”, kommer att spridas till samtliga medarbetare.

Revisionen pekar på att ”Inga utbildningar inom Informationssäkerhet genomförs”, men att sådana planeras. Under hösten har samtliga förvaltnings- och bolagschefer fått en kortare genomgång av Dataskyddsförordningen. Ett antal styr- och ledningsgrupper på förvaltningarna samt samtliga IT-ansvariga, har fått en längre genomgång. Samtliga systemansvariga för våra verksamhetssystem och snarlika kompetenser (ca 90 personer), har fått en heldagsgenomgång av ISO 27000 och KLASSA. För att snabbt sätta fokus på och höja kunskapen om informationssäkerhetsfrågorna bland anställda, beslutade IT-styrgruppen den 30 oktober 2017 att samt-liga anställda ska genomgå MSBs informationssäkerhetsutbildning DISA (Datorstödd Informat-ionssäkerhetsutbildning för Användare).

Kommunstyrelsen kommer att följa upp hur bolagen arbetar med den nya Dataskyddsförordningen som träder i kraft den 25/5 2018, t.ex. vid planerings- och uppföljningssamtalen.

Kommunstyrelsen anser det dock varken nödvändigt eller lämpligt att skriva in i bolagens ägar-direktiv, vilka policys som gäller för bolagen. Detta framgår när besluten tas i Kommunfullmäktige.

De två dokument som uppges ej ha beslutats enligt delegationsordningen är ”Informationssäkerhetsinstruktion användare” och ”Riktlinjer för informationssäkerhet - Brandväggfunktion”.

Det förstnämnda dokumentet ingick i BITS-konceptet (Basnivå för IT-säkerhet) framtaget av Krisberedskapsmyndigheten. Dokumentet ansågs när det togs fram ligga inom verkställighet och underställdes därför inte för politiskt beslut. Dock var avsikten att ta fram en överordnad Informationssäkerhetspolicy till politiskt beslut, i vilken underliggande dokument, bl.a. detta, skulle pekas ut.

Vad gäller dokumentet ”Riktlinjer för informationssäkerhet - Brandväggfunktion”, så är det inte avsett att ingå bland Borås Stads styrdokument, även om ordet ”brandväggspolicy” förekommer i själva dokumentet. Uttrycket ”brandväggspolicy” är vedertagen branschstandard och avser den uppsättning regler som läggs in i brandväggen, så att den ger det skydd och de funktioner som organisationen är i behov av. Dokumentet benämns istället ”Standardiserad IT - Brand-väggsfunktion”. Det kommer inte, i sin nuvarande form, att tas upp till politiskt beslut, då dokumentet rör teknisk konfiguration av brandväggens funktion.

Borås Stads IT-styrgrupp fattade den 30 november 2017 beslut om att använda SKL's metod KLASSA för klassning av personuppgiftsbehandlingar. I detta sammanhang hanteras såväl frå-gan om klassning av information och personuppgiftsbiträdesavtal samt med vilket lagstöd registreringen görs.

Stadsrevisionen framhåller att ”Det finns inga dokumenterade säkerhetsrutiner för Heroma” och att ”Kommunstyrelsen bör i samarbete med övriga nämnder ta fram säkerhetsrutiner…”.

Tjänsteförvaltaren kommer att få i uppdrag att tillsammans med informationssäkerhetsansvarig ta fram säkerhetsrutiner.

Stadsrevisionen menar att ”Kommunstyrelsen bör säkerställa att behörighetskontroller sker löpande…” samt att ”kontinuitetsplaner prövas löpande”. Detta är uppgifter som ingår i ordinarie systemförvaltning för respektive verksamhetssystem. Kommande LIS för informationssäker-het, kommer att täcka in och ställa krav på att dessa aspekter beaktas och följs upp.

Samverkan

Ej aktuellt.

Beslutet expedieras till

1. Revisionskontoret, Borås Stad

Ulf Olsson
Kommunstyrelsens ordförande

Magnus Widén
Ekonomichef

BORÅS STAD
Stadsrevisionen

Missiv
2017-10-09

Kommunstyrelsen
Servicenämnden
Vård- och äldrenämnden

INFORMATIONSSÄKERHET

Stadsrevisionen har granskat informationssäkerheten i Borås Stad. Den sammantagna bedömningen är att den interna kontrollen avseende informationssäkerheten inte är tillräcklig.

De brister som har identifierats i granskningen bedöms främst bero på att Borås Stad till stor del saknar uppdaterade policys och rutiner för informationssäkerhet. De dokument som finns har i flertalet fall inte beslutats i enlighet med delegationsordningen.

Borås Stad saknar tillfredställande avtal med tekniska och rättsliga begränsningar som hindrar systemleverantör att ta del av uppgifter som Borås Stad gör tillgängliga via säkerhetskopiering. De uppgifter som skickas till leverantören av Viva har stark sekretess. Kommunstyrelsen och berörda nämnder ska säkerställa att samtliga avtal som reglerar hanteringen av sekretessbelagda uppgifter är förenliga med Offentlighets- och sekretesslagen.

Svar på rapporten från Kommunstyrelsen, Servicenämnden, och Vård- och äldrenämnden emotses senast 2017-12-31.

FÖRSTA REVISORSGRUPPEN

Nils-Gunnar Blanc
Ordförande

ANDRA REVISORSGRUPPEN

Boris Preijde
Ordförande

Borås Stads revisionskontor

Postadress	Besöksadress	Webbplats	E-Post	Tel	Fax
501 80 Borås	Sturegatan 42	boras.se/revisionskontoret	revisionskontoret@boras.se	033-35 71 54	033-35 71 57

Informationssäkerhet

Stadsrevisionen. Borås

Rapport

2017

Olof Fredholm
Anna Duong

Innehållsförteckning

1 Projektbeskrivning

1.1 Bakgrund till revisionens granskningsprojekt

Borås Stad liksom övriga kommuner blir allt mer beroende av sina IT-system. Ny teknik utgör en viktig komponent för fungerande och effektiva verksamhetsprocesser men medför även risker när det gäller informationssäkerhet. En stor del av den samhällsviktiga verksamheten ligger under kommunens ansvar i form av förvaltningar eller bolag. Säker informationshantering är central för att säkerställa detta uppdrag. Är informationssäkerheten undermålig finns risk för att känslig information sprids, vilket kan leda till förtroendeförlust och ekonomisk skada.

Myndigheten för samhällsskydd och beredskap (MSB) har publicerat rapporten *En bild av kommunernas informationssäkerhetsarbete 2015*. Rapporten syftar till att fördjupa och belysa den problematik som kommunerna står inför när det gäller arbetet med informationssäkerhet.

Stadsledningskansliet (Stadsarkivet och Strategisk IT) har genomfört en granskning avseende kommunens informationssystem och dess innehåll.[1] Huvudsyftet med granskningen var att skapa en bild av vilken information som finns i kommunens olika informationssystem och hur den hanteras, men också att ge stöd till arbetet med att ta fram ett underlag för att kunna bedöma vilken information som skulle kunna vara aktuell att arkivera digitalt. Granskningen tar sin utgångspunkt i Arkivlagen. Granskningen resultat visar att informationshanteringen i Borås Stads IT-system på många sätt är eftersatt. I rapporten berörs informationssäkerheten, men man framhåller att ytterligare granskning behövs för att få en fullständig bild av denna.

1.2 Syfte och revisionsfrågor

Utifrån ovanstående bakgrund syftar projektet till att granska om Borås Stad har en tillfredsställande intern kontroll när det gäller informationssäkerhet.

Revisionsfrågor

- Bedrivs ett strukturerat arbete för att säkerställa förutsättningar för god informationssäkerhet?
- Säkerställer Kommunstyrelsen en tillräcklig intern kontroll avseende den övergripande informationssäkerheten?

1.3 Avgränsningar

Granskningen omfattar Borås Stads övergripande informationssäkerhetsarbete, samt granskning av verksamhetssystemen Viva och Heroma. Urvalet av verksamhetsystem har skett genom risk- och väsentlighetsanalys. Granskningen genomförs genom dokumentstudier och enkäter/intervjuer. Inga tester av den faktiska informationssäkerheten har genomförts.

1.4 Revisionskriterier

Granskningen utgår från Kommunallagen, samt Myndigheten för samhällsskydd och beredskaps (MSB) rekommendationer för kommuners informationssäkerhet.

Revisionskriterier är:

- Kommunallagen (1991:900)
- Offentlighets- och sekretesslagen (2009:400)
- MSB:s rekommendationer

[1] Granskning av informationshantering i Borås Stads IT-system 2016

1.4.1 Kommunallagen

Enligt 6 kap. 7 § Kommunallagen skall nämnderna var och en inom sitt område se till att verksamheten bedrivs i enlighet med de mål och riktlinjer som fullmäktige har bestämt samt de föreskrifter som gäller för verksamheten. De ska också se till att den interna kontrollen är tillräcklig samt att verksamheten bedrivs på ett i övrigt tillfredsställande sätt.

1.4.2 Offentlighets- och sekretesslagen

Rätten att ta del av allmänna handlingar regleras i Tryckfrihetsförordningen och Offentlighets- och sekretesslagen (OSL). Enligt 3 kap 1 § OSL innebär sekretess ett förbud att röja en uppgift, vare sig det sker muntligen, genom utlämnande av en allmän handling eller på något annat sätt.

Vid kontraktering som medför att informationen hos myndighet blir tillgänglig även för tjänsteleverantör måste OSL begräsningar beaktas, och bedömning ske om överlämnandet är förenligt med OSL.

1.4.3 MSB:s rekommendationer

MSB har givit ut föreskrifter om statliga myndigheters informationssäkerhet. Föreskrifterna pekar på att myndigheterna ska följa de internationella standarderna på området, ISO/IEC 27001 och ISO/IEC 27002. Dessa föreskrifter är endast bindande för statliga myndigheter men det finns enligt MSB stora vinster med att också kommuner arbetar med informationssäkerhet på samma systematiska sätt.[2] Granskningen kommer därför att utgå från utvalda delar av MSB:s rekommendationer och i tillämpliga delar utgå från den struktur som finns i ledningssystem för informationssäkerhet (LIS[3]

1.5 Ansvariga nämnder

Kommunstyrelsen är ansvarig för att driva övergripande IT-frågor och systemägare för verksamhetssystemet Heroma. Servicenämnden är operativt ansvarig för stora delen av infrastrukturen och drift av IT-miljön. Vård- och äldrenämnden är systemägare till verksamhetssystemet Viva.

1.6 Granskningsansvariga

Granskningsledare för projektet är Olof Fredholm vid Revisionskontoret. Projektmedarbetare är Anna Duong vid Revisionskontoret.

1.7 Metoder

Metoderna för granskningen är dokumentstudier och intervjuer/enkäter riktade mot tjänstemän vid berörda förvaltningar.

[2] Kommunens informationssäkerhet – en vägledning s.2

[3] ISO/IEC 27001:2006

2 Granskningsresultat

Stadsrevisionens bedömningar presenteras i anslutning till respektive område och sammanfattas i avsnitt *3 Bedömningar*. Granskningen fokuserar på avvikelser. Granskade delområden som bedöms fungera tillfredsställande är som regel inte med i rapporten.

2.1 Organisation av informationssäkerheten

Informationssäkerhet handlar om att skydda all känslig information oavsett i vilken form den finns i eller uppkommer i. Då informationen i allt högre utsträckning finns i IT-system handlar informationssäkerhet i allt högre utsträckning om teknik.

Borås Stad med dess bolag hanterar en betydande del av samhällsservicen. Bolagens IT-service är skild från koncernen i övrigt. Det finns därför ingen sammanhållen bild över hela kommunkoncernens informationssäkerhet.

Avseende förvaltningarna sköts IT-verksamheten utifrån en modifierad beställar-utförarmodell, modellen benämns Tjänsteförvaltningsmodellen. Stadsledningskansliet är ansvarig beställare, men utföraren som är Servicekontoret (Dataservice) har budgeten. IT-tjänster levereras också av externa utförare. Stadsrevisionen granskade beställar-utförarmodellen i Borås Stad 2015. I granskningen konstaterades bl.a. att Tjänsteförvaltningsmodellen är under översyn vilket den fortsatt uppges vara. Arbetet leds av Borås Stads IT-styrgrupp.

Respektive verksamhetssystem förvaltas ute på berörda förvaltningar och har utsedda tjänsteägare och tjänsteförvaltare. Respektive förvaltning har en IT-samordnare som ansvarar för att samordna IT-arbetet på förvaltningen.

Verksamhetssystemet Viva förvaltas av Vård- och äldrenämnden men används av samtliga nämnder i det sociala klustret. Driften av Viva sköts av Servicekontoret Dataservice. Flertalet av uppgifterna i Viva omfattas av stark sekretess.

Verksamhetssystemet Heroma är Borås Stads personal- och lönesystem och förvaltas av Stadsledningskansliet men används av samtliga nämnder och några bolag i Borås Stad. Driften av systemet sköts av Servicekontoret, Dataservice. Vissa uppgifter i Heroma omfattas av sekretess.

Det primära uppdraget med att samordna informationssäkerheten ligger på Stadsledningskansliet. Det finns ingen utsedd person som arbetar med övergripande informationssäkerhet för hela Borås Stad. Vid intervju uppges att Stadsledningskansliet kommer att rekrytera en informationssäkerhetssamordnare till år 2018.

Iakttagelse	Bedömning
Det finns ingen samlad bild över koncernens informationssäkerhetsharbete	Kommunstyrelsen bör säkerställa att det finns en samlad bild över kommunkoncernens informationssäkerhetsarbete. Fokus bör initialt riktas på de bolag som driver eller understödjer kritisk infrastruktur. Detta då bolagens informationssäkerhetsarbete ligger utanför kommunens ordinarie organisation
Det finns ingen utsedd person som arbetar med informationssäkerhet	Kommunstyrelsen hanterar frågan genom rekrytering

2.2 Informationssäkerhetspolicy, och styrdokument

Borås Stad har ingen av Kommunstyrelsen eller Kommunfullmäktige fastställd informationssäkerhetspolicy. Enligt intervjuer arbetar man delvis efter en äldre ej färdigställd informationspolicy. Det pågår ett arbete i samarbete med övriga Sjuhäradskommuner som syftar till att ta fram en gemensam informationssäkerhetspolicy.

Flera av styrdokumenten avseende informationssäkerhet är till följd av bl.a. den snabba IT-utvecklingen inaktuella.[4] Enligt intervjuer kommer arbetet med att se över styrdokumenten påbörjas när en informationssäkerhetssamordnare är rekryterad. I granskningen noteras att Riktlinjer för informationssäkerhet och Brandväggspolicy inte har antagits i enlighet med delegationsordning.

Iakttagelse	Bedömning
Det finns ingen informationssäkerhetspolicy	Kommunstyrelsen bör ta fram en informationssäkerhetspolicy, och utifrån policyn se över vilka övriga styrdokument som behöver uppdateras. Kommunstyrelsen bör genom ägardirektiv säkerställa att bolagen omfattas av informationssäkerhetspolicyn
Styrdokumenten inom området är inte alltid antagna av rätt instans	Kommunstyrelsen bör i det pågående arbetet med informationssäkerhetspolicyn säkerställa att styrdokumenten beslutas enligt delegationsordningen samt att de kommunala bolagen omfattas av policyn genom ägardirektiven
Det finns inga dokumenterade säkerhetsrutiner för Viva	Vård- och äldrenämnden bör i samarbete med övriga nämnder i det sociala klustret ta fram säkerhetsrutiner för Viva där det framgår vad användare får, respektive inte får, göra i systemet, och hur användare ska använda systemet när de är ute hos brukare
Det finns inga dokumenterade säkerhetsrutiner för Heroma	Kommunstyrelsen bör i samarbete med övriga nämnder ta fram säkerhetsrutiner för Heroma där det framgår vad användare får, respektive inte får, göra i systemet

2.3 Hantering av tillgångar

Samtliga informationssystem uppges i intervju ha dokumenterats i en systemförteckning (avseende förvaltningarnas system).

Stadsledningskansliet inleder hösten 2017 ett arbete med informationsklassning av verksamhetssystem. Arbetet ska vara slutfört senast 25 maj 2018 i samband med att den nya Dataskyddsförordningen träder i kraft.

[4] Bl.a. Informationssäkerhetspolicy, Säkerhetsinstruktioner för användare, Riktlinjer avseende förvaringstid för datamedia, brandväggspolicy, gemensam kontinuitetsplan etc.

Informationsklassning av verksamhetssystemen Viva och Heroma kommer att ske under hösten 2017. En projektledare som ska arbeta med informationsklassning avseende Viva är rekryterad. Informationsklassning av Heroma planeras att genomföras inom befintlig förvaltningsorganisation.

2.4 Personal och säkerhet

Alla nya användare (anställda och inhyrd personal) får information i samband med att de får sina anställningsuppgifter. I informationen framgår bl.a. att användaren ska byta lösenord vid första inloggning, lösenordspolicy, samt att sekretessuppgifter eller personuppgifter enligt PuL inte får förvaras där icke behörig personal kan få tillgång till uppgifterna. Det finns en särskild *Informationssäkerhetsinstruktion användare* som inte skickas till nya användare. Detta är enligt intervjuade en brist. Instruktionen som är från 2009 behöver enligt de intervjuade uppdateras.

Inga särskilda utbildningar anordnas avseende informationssäkerhet. Utbildning planeras under hösten avseende ISO 27 000 och informationsklassning. Detta är en metod som hjälper verksamheten att kartlägga brister, ta fram handlingsplaner, samt att ställa upphandlingskrav i syfte att öka informationssäkerheten.

Beställning av behörighet i Viva sker genom att behörig chef fyller i blankett och skickar till IT-administratör eller IT-samordnare som skickar beställning till IT-vård och omsorg för upplägg. Anställda behöver byta lösenord första gången de loggar in i systemet. Upplåsning av låsta konton sker först efter säker identifiering. En anställd kan bara ha en titel i Viva, och det går bara att ha ett inlogg.

Beställning av behörighet i Heroma sker genom blankett och godkänns av behörig chef. Upplåsning av låsta konton sker först efter säker identifiering.

Iakttagelse	Bedömning
Informationssäkerhetsinstruktion användare är inte uppdaterad och skickas inte till nya användare	Kommunstyrelsen bör uppdatera informationssäkerhetsinstruktionen och säkerstalla att den skickas till nya användare
Inga utbildningar inom informationssäkerhet genomförs	Kommunstyrelsen planerar att genomföra utbildningar i informationssäkerhet
En anställd kan bara ha ett inlogg i Viva, vilket innebär att samma behörigheter fungerar på samtliga förvaltningar	Vård- och äldrenämnden bör undersöka möjligheten att införa dubbla inlogg för anställda

2.5 Systemsäkerhet

Säkerhetskopior av de viktiga verksamhetssystemen genomförs regelbundet och bevaras i ett antal versioner. Det genomförs dock inga regelbundna kontroller för att säkerställa att informationssystem kan återstartas med tagna säkerhetskopior. I intervju uppges Dataservice arbeta med att ta fram riktlinjer avseende förvaringstid för datamedia.

Dataservice och systemleverantören säkerhetskopierar Viva. Skulle systemet haverera kan en begränsad mängd användare koppla upp sig mot systemleverantörens server och därmed uppges patientsäkerheten vara säkrad. Driftsättningar i programmet testas först i utbildningsmiljön innan de implementeras vilket uppges fungera väl.

För att Borås Stad ska kunna säkerställa sin reservdriftsmiljö, överförs löpande starkt sekretessbelagda uppgifter[5] från hela Borås Stads sociala kluster till systemleverantören. I avtalet med leverantören finns inga krav på tekniska och / eller rättsliga begräsningar som hindrar systemleverantören eller dennes personal från att ta del av sekretessbelagda uppgifter som Borås Stad gör tillgängliga genom säkerhetskopieringen. Det finns inte heller några krav i avtalet avseende hur leverantören ska skydda de sekretessbelagda uppgifterna mot förstörelse eller olagliga angrepp.

Dataservice säkerhetskopierar Heroma varje natt och systemleverantören säkerhetskopierar Heroma en gång per månad. Sekretess regleras översiktligt i avtal, det finns krav på sekretessförbindelser för leverantörens personal. Skulle systemet haverera finns det möjlighet att arbeta i systemet från andra kommuner med samma system. Hittills har man inte behövt återstarta systemet från en backup. Driftsättningar i programmet testas först i testsmiljön innan de implementeras vilket uppges fungera väl.

Alla användare är administratörer på sina egna datorer, Borås Stad införde modellen på prov vid senaste plattformsuppdatering och intervjuade uppger att det fungerar väl.

Avseende det övergripande användarkontot i Borås Stad sker avstängning av konton per automatik genom att användarkontot är kopplat till AD[6] Motsvarande kontroller sker inte i alla verksamhetsystem.

Förvaltningsorganisationerna för Viva och Heroma har rutiner för tilldelning, borttagning och förändring av behörigheter, och behörigheter sätts utifrån behov. Rutinerna för tilldelning uppges fungera, då verksamheten har ett intresse av att användare får behörighet till systemet. Däremot fungerar det inte avseende borttagning och förändring av behörigheter. Förvaltningsorganisationerna är beroende av att verksamheten meddelar om en person inte längre har behov av befintlig behörighet. Detta uppges inte alltid fungera optimalt. En gång per år uppges behörigheterna stämmas av mot Heroma, och avvikelser rättas till. Heromas behörigheter uppges rättas när felaktigheter upptäcks. Revisionsloggar i Viva uppges granskas löpande. Revisionsloggar i Heroma uppges granskas vid påkallat behov. Det framgår inte av granskningen vilka eventuella åtgärder som vidtas vid brister. Det pågår en översyn av inloggningen och behörigheter i Viva, efter ett föreläggande från Datainspektionen.[7] Det som användare ser i systemet har minskats för vissa användargrupper, och framöver kommer det att krävas tvåfaktorsinloggning för att komma in i systemet.

[5] Sekretessuppgifter med så kallad omvänd skaderekvisit

[6] Som är en katalogtjänst från Microsoft som bl.a. hanterar användarnamn

[7] Tillsyn enligt personuppgiftslagen (1998:204) – åtkomst till uppgifter i journalsystem inom socialtjänst (Sociala omsorgsnämndens diarienummer: 2016/SON0023).

Iakttagelse	Bedömning
Tillfredsställande avtal med tekniska och rättsliga begränsningar som hindrar systemleverantören eller dennes personal från att ta del av sekretessbelagda uppgifter som Borås Stad gör tillgänglig via säkerhetskopiering saknas	Vård- och äldrenämnden ska i samarbete med övriga nämnder i det sociala klustret, och Servicenämnden säkerställa att tillfredsställande avtal tecknas med tekniska och rättsliga begränsningar med leverantör. I avtalet är det också viktigt att tydliggöra hur leverantören ska skydda lagrade uppgifter mot förstörelse eller olagliga angrepp.
Behörighetskontroller i alla verksamhetssystem sker inte löpande	Kommunstyrelsen bör säkerställa att behörighetskontroller sker löpande i samtliga verksamhetssystem med känsliga uppgifter
Rutiner för borttagning av användare och förändring av användare i Viva fungerar inte tillfredsställande	Vård- och äldrenämnden bör i samarbete med övriga nämnder i det sociala klustret säkerställa att ändamålsenliga och fungerande rutiner för borttagning av användare och förändring av behörighetsrutiner i Viva finns och fungerar tillfredsällande
Rutiner för borttagning av användare och förändring av användare i Heroma fungerar inte tillfredsställande	Servicenämnden bör i samarbete med övriga nämnder säkerställa att ändamålsenliga och fungerande rutiner för borttagning av användare och förändring av behörighetsrutiner i Heroma finns och fungerar tillfredsställande

2.6 Incidenthantering och kontinuitetshantering

Det finns ingen gemensam kontinuitetsplan[8] dokumenterad för Borås Stad. Däremot uppges respektive kritiskt system ha en kontinuitetsplan. Det har inte framgått vid granskningen om kontinuitetsplanerna prövas löpande.

Vid ett tillfälle har Viva i samband med brand i en serverhall haft en större driftsstörning. Verksamheten uppges ha lärt sig av händelsen, och det finns en kontinuitetsplan för verksamheten, som dock uppges vara i behov av revidering.

Enligt Överenskommelse om tjänsteleverans för Viva och Heroma ska Servicekontoret löpande följa nedanstående punkter i systemet och kvartalsvis rapportera till kontaktperson via e-post:

- Antal incidenter
- Utifrån ärendeprioritering mäts uppfyllandegraden i % inom uppsatt tid
- Analys avvikelser
- Målsättning att mäta tillgänglighet i % under öppettider.

Ovanstående mätningar är inte levererade till berörda kundkontakter. Enligt Servicekontoret pågår en översyn kring vilken mätdata som ska levereras till kontaktpersoner.

[8] En kontinuitetsplan syftar till att en organisation ska kunna fortsätta verksamheten vid incidenter, exempelvis brand i server, elavbrott etc.

Iakttagelse	Bedömning
Det har inte framgått vid granskningen om kontinuitetsplanerna prövas löpande	Kommunstyrelsen bör säkerställa att kontinuitetsplaner prövas löpande
Kontinuitetsplanen för Viva är inte uppdaterad	Vård- och äldrenämnden bör säkerställa att kontinuitetsplanen är uppdaterad
Rapportering av mätning i Viva och Heroma är inte levererad till kontaktperson	Servicenämnden bör säkerställa att mätdata levereras i enlighet med Överenskommelse om tjänstelevereans

2.7 Implementeringen av Dataskyddsförordningen

I maj 2018 träder den nya lagen Dataskyddsförordningen i kraft. Lagen ersätter Personuppgiftslagen och delvis även patientdatalagen. Det nya regelverket innehåller flera förändringar jämfört med nuvarande regler och ett relativt omfattande arbete krävs för att anpassa verksamheten till den nya lagen.

Enligt Stadsledningskansliet pågår ett arbete med att förbereda Borås Stad inför det nya regelverket. Samtliga systemansvariga i Borås Stad kommer under hösten 2017 att få utbildning i Sveriges Kommuner och Landstings informationsklassningsverktyg KLASSA, och därefter följer informationsklassning och handlingsplan för respektive verksamhetssystem.

Respektive förvaltning behöver enligt Stadsledningskansliet påbörja ett arbete för att förnya och anpassa samtyckeshanteringen. Flera av de rättigheter som följer med Dataskyddsförordningen uppges enligt intervjuade vara begränsade av andra lagkrav. Borås Stad behöver dock ta fram nya rutiner för samtyckeshantering och se över samtliga personuppgiftsbiträdesavtal. Vidare behöver Borås Stad ta fram en rutin för IT-incidentrapportering, och det behöver det utses ett dataskyddsombud.

3. Sammanfattande bedömning

Den sammantagna bedömningen är att den interna kontrollen avseende informationssäkerheten inte är tillfredsställande i Borås Stad.

De brister som har identifierats i granskningen bedöms främst bero på att Borås Stad till stor del saknar uppdaterade policys och rutiner för informationssäkerhet. De dokument som finns har i flertalet fall inte beslutats i enlighet med delegationsordningen. Det finns i dagsläget inte någon särskilt utsedd person som arbetar med övergripande informationssäkerhetsfrågor. Enligt Stadsledningskansliet ska en person som ansvarar för informationssäkerheten rekryteras. Det är väsentligt att Kommunstyrelsen i utvecklingsarbetet säkerställer att informationssäkerheten är tillfredsställande i såväl förvaltningar som bolag.

Borås Stad saknar tillfredsställande avtal med tekniska och rättsliga begränsningar som hindrar systemleverantör att ta del av uppgifter som Borås Stad gör tillgängliga via säkerhetskopiering. De uppgifter som skickas till leverantören av Viva har stark sekretess. Kommunstyrelsen och berörda nämnder ska säkerställa att samtliga avtal som reglerar hanteringen av sekretessbelagda uppgifter är förenliga med Offentlighets- och sekretesslagen.

Dataskyddsförordningen träder i kraft i maj 2018. Lagen kommer ställa högre krav på organisationen än vad PuL gör, bl.a. behöver alla personuppgiftbiträdesavtal ses över.

Kommunstyrelsen och övriga nämnder bör i samband med kommande informationsklassning tydliggöra vilken information som hanteras i respektive verksamhet, med vilket stöd, och på vilka grunder, till vem uppgifter lämnas ut, hur samtycke inhämtas, och utifrån resultatet vidta relevanta åtgärder för att säkerställa registrerades rättigheter.

I granskningen noteras att statistik avseende driftstörningar i Viva och Heroma inte löpande rapporteras till kontaktperson. Dataskyddsförordningen innehåller nya bestämmelser kring vad en organisation måste göra om de blir utsatta för dataintrång eller på annat sätt förlorar kontrollen över uppgifter som behandlas. I sammanhanget är det därför viktigt att säkerställa att avvikelser identifieras och rapporteras löpande.

Ola Sabel
revisionschef
certifierad kommunal yrkesrevisor

Olof Fredholm
granskningsledare
kommunal yrkesrevisor

4. Källor

Lagar och förordningar

Kommunallagen (1991:900)

Offentlighets- och sekretesslagen (2009:400)

GDPR Dataskyddsförordningen

Normgivande rekommendationer och tillsyn

MSB (2015) Informationssäkerheten i Sveriges kommuner, Analys och rekommendationer utifrån MSB:s kommunenkät 2015

MSB (2012) Kommunens informationssäkerhet – en vägledning

Datainspektionen (2016) Tillsyn enligt personuppgiftslagen (1998:204) åtkomst till uppgifter i journalsystem inom socialtjänst (Datainspektionens diarienr 353/2016)

Kommunala styrdokument och rapporter

Informationssäkerhetsinstruktion användare

Riktlinjer för informationssäkerhet (ej formellt antaget)

Brandväggspolicy (ej formellt antagen)

Överenskommelse om tjänsteleverans för Viva

Granskning av informationshantering i Borås Stads IT-system 2016

Intervjuer

Intervju 1 med representanter för Stadsledningskansliet. 2017-06-12

Intervju 2 med representanter för Vård- och äldreförvaltningen. 2017-07-04

Intervju 3 med representant för Servicekontoret. 2017-08-23

Intervju 4 med representanter för Stadsledningskansliet och Serviceförvaltningen. 2017-08-28

Intervju 5 med representanter från Serviceförvaltningen och Vård- och äldreförvaltningen 2017-09-21

Intervju 6 med förbundsjurist på SKL med specialkunskap inom bl.a. PuL, offentlighet- och sekretess, och IT-rätt 2017-09-26

Övrigt

MSB (2015) En bild av kommunernas informationssäkerhetsarbete 2015

BORÅS STAD

Stadsrevisionen

Besöksadress Sturegatan 42 **Postadress** 501 80 Borås
Telefon 033-35 71 54 **e-post** revisionskontoret@boras.se
Webbplats boras.se/revisionskontoret

Informationssäkerhet

Stadsrevisionen. Borås

Rapportsammandrag

2017-10-03

2017

Borås Stad liksom övriga kommuner blir allt mer beroende av sina IT-system. Ny teknik utgör en viktig komponent för fungerande och effektiva verksamhetsprocesser men medför även risker när det gäller informationssäkerhet. En stor del av den samhällsviktiga verksamheten ligger under kommunens ansvar i form av förvaltningar eller bolag. Säker informationshantering är central för att säkerställa detta uppdrag. Är informationssäkerheten undermålig finns risk för att känslig information sprids, vilket kan leda till förtroendeförlust och ekonomisk skada.

Utifrån ovanstående bakgrund har Stadsrevisionen granskat om Borås Stad har en tillfredsställande intern kontroll när det gäller informationssäkerhet.

Bedömningar

Den sammantagna bedömningen är att den interna kontrollen avseende informationssäkerheten inte är tillfredsställande i Borås Stad.

De brister som har identifierats i granskningen bedöms främst bero på att Borås Stad till stor del saknar uppdaterade policys och rutiner för informationssäkerhet. De dokument som finns har i flertalet fall inte beslutats i enlighet med delegationsordningen. Det finns i dagsläget inte någon särskilt utsedd person som arbetar med övergripande informationssäkerhetsfrågor. Enligt Stadsledningskansliet ska en person som ansvarar för informationssäkerheten rekryteras. Det är väsentligt att Kommunstyrelsen i utvecklingsarbetet säkerställer att informationssäkerheten är tillfredsställande i såväl förvaltningar som bolag.

Borås Stad saknar tillfredsställande avtal med tekniska och rättsliga begränsningar som hindrar systemleverantör att ta del av uppgifter som Borås Stad gör tillgängliga via säkerhetskopiering. De uppgifter som skickas till leverantören av Viva har stark sekretess. Kommunstyrelsen och berörda nämnder ska säkerställa att samtliga avtal som reglerar hanteringen av sekretessbelagda uppgifter är förenliga med Offentlighets- och sekretesslagen.

Dataskyddsförordningen träder i kraft i maj 2018. Lagen kommer ställa högre krav på organisationen än vad PuL gör, bl.a. behöver alla personuppgiftbiträdesavtal ses över.

Kommunstyrelsen och övriga nämnder bör i samband med kommande informationsklassning tydliggöra vilken information som hanteras i respektive verksamhet, med vilket stöd, och på vilka grunder, till vem uppgifter lämnas ut, hur samtycke inhämtas, och utifrån resultatet vidta relevanta åtgärder för att säkerställa registrerades rättigheter.

I granskningen noteras att statistik avseende driftstörningar i Viva och Heroma inte löpande rapporteras till kontaktperson. Dataskyddsförordningen innehåller nya bestämmelser kring vad en organisation måste göra om de blir utsatta för dataintrång eller på annat sätt förlorar kontrollen över uppgifter som behandlas. I sammanhanget är det därför viktigt att säkerställa att avvikelser identifieras och rapporteras löpande.

BORÅS STAD

Stadsrevisionen

Besöksadress Sturegatan 42 **Postadress** 501 80 Borås
Telefon 033-35 71 54 **e-post** revisionskontoret@boras.se
Webbplats boras.se/revisionskontoret