Kommunstyrelsen

Utdrag ur
PROTOKOLL
2018-03-19

§ 42

Svar på revisionsrapport – Granskning av IT- och informationssäkerhet inom samverkansnämnden
KS-2017/711

Beslut

Kommunstyrelsen beslutar

att godkänna svaret till revisorerna

att anmäla svaret till kommunfullmäktige i Knivsta kommun.

Sammanfattning av ärendet

Revisionsbyrån PWC har på uppdrag av revisorerna i Knivsta och Heby kommuner genomfört en översiktlig granskning av Samverkansnämndens arbete med IT- och informationssäkerhetsarbete. Granskningen har även gällt kommunernas informationssäkerhetsarbete på en övergripande nivå.

Underlag i ärendet

Tjänsteskrivelse 2018-03-10 delas ut på sammanträdet. Beslut från arbetsutskottet, § 48, 2018-03-05, beslut från samverkansnämnden, § 9, 2018-02-28, samverkansnämndens tjänsteskrivelse 2018-02-01, yttrande del 1 2018-02-05, yttrande del 2 2018-02-01, PM från Heby kommun, 2018-01-26, revisionsrapport 2017-10-10 samt missiv/följebrev 2017-10-25 har varit utsända.

Anders Fredriksson, IT-strateg, informerar.

Expedieras till:
Akten
Revisionen
Kommunfullmäktige (för anmälan)

Expedierat av Siobhán Górny 2018-04-03

Knivsta kommun

Handläggare	Tjänsteskrivelse	Diarienummer
Åsa Franzén	Datum	KS-2017/711
Kanslichef	2018-03-10	

Kommunstyrelsen

Svar till revisorerna avseende granskningsrapport om informationssäkerhet inom samverkansnämnden oktober 2017

KS-2017/711

Förslag till beslut

Kommunstyrelsen beslutar

att godkänna svaret till revisorerna

att anmäla svaret till kommunfullmäktige i Knivsta kommun.

Sammanfattning

Revisonsbyrån PWC har på uppdrag av revisorerna i Knivsta och Heby kommuner genomfört en översiktlig granskning av Samverkansnämndens arbete med IT- och informationssäkerhetsarbete. Granskningen har även gällt kommunernas informationssäkerhetsarbete på en övergripande nivå.

Bakgrund

Granskningen berör det övergripande informationssäkerhetsarbetet i Knivsta och Heby, vilket till stora delar ligger under KS i respektive kommun. Samverkansnämnden ansvarar för IT-enhetens arbete med informationssäkerhet. Därför har svaret kompletterats med en bilaga från kommunstyrelsens verksamhet i vardera kommun.

Ekonomisk konsekvensanalys

Granskningen medför inga omedelbara kostnader för nämndens verksamhet. Dock kommer det åtgärder som behövs utifrån den nya Dataskyddslagen och övriga justeringar av svensk lagstiftning. Dessa är för att uppfylla EU:s nya dataskyddsförordning (GDPR).

Barnkonsekvensanalys

Barnkonsekvensanalys är gjord enligt checklista.

Lena Fransson
kommundirektör

Beslutet ska expedieras till:
Akten
Mottagare 1
Mottagare 2 osv

Knivsta kommun

Barnchecklista inför beslut

1. Påverkar beslutet barn?

Enligt FN är alla under 18 år att betrakta som barn

Ja ☒ Nej ☐

Förklara oavsett svar.

Informationssäkerhet är viktigt för att många uppgifter som rör barn hanteras i kommuns olika system.

*Om, **ja fortsätt** med frågorna.*

2. Hur har barns bästa beaktats?

Kommunstyrelsen beaktar barns bästa i hanteringen.

3. Beskriv eventuella intressekonflikter.

4. Barn tillfrågas vid övergripande fleråriga planer/styrdokument. Har så skett?

Ja ☐ Nej ☐

Inte aktuellt. Beslutet rör inte övergripande flerårig plan/flerårigt styrdokument ☒

Om ja, förklara på vilket sätt barn varit delaktiga i beslutet, vilka åsikter barnen lyft fram samt hur dessa åsikter beaktats i beslutet. Om nej, förklara varför barn inte tillfrågats.

Samverkansnämnden

Utdrag ur
PROTOKOLL
2018-02-28

§ 9

Svar på revisionsrapport - Granskning av IT- och informationssäkerhet inom samverkansnämnden
SMN-2017/36

Beslut

Samverkansnämnden beslutar

att överlämna yttranden del 1 och 2 samt Heby kommuns PM till kommunfullmäktige i Knivsta kommun samt till revisorerna.

Sammanfattning av ärendet

Revisonsbyrån PWC har på uppdrag av revisorerna i Knivsta och Heby kommuner genomfört en översiktlig granskning av Samverkansnämndens arbete med IT- och informationssäkerhetsarbete. Granskningen har även gällt kommunernas informationssäkerhetsarbete på en övergripande nivå.

Underlag i ärendet

Tjänsteskrivelse 2018-02-01, förslag på yttrande del 1 2018-02-05, förslag på yttrande del 2 2018-02-01 och PM från Heby kommun, 2018-01-26 har varit utsända. Åsa Franzén, kanslichef, Anders Fredriksson, IT-strateg och informationssäkerhetssamordnare, samt Michael von Essen, chef IT-drift, informerar och presenterar ett justerat förslag till beslut.

Expedieras till:
Akten
Kommunfullmäktige
Revisorerna
Heby kommun, för kännedom

Expedierat av Siobhán Górny 2018-03-02

Knivsta kommun

Handläggare	Tjänsteskrivelse	Diarienummer
Anders Fredriksson	Datum	SMN-2017/36
IT-strateg	2018-02-01	

Samverkansnämnden

Svar på revisionsrapport - Granskning av IT- och informationssäkerhet inom samverkansnämnden

SMN-2017/36

Förslag till beslut

Samverkansnämnden beslutar

att godkänna svaret till revisorerna

att anmäla svaret till kommunfullmäktige i Knivsta kommun

att skicka svaret till revisorerna.

Sammanfattning

Revisonsbyrån PWC har på uppdrag av revisorerna i Knivsta och Heby kommuner genomfört en översiktlig granskning av Samverkansnämndens arbete med IT- och informationssäkerhetsarbete. Granskningen har även gällt kommunernas informationssäkerhetsarbete på en övergripande nivå.

Bakgrund

Samverkansnämndens verksamhet hanterar driften av Knivsta och Hebys IT-resurser avseende teknisk infrastruktur, kommungemensamma systemresurser och klienter med tillhörande gemensamma programvaror. IT-enheten har också ansvaret för beställning och samverkan med kommunens olika leverantörer av driftstjänster. Ansvaret för kommunernas förvaltning av de verksamhetsspecifika informationsresurser ligger på respektive verksamhet.

Verksamheternas yttrande

Granskningen berör det övergripande informationssäkerhetsarbetet i Knivsta och Heby, vilket till stora delar ligger under KS i respektive kommun. Nämnden ansvarar för IT-enhetens arbete med informationssäkerhet. Därför har svaret kompletterats med en bilaga från kommunstyrelsens verksamhet i vardera kommun.

Knivsta kommun

Ekonomisk konsekvensanalys

Granskningen medför inga omedelbara kostnader för nämndens verksamhet. Dock kommer det åtgärder som behövers utifrån den nya Dataskyddslagen och övriga justeringar av svensk lagstiftning. Dessa är för att uppfylla EU:s nya dataskyddsförordning (GDPR).

Barnkonsekvensanalys
Barnkonsekvensanalys är gjord enligt checklista.

Åsa Franzén
Kanslichef

Lars-Erik Anderson
IT-chef

Knivsta kommun

Barnchecklista inför beslut

1. Påverkar beslutet barn?

Enligt FN är alla under 18 år att betrakta som barn

Ja **X** Nej ☐

Förklara oavsett svar.

Informationssäkerhet är viktigt för att många uppgifter som rör barn hanteras i kommuns olika system.

*Om, **ja fortsätt** med frågorna.*

2. Hur har barns bästa beaktats?

Samverkansnämnden har ställer höga krav på Informationssäkerhetsarbetet.

3. Beskriv eventuella intressekonflikter.

4. Barn tillfrågas vid övergripande flerårigа planer/styrdokument. Har så skett?

Ja ☐ Nej **X**

Inte aktuellt. Beslutet rör inte övergripande flerårig plan/flerårigt styrdokument **X**

Om ja, förklara på vilket sätt barn varit delaktiga i beslutet, vilka åsikter barnen lyft fram samt hur dessa åsikter beaktats i beslutet. Om nej, förklara varför barn inte tillfrågats.

Knivsta kommun

Samverkansnämnden	Datum	Diarienummer
Handläggare	2018-02-05	SMN-2017/36
Lars-Erik Andersson		

Svar på revisionsrapport del 1 - Granskning av IT- och informationssäkerhet inom samverkansnämnden

Bakgrund

Under perioden augusti till oktober 2017 har PwC på uppdrag av revisorerna i Knivsta och Heby kommuner genomfört en översiktlig granskning av Samverkansnämndens arbete med IT- och informationssäkerhet. Syftet har varit att granska om Samverkansnämnden på en övergripande nivå har ändamålsenliga rutiner och processer för att hantera IT- och informationssäkerhet.

1.1 Övergripande beskrivning av samverkansnämndens kontra kommunstyrelsens ansvar i de två kommunerna Knivsta och Heby

När det gäller informationssäkerheten i de i samverkansnämnden ingående kommunerna så delas ansvaret mellan dels samverkansnämnden, dels de två kommunerna. Vi får här definiera två olika huvudområden, det ena området, *informationssäkerhet* är respektive kommunstyrelses ansvar, det andra området, *informationsteknologi*, ofta förkortat ”it” är det i huvudsak samverkansnämndens ansvar. Man behöver även definiera det ansvarsområde där slutanvändarens ansvar för både ”it” och informationssäkerhet. Ett borttappat USB-minne är inte samverkansnämndens ansvar utan slutanvändaren på respektive förvaltning.

Informationssäkerhet är i huvudsak rutiner och beteenden hos våra medarbetare. En glömd Ipad eller en glömd väska med papper utgör en lika stor risk. Utöver detta har den mobilitet som växt fram under de senaste årtiondena och den vana(ovana) att hantera allt här och nu, gjort att vi har en tendens att glömma bort var vi är när det viktiga samtalet kommer till vår mobiltelefon.

Informationsteknologi, ”det som blinkar och lyser” enkelt uttryckt, är samverkansnämndens ansvar. I detta ligger ansvar för våra nätverk samt den serverinfrastruktur som nämnden förfogar över för att serva förvaltningarna. I ovanstående ingår även att se till att de klienter(datorer och Ipads) som idag nyttjas inom kommunerna har ett fullgott skydd mot intrång.
De båda kommunernas användare har inte fått en god utbildning i informationssäkerhet, något som även påpekas i rapporten. Både MSB, Myndigheten för skydd och beredskap samt PTS, Post- och telestyrelsen har utbildning och ger bra stöd för utbildning av användaren. En god

informationssäkerhet bygger på bra rutiner, medvetenhet om vilken information man hanterar och en struktur för informationsklassning.

1 Svar på revisionsfrågorna

2.1 Styrning av IT

Revisionsfråga 1:
Finns det en etablerad styrmodell för IT-verksamheten avseende IT-relaterade prioriteringar inklusive informationssäkerhet?

De båda kommunerna använder idag en modell kallad ”e-styr”. Denna behöver beskrivas tydligare och kompletteras samt informeras om i alla verksamheter så att den etableras. En it-strategi skall tas fram under 2018 samt en övergripande styrmodell för de båda kommunernas IT-verksamhet.

Styrmodellen ska:
- Utgå från de båda kommunernas långsiktiga strategiska mål
- Ta hänsyn till Samverkansnämndens mål och prioriteringar
- Beskriva hur IT kan bidra till att uppfylla kommunens mål
- Kompletteras med en handlingsplan med prioriterade aktiviteter
- Innehålla både egna och gemensamma prioriteringar
- Ta stöd och hämta ledning för Uppsala läns digitala strategi.

SMN och de två kommunernas definitioner:
- IT-strategi = det som blinkar och lyser, hanterar tekniken, tillhör SMN.
- E-strategi = e-tjänster, intranät, kommunikation, tillhör KS
- Digital strategi = leverans till invånarna, ex resfria möten, trygghetskamera i vården, IKT-arbetet i skolan. Tillhör e-styr i respektive kommun.

Styrmodellen beskriver relationerna mellan ovanstående samt ansvar. Styrmodellen ska vara klar under 2018.

Ansvarig: IT-chef

Beslutas av: KS

Ägs av: IT-chef och administrativ chef i respektive kommun

Informeras innan beslut: Centrala e-Styr

2.2 Styrande dokument

Revisionsfråga 2:
Finns beslutade styrande dokument (t.ex. IT-strategi, IT-policy, IT/informationssäkerhetspolicy samt kontinuitetsplan kopplat till informationssäkerhet? Är dessa kommunicerade?)

De styrdokument som idag finns inom IT-området är inaktuella och IT-strategi samt IT-policy och underliggande styrdokument inklusive kontinuitetsplan ska tas fram under 2018.

Ansvarig: IT-chef

Beslutas av: SMN

Ägs av: IT-chef

Delges: *e-styr och chefer*

2.3 Informationssäkerhet

Revisionsfråga 3:
Har informationssäkerhetsarbetet organiserats på ett ändamålsenligt sätt?

Besvaras av respektive kommuns informationssäkerhetsansvarig.

Ansvarig: Administrativ chef

Beslutas av: KS

Ägs av: informations-säkerhetsansvarig

Informeras innan beslut: e-styr

Delges: alla anställda

Revisionsfråga 4:
Kontrolleras efterlevnaden av riktlinjer för informationssäkerhet?

Besvaras av respektive kommuns informationssäkerhetsansvarig.

Ansvarig: Informations-säkerhetsansvarig

Beslutas av: e-styr

Ägs av: Förvaltningschefer

Revisionsfråga 5:
Sker informationsklassning enligt en systematisk metod?

Besvaras av respektive kommuns informationssäkerhetsansvarig.

Ansvarig: Informations-säkerhetsansvarig

Beslutas av: e-styr

Ägs av: Administrativ chef

Delges: Alla anställda

Revisionsfråga 6:
Sker utbildning av medarbetare i IT-och informationssäkerhet?

Besvaras av respektive kommuns informationssäkerhetsansvarig.

Ansvarig: Informations-säkerhetsansvarig

Beslutas av: e-styr

Ägs av: förvaltningschefer

Delges: alla anställda

Revisionsfråga 7:
Beaktas IT-och informationssäkerhetsrelaterade aspekter vid upphandling/anskaffning av system och applikationer?

Besvaras av respektive kommuns informationssäkerhetsansvarig.

Ansvarig: Upphandlings-ansvarig

Beslutas av: e-styr

Ägs av: Ekonomichef

Information innan upphandling: e-styr

2.4 IT-processer

Revisionsfråga 8:
Finns det rutiner för rapportering och hantering av säkerhetsbrister och incidenter kopplade till IT och informationssäkerhet?

IT säkerhet (teknisk plattform) ingår som en del i begreppet Informationssäkerhet (systemsäkerhet). Säkerhetsbrister och incidenter (kritiska och hög prioritering) kopplade till den tekniska plattformen hanteras efter gängse ITIL processer som är verifierade mellan SMN och driftleverantören Advania. ”SMN – Ärende- och Incidentprocess” är en process- och rutinhandbok där incidentprocessen beskrivs och hur den hanteras. I detta dokument beskrivs hur incidentprocessen med kritisk- och hög prioritering sköts och hur eskaleringen hanteras. Uppföljning sker varje månad med genomgång av föregående månads incidenter, samt beslut om eventuella ytterligare åtgärder och uppföljning.
Systemsäkerhet hanteras inom förvaltningsorganisation för respektive system, som används av respektive verksamheter. Där ingår informationsklassning, tillgänglighet och riktighet samt accesshantering. Till hjälp för detta arbete finns SKLs verktyg KLASSA där systemansvariga utifrån givna mallar kan säkerhetsklassa sina respektive system. Systemet skapar också en åtgärdslista samt rekommendationer utifrån givna svar från systemanalysen.

Ansvarig: IT-driftchef

Beslutas av: IT-Chef

Ägs av: Samverkansnämnden

Delges: Systemansvariga

2.5 IT-säkerhet

Revisionsfråga 9: Har risk-och systemsäkerhetsanalyser genomförts för verksamhetskritiska system?

Besvaras av respektive kommuns informationssäkerhetsansvarig.

Ansvarig: Informations-säkerhetsansvarig

Beslutas av: e-styr

Äga av: Informations-säkerhetsansvarig

Revisionsfråga 10: Är åtkomstskydd till kritiska system och applikationer lämpligt utformade? Genomförs periodisk granskning av tilldelade behörigheter?

Besvaras av respektive kommuns informationssäkerhetsansvarig.

Ansvarig: Systemansvarig

Beslutas av: förvaltningschef

Ägs av: Systemägare

Delges: alla anställda

2.6 IT-drift

Revisionsfråga 11: Är IT-infrastrukturen uppbyggd enligt god praxis och skapar den förutsättningar för ett kvalitativt och säkert IT-stöd?

Samverkansnämnden kommer att ta fram en handlingsplan för att hantera samtliga frågor inom detta område. Det saknas idag fullständiga kontinuitetsplaner, disaster recovery-planer backup, m.m. Frågan behöver i vissa områden även hanteras tillsammans med den externa it-partnern Advania. Advanias kompetenser förbisågs tyvärr i rapporten då nämnden under hösten var i övergång från den tidigare leverantören Axians.Inom denna handlingsplan ska även en process för genomförande av återkommande riskanalyser och penetrationstester finnas med. Handlingsplan samt underliggande styrdokument ska tas fram under 2018.

Ansvarig: IT-chef

Beslutas av: SMN

Ägs av: IT-chef

Delges: Informations-säkerhetsansvarig

Knivsta kommun

Samverkansnämnden	Datum	Bilaga
Handläggare	2018-02-01	2017/36
Anders Fredriksson		

Svar på revisionsrapport del 2 - Granskning av IT- och informationssäkerhet inom samverkansnämnden

Bakgrund

Knivsta kommun har mottagit PwC:s granskning av IT och informationssäkerheten i samverkansnämndens arbete. Det är viktigt att arbetet med informationssäkerheten granskas av en oberoende part för att upptäcka brister i detta viktiga arbete.
Informationssäkerhetsarbetet är ett ansvar för respektive kommun och regleras av ett antal lagar och föreskrifter.
Samverkansnämnden ansvarar för att hantera kommunernas informationsresurser i enlighet med lagar, föreskrifter och kommunernas verksamhets riktlinjer. Nämndens verksamhet kan även stödja förvaltningen i informationssäkerhetsarbete och ansvarar för att kontrollera att kommunens driftsleverantörer följer gällande avtal och instruktioner.

Kommentarer till PWC:s rekommendationer

1. Kommunens styr och ledningssystem ska leda till ett tydligt underlag för Samverkansnämndens planering av verksamheten och resultera i en årlig plan för hur nämndens verksamhet ska utformas. Den ska inkluderas i kommunens årshjul och finnas med i dialog och beslutsprocesserna mellan politik och verksamhet. IT-strategiska beslut ska beredas i dialog mellan kommunens verksamheter och dokumenteras i en IT-strategi och beslutas i respektive kommunstyrelse och samverkansnämnden.
   1.1. Handlingsplan för genomförandet tas fram av Samverkansnämndens verksamhet och bereds i respektive kommuns e-styr. Planen tas fram under 2018.
   1.2. Handlingsplanen beslutas av Samverkansnämnden

2. Styrdokument för säkerhetsarbetet ska hanteras av en informationssäkerhetspolicy med underliggande riktlinjer för informationssäkerhet. Under dessa ska finas rutiner och anvisningar för kontinuitetshantering för respektive verksamheter inklusive IT-enheten. Rutiner för incidenthantering tas fram, i samklang med Process och rutinhandbok, av IT-enheten. Respektive verksamhets handledningar gällande användande av aktuella informationsresurser tas fram i samverkan mellan IT-enheten och verksamhet. Övergripande anvisningar gällande kommungemensamma informationsresurser tas fram av IT-enheten i samverkan med kommunens verksamhet. Se vidare under delfråga 1.
   2.1. Kontinuitetsplanering/omfallshantering ska ske i samtliga av kommunernas verksamheter utifrån resultat i risk och sårbarhetsarbetet. IT-enheten ska ge övriga verksamheter underlag för olika scenarier och hur länge dessa kan pågå och även själva arbeta med planering för att minimera skadorna på kommunens förmåga. Beslutas av e-styr under 2018.
   2.2. Informationssäkerhetspolicy finns beslutad av kommunfullmäktige och riktlinjer för informationssäkerhet av kommunledningen/e-styr ska beslutas under våren 2018. Underliggande anvisningar och instruktioner tas fram av berörd verksamhet och

beslutas av respektive berörd verksamhetschef och kommuniceras till e-styr och samverkansnämnden.

3. IT och informationssäkerhetsarbetet leds av Informationssäkerhetsamordnare i samverkan med e-styr och regleras av Riktlinjer informationssäkerhet.
   3.1. Plan för årliga arbetet upprättas av informationssäkerhetsansvarig i samverkan med säkerhetssamordnare och e-styr. Planen ska vara klar under våren 2018.
   3.2. Roller och ansvar regleras i Riktlinjer informationssäkerhet och där ingår även Dataskyddsombudet. En projektledare för GDPR arbetet är anställd i februari och tjänsten övergår i dataskyddsombud på 60% . Detta är en kombinationstjänst dataskyddsombud/kommunjurist.
   3.3. En projektgrupp arbetar med frågan och flera arbetsgrupper har startats. Processen för tilldelning av informationsägarskapet är inte förändrad sedan tidigare styrdokument och följer linjeorganisationen och dokumenteras i styrkorten för respektive verksamhetssystem.
   3.4. Kommunen planerar både övningar gemensamt i länet och i kommunen. Denna planering utförs av säkerhetssamordnare och kommunledning. Regleringen av incidenthanteringen kommer att finnas i Anvisning incidenthantering.

4. Rutiner för kontroll av efterlevnad av riktlinjer och anvisningar ska fram av informationssäkerhetssamordnare och beslutas av e-styr under 2018. Detta ska ske dels genom egenkontroll av respektive chef men även genom regelbundet slummässiga stickprovskontroller. Ansvaret är kontorscheferna och resultatet delges e-styr.

5. System och informationsklassning är grunden för kravställning för hur kommunernas informationsresurser hanteras. Detta viktiga arbete har Knivsta kommun valt att genomföra med stöd av SKL:s verktyg Klassa. Ansvaret för genomförandet ligger på verksamheterna med stöd av Informationssäkerhetssamordnare och verksamhetsutvecklare. Det gäller även Samverkansnämndens verksamhet och systemresurser. Ansvaret för genomförande och redovisning av planerade och utförda åtgärder ligger på systemägare och ska redovisas för ansvarig nämnd eller kommunstyrelse under 2018.

6. Plan för Utbildning av samtliga medarbetare och chefer avseende informationssäkerhet ska tas fram under våren.
   6.1. Ansvaret för medarbetarnas kompetens ligger på respektive chef. Utbildning av chefer sker i Knivsta inom ramen för chefskörkortet. Stöd för cheferna ska tas fram av Informationssäkerhetssamordnare och verksamhetsutvecklare i samverkan med HR-enheten under 2018.
   6.2. Utbildning avseende GDPR har genomförts till alla chefer, alla som sitter i e-styr samt ett extra tillfälle till ledningsgruppen. Dessutom har alla politiker erbjudits en utbildning som även spelats in. Projektgruppen samt arbetsgrupperna inom arbetet med GDPR har fått specifika utbildningar. Därtill kommer filmer och information tas fram för att spridas och finnas tillgängligt på intranätet. +

7. Att informationssäkerhetsaspekter beaktas vid upphandling.

7.1. I Knivsta är det verksamhetschefen som gör beställning av varor/tjänster och förväntas använda tecknade ramavtal (exempelvis från kammarkollegiet). När en upphandling görs utanför kammarkollegiets ramavtal ska aspekter som säkerhet tas med. I riktlinjerna som är generella kan vi bara beröra generell nationell säkerhet som gäller alla typer av upphandlingar av varor och tjänster. Upphandlingsolicyn är aktuell och inte nödvändig att uppdatera, de generella riktlinjerna är under uppdatering och planeras antas till KS under våren. I anvisningarna för systemförvaltning finns rutiner för vad som ska tas med för generella krav på informationssäkerhet och det rekommenderas att använda Klassa för att få fram specifika krav utifrån den information som behandlas.

7.2. I befintliga styrdokument är IT-enheten obligatorisk samverkanspart vid upphandling av IT-relaterade produkter och tjänster och där föreslås ingen ändring i kommande anvisning.

8. Hanteringen av incidenter som är IT-relaterade spänner från tekniska felmeddelanden till massiva angrepp av utomstående part.

8.1. Det är en Anvisning för incidenthantering under framtagande och den ska styra hur de ska hanteras och vilka åtgärder som ska vidtas och därmed vilken information som ska ges berörda och aktuell myndighet. Den ska självklart vara likartad mellan ingående kommuner i samverkan. Den tas fram med utgångspunkt från driftshandboken mellan IT-enheten och driftsleverantör. Den beslutas av e-styr och sprids via linjeorganisationen. Den planeras antas under våren 2018.

9. Ett arbete med att genomföra Risk och sårbarhetsanalyser ska genomföras i samverkan med kommunens samtliga verksamheter i enlighet med MSB:s rekommendationer, gällande samtliga hot och risker som har påverkan på kommunens förmåga. Det sker med stöd av säkerhetssamordnare och informationssäkerhetsamordnare. Resultaten ska analyseras och GAP-analys genomföras och ska vara ett underlag för verksamheternas kontinuitetsplanering. Samverkansnämndens verksamhet ska ge övriga verksamheter underlag för olika scenarier och hur länge dessa kan pågå och även själva arbeta med planering för att minimera skadorna på kommunens förmåga.

9.1. Hot och riskanalys ska även göras i samband med inköp eller större förändring av verkssamhetssystem eller teknisk plattform. I enlighet med anvisning systemförvaltning.

9.2. Förvaltningen av verkssamhetssystem ska ske i enlighet med leverantörens och IT-enhetens rekommendationer. Detta ska dokumenteras i respektive systemkort och i driftsdokumentationen. Ansvaret är respektive systemägare.

10. Åtkomstskyddet för samtliga applikationer ska vara utifrån informationens värde och känslighet. Det sker en tydlig kravställning i dessa frågor när Klassa används.

10.1. Processer för behörighetstilldelning ska finnas i systemförvaltningsplaner och dessa ska finnas i systemkorten. I aktuella fall ska rutinerna finnas i driftsinstruktionerna för kommunens driftsleverantörer. Samtlig behörighetshantering för verksamhetssystem ska skötas av verksamheternas systemansvariga och inte vara ett ansvar för samverkansnämnden.

10.2. I anvisning om informationssäkerhet för användare finns ett eget kapitel om användarkonto och behörigheter. Där beskrivs upplägg, avslut och förändring av tjänst.
Beslutas av Administrativ chef och ägs av informationssäkerhetsamordnare.

Datum
26 januari 2018

Diarienr/Dplankod

Central förvaltning
Karin Eljansbo
Administrativ chef
0224-36113

Tjänsteskrivelse avseende granskningsrapport om informationssäkerhet, Pwc.

Under perioden augusti till oktober 2017 har PwC på uppdrag av revisorerna i Knivsta och Heby kommuner genomfört en översiktlig granskning av arbetet med IT-och informationssäkerhet. Granskningen omfattar samverkansnämndens och kommunstyrelsernas ansvarsområden.

Granskningen har översiktligt fokuserat på; styrning och ledning av IT-och informationssäkerhet, samt rutiner, processer, uppföljning, samt personalaspekter såsom kompetens och bredd. Syftet med granskningen är att klargöra vilka eventuella områden som samverkansnämnden behöver utveckla för att uppnå ändamålsenliga rutiner och processer för att hantera IT-och informationssäkerhet på ett för kommunen lämpligt sätt. Då ansvaret för informationssäkerheten ligger på respektive kommun klargör även granskningen vilka områden som respektive kommunstyrelse i Heby Kommun och Knivsta kommun behöver utveckla. Av rapporten framkommer att det krävs ett antal åtgärder för att säkerställa en god informationssäkerhet varav några bedöms behöva verkställas snarast.

Rapporten är indelad i elva delområden.

1. Styrning av IT
2. Styrande dokument
3. Informationssäkerhet (3-7)
8. IT-processer
9. IT-säkerhet (9-10)
11. IT-drift

Nedan följer en beskrivning av de åtgärder Heby kommun behöver vidta för att säkerställa god informationssäkerhet.

Styrning av IT

1. Finns det en etablerad styrmodell för IT-verksamheten avseende IT-relaterade prioriteringar inklusive informationssäkerhet?

Observation från PwC	Heby kommuns kommentarer/åtgärder
Det finns inte någon ”tydligt etablerad” styrmodell för IT-verksamheten. Det som finns i dagsläget är generella mål för IT.	Kommunens styrning och ledningssystem ska leda till ett tydligt underlag för Samverkansnämndens planering av verksamheten och resultera i en årlig strategi för hur nämndens verksamhet ska utformas. Den ska finnas med i dialog och beslutsprocesserna mellan politik och verksamhet. IT-strategiska beslut ska beredas i dialog mellan kommunens verksamheter och dokumenteras i en IT-strategi och beslutas i respektive kommunstyrelse och samverkansnämnden. Handlingsplan för genomförandet tas fram av Samverkansnämndens verksamhet och bereds i respektive kommuns e-styr.

Styrande dokument

2. Finns beslutade styrande dokument?

Observation från PwC	Heby kommuns kommentarer/åtgärder
Det saknas aktuell informationssäkerhetspolicy	• Anvisning om informationssäkerhet, både för användare och för mobila enheter, är antagen av administrativ chef den 9 oktober 2017 • Alla chefer är informerade via e-post • Egen sida på intranätet är skapad för informationssäkerhet med hänvisning till antagna anvisningar • En Datorstödd Informationssäkerhetsutbildning för användare finns på intranätet och är obligatorisk för alla medarbetare Mer övergripande styrdokument såsom policy och riktlinjer för informationssäkerhet och övrig säkerhet saknas. Det saknas även policy för dataskyddsarbete som enligt GDPR, ska finnas på plats senast maj 2018. Dessa dokument behöver tas fram snarast.
Det saknas en övergripande kontinuitetsplan för kommunens verksamheter.	Heby kommun behöver ta fram rutiner och anvisningar för kontinuitetshantering för alla IT- system i alla verksamheter, dvs. en plan för hur verksamheten agerar om ett IT-system går ner eller vi har ett driftsstopp. Det krävs också en prioriteringsordning av alla IT-system i hela kommunen, vilka IT-system som prioriteras först vid uppstart, prioriteringsordningen beslutas av centralt E-styr. Dessa planer ska tas fram i samråd med IT, men ansvaret ligger på verksamheterna i kommunen. Dessa planer och prioriteringar ska kontinuerligt hållas uppdaterade.

Informationssäkerhet

3. Har informationssäkerhetsarbetet organiserats på ett ändamålsenligt sätt?

Observation från PwC	Heby kommuns kommentarer/åtgärder
Det saknas dokumenterade roll- och ansvarsbeskrivningar relaterat till informationssäkerhetsarbetet. Även rollen för att leda arbetet med att anpassa respektive verksamhet till GDPR ska finnas med.	Kommunen behöver ta fram en tydlig roll- och ansvarsbeskrivning och förankra den väl i verksamheterna. Följande roller är aktuella: **Systemägare:** Förvaltningschef ytterst ansvarig för förvaltningens IT-system, förvaltningens representant i E-styr. **Systemförvaltare**: Den chef som har det övergripande ansvaret för systemet, budget för inköp och kontinuerliga uppdateringar, upphandling mm, **Systemansvarig**: Den person i verksamheten som har det praktiska ansvaret för systemet, kontakt med leverantör, IT-enheten och övriga användare. **Datasamordnare**: central funktion som samordnar det centrala arbetet med systemansvariga och kontakt med IT, Samordnar kommunövergripande IT-aktiviteter och verksamhetsutveckling. Samverkar med dataskyddsombud och informationssäkerhetsansvarig. **Informationssäkerhetsansvarig**: Planerar och genomför återkommande kris- och katastrofövningar kopplade till informationssäkerhet och integritet, Samordna arbetet med att ta fram kontinuitetsplaner för samtliga IT- system i kommunen. Kontaktperson vid haverier, intrång, kontakta med datainspektionen, dataskyddsombud, polismyndighet m.fl. Ta fram en strukturerad plan som säkerställer medarbetarnas efterlevnad av policy, riktlinjer, anvisningar och instruktioner. Ta fram en strukturerad plan för hur arbetet gällande informationsklassning ska genomföras. Planen ska • Innehålla tydlig beskrivning av målen • Beskriva hur målen ska uppfyllas inom respektive förvaltning • Föreslå att använda SKL:s metod, KLASSA **Dataskyddsombud:** Från och med maj 2018 måste kommunen ha ett dataskyddsombud . Namn och kontaktuppgifter ska anmälas till Datainspektionen senast maj 2018. Dataskyddsombudet ska gå datainspektionens 6-dagars utbildning. Då rollen är ny behöver en organisation kring dataskyddsombudet göras. SKL gör bedömning att det arbete som dataskyddsombudet ansvarar för motsvara ca 50% tjänstgöringsgrad och att det är fördel om det finns juridiks kompentens. Ett dataskyddsombud har enligt lagstiftningen följande arbetsuppgifter: • Informera och ge råd till personuppgiftsansvarig eller personuppgiftsbiträde. • Övervaka efterlevnaden av förordningen • Riskbedömningar

Observation från PwC	Heby kommuns kommentarer/åtgärder
	• Ge råd gällande konsekvensbedömning avseende dataskydd. • Samarbeta med Datainspektionen • Fungera som kontaktpunkt för Datainspektionen. • Utbilda nya medarbetare och samordna årlig återkommande utbildning i dataskydd i kommunen. • Rapportera incidenter till Datainspektionen. • Samordna den årliga inventeringen/uppdateringen av system i kommunen.
	En datasamordnare är anställd för att leda arbetet med anpassningar till GDPR. Fram till 2019 är arbetet omfattande på ca 75%. Resterande 25 % utgörs av ett samordningsarbete för förvaltningsövergripande IT frågor ur ett verksamhetsperspektiv samt organisera och samordna kommunens systemansvariga. Vara delaktigt i arbetet med säkerhetsklassning av system. Sekreterare i E-styr. Samordnare för införande av E-tjänster i kommunen.
Det saknas process för identifiering/tilldelning av informationsägarskap.	En process för identifiering och tilldelning av informationsägarskap ska tas fram. Systemförvaltare, systemägare och systemansvariga är roller som inte finns idag och som är nödvändiga att utse för varje system för att sedan kunna arbeta med säkerhetsklassning. Detta arbete skulle kunna ledas av informationssäkerhetsansvarig i samverkan med datasamordnaren. Detta arbete bör påbörjas snarast.
Det råder brist i samarbetet och kommunikationen mellan verksamheten och IT.	I dagsläget finns lokala e-styrsmöten där verksamheterna och IT träffas och diskuterar IT-relaterade utvecklingsfrågor som förvaltningen har. Det finns även ett centralt e-styr, kommunchefens ledningsgrupp bestående av förvaltningschefer, IT-chef, administrativ chef, ekonomichef, personalchef och kvalitetsstrateg. Där tas strategiska IT och e-frågor upp som berör hela kommunen. En tydlig roll och ansvarsbeskrivning för lokala och centrala e-styr behöver tas fram och vår IT-leverantör Advania behöver delta på dessa möten.
Det saknas tydliga och uppdaterade kontinuitetsplaner kopplade till informationssäkerhets-incidenter.	Informationssäkerhetsvarig behöver utses som jobbar med dessa frågor. Planerar och genomför återkommande kris- och katastrofövningar kopplade till informationssäkerhet och integritet,

4. Kontrolleras efterlevnaden av riktlinjer för informationssäkerhet?

Observation från PwC	Heby kommuns kommentarer/åtgärder
Det inte finns några etablerade rutiner, strukturerade processer eller kontroller avseende uppföljning av medarbetarnas efterlevnad av riktlinjer inom IT- och informationssäkerhet eller övriga IT-relaterade styrdokument.	Ta fram en strukturerad plan som säkerställer medarbetarnas efterlevnad av policy, riktlinjer, anvisningar och instruktioner. Planen ska rapportera efterlevnaden till e-styr och lyftas i medarbetarenkäten, Ansvarig: informationssäkerhetsansvarig.

5. Sker informationsklassning enligt en systematisk metod?

Observation från PwC	Heby kommuns kommentarer/åtgärder
I Heby kommun har arbetet med informationsklassning inte påbörjats i någon större omfattning. Arbetet med informationsklassning behöver skyndsamt påbörjas utifrån GDPR.	Ta fram en strukturerad plan för hur arbetet gällande informationsklassning ska genomföras, Informationssäkerhetsansvarig i samverkan med datasamordnare och systemägare. Planen ska • Innehålla tydlig beskrivning av målen • Beskriva hur målen ska uppfyllas inom respektive förvaltning • Föreslå att använda SKL:s metod, KLASSA Detta arbete förutsätter att roller och ansvar för systemen är klara. Detta arbete bör påbörjas snarast.

6. Sker utbildning av medarbetare i IT- och informationssäkerhet?

Observation från PwC	Heby kommuns kommentarer/åtgärder
Det saknas en fastställd utbildningsplan för utbildning inom IT och informationssäkerhet	Ta fram och förankra en utbildningsplan inom IT- och informationssäkerhet. Digital utbildning om informationssäkerhet finns i dag men behöver kompletteras med utbildning i kontinuitetsplaner. Det bör finnas utbildningsplaner för alla medarbetare, men även specifika för systemägare och systemansvariga. Utbildningsplanerna kan tas för informationssäkerhet tas fram av informationssäkerhetsansvarig. Övriga utbildningsplaner för användare av system tas fram av ansvarig chef.
Ingen medarbetare i Heby kommun genomgår någon utbildning avseende IT- och/eller informationssäkerhet	Det finns en sida på intranätet som handlar om informationssäkerhet. Där finns även DISA-utbildning samt länk till anvisningar kring informationssäkerhet. Utbildningen är obligatorisk för alla medarbetare. Utbildning kring informationssäkerhet och GDPR kan slås ihop. Ansvarig för genomförande av utbildning är närmaste chef.

Observation från PwC	Heby kommuns kommentarer/åtgärder
Skyndsamt säkerställa att utbildning kring GDPR genomförs.	Utbildning kring GDPR finns med i projektet ”Projekt för att följa EU:s nya dataskyddsförordning”. Målet är att alla medarbetare ska ha tillgång till utbildning innan 25 maj 2018. Ansvarig för genomförande av utbildning är närmaste chef.

7. Beaktas IT- och informationssäkerhetsrelaterade aspekter vid upphandling/anskaffning av system och applikationer?

Observation från PwC	Heby kommuns kommentarer/åtgärder
Vid upphandling används inte alltid Kammarkollegiets ramavtal vilket leder till att informationssäkerhetsrelaterade aspekter inte beaktas.	Att upphandling av kritiska system/applikationer/tjänster, ska ske i enlighet med de utökade kraven på informationssäkerhet och införandet av GDPR. Att göra • Uppdatera befintliga policy, riktlinjer, anvisningar och instruktioner • Förtydliga att Kammarkollegiets ramavtal ska användas för informationssäkerhetsrelaterade aspekter • I samband med upphandling ska KLASSA användas • Hänsyns ska tas till informationssäkerhet och GDPR vid upphandling av kritiska system/applikationer/tjänster Ansvarig för detta är upphandlingsansvarig i samråd med dataskyddsombud.
Respektive förvaltningschef är i dagsläget ansvarig för upphandling av verksamhetssystem.	• IT måste rådfrågas i tekniska frågor • Informationssäkerhetsansvarig ska även vara rådgivande vid upphandling. • Innan upphandling påbörjas ska ärendet hanterats av e-styr

IT-processer

8. Finns det rutiner för rapportering och hantering av säkerhetsbrister och incidenter kopplade till IT och informationssäkerhet?

Observation från PwC	Heby kommuns kommentarer/åtgärder
Ändrings-, incident, och problemhantering avseende verksamhetskritiska IT-system och applikationer är utlagd på extern leverantör.	Advania sköter driften av IT för Heby kommun.
Det saknas generella rutiner för rapportering och hantering av säkerhetsbrister och incidenter kopplade till IT- och informationssäkerhet.	Rutiner för rapportering och hantering av säkerhetsbrister och incidenter behöver snarast tas fram upprättas och förankras i kommunen. Rutinen ska • Tydliggöra rapportering av IT-incidenter och säkerhetsbrister • Beskriva skillnaden mellan en IT-incident och en säkerhetsbrist • Tydliggöra ansvarsfördelning för hantering av IT-incidenter och säkerhetsbrister • Uppdatera anvisning om informationssäkerhet för användare • Tas fram skyndsamt • Informera systemägare, systemförvaltare och systemansvariga om ny rutin • Här bör vi använda samma rutiner som Knivsta kommun eftersom vi har gemensam IT-enheten. Ansvarig roll: Informationssäkerhetsansvarig.

IT-säkerhet

9. Har risk- och systemsäkerhetsanalyser genomförts för verksamhetskritiska system?

Observation från PwC	Heby kommuns kommentarer/åtgärder
I Heby kommun genomförs inte regelbundna riskanalyser avseende IT- och informationssäkerhet. Det saknas strukturerade processer och rutiner för arbetet med riskanalyser	Ta fram tydlig process och rutin för att säkerställa att risk- och systemsäkerhetsanalyser genomförs, Processen och rutinen ska • Synliggöra ansvar • Övergripande visa hur en analys genomförs • Resultera i en systemsäkerhetsplan • Kontroll av efterlevnad bör ske årsvis Ansvarig roll: informationssäkerhetsansvarig i samarbetet med systemansvarig.
	Systemförvaltare ska inom sin verksamhet ta fram en strukturerad plan för vilka system och applikationer som ska uppdateras och med vilka tidsintervall, detta måste se i samråd med IT-enheten och It samordnaren. Planen ska

Observation från PwC	Heby kommuns kommentarer/åtgärder
	• Innehålla alla system och applikationer • Ange med vilka tidsintervall uppdateringar sker • Innehålla rutin för information till berörda • Innehålla rutin för test innan uppdatering, uppdatering och verifiering efter uppdatering
Uppdateringar av vissa verksamhetskritiska system har varit bristfällig under de senaste åren.	

10. Är åtkomstskydd till kritiska system och applikationer lämpligt utformade? Genomförs periodisk granskning av tilldelade behörigheter?

Observation från PwC	Heby kommuns kommentarer/åtgärder
Det genomförs inga strukturerade kontroller huruvida medarbetares behörigheter genomförs i enlighet med uppsatta rutiner eller inte.	Befintlig anvisning om informationssäkerhet för användare, kapitel användarkonto och behörigheter, behöver kompletteras med information om kontroll av efterlevnad. Ansvariga roller: Informationssäkerhetsansvarig,
Det saknas dokumenterade riktlinjer, anvisningar eller instruktioner kopplade till behörighetskontroll.	I anvisning om informationssäkerhet för användare finns ett eget kapitel om användarkonto och behörigheter. Där beskrivs upplägg, avslut och förändring av tjänst. Behöver kompletteras om hur och när kontroller ska genomföra och ansvarsroller.
Vid internt byte av tjänst eller avslut av tjänst upplevs behörighetskontrollen i vissa situationer som bristfällig.	I anvisning om informationssäkerhet för användare finns ett eget kapitel om användarkonto och behörigheter. Där beskrivs upplägg, avslut och förändring av tjänst. Ta fram rutin för behörighetskontroll Rutinen ska • Beskriva stegvis hur ny behörighet ges • Beskriva stegvis hur behörighet tas bort vid avslut av tjänst eller byte av arbetsuppgifter • Ange vem som är ansvarig för vad • Innehålla både verksamhetssystem, molntjänster och basprogram (Officepaketet, Internet Explorer)

IT-drift

11. Är IT-infrastrukturen uppbyggd enligt god praxis och skapar den förutsättningar för ett kvalitativt och säkert IT-stöd?

Observation från PwC	Heby kommuns kommentarer/åtgärder
Det har inte genomförts några återkommande riskanalyser som grund för nätverkets säkerhetsnivå eller några penetrationstester.	IT-chefens ansvarsområde.
Det har inte genomförts några planerade tester av leverantörens förmåga avseende backup- och återställning av data.	IT-chefens ansvarsområde.

Sammanfattning:

Digitaliseringen är både en utmaning och en möjlighet för kommunen. Digitala tjänster och lösningar ger stora möjligheter till ökade tillgänglighet av kommunens service till medborgarna, speciellt för en kommun som Heby som har en stor geografisk yta. Digitaliseringen ger oss också en möjlighet att på sikt effektivisera våra verksamheter. Utmaningen ligger i själva genomförandet och kraven kring GDPR, informationssäkerhet och IT-säkerhet. Av rapporten framkommer att det krävs ett omfattande grundarbete inom informationssäkerhet, IT-säkerhet och dataskydd för att vi ska kunna påbörja någon digitaliseringsresa.

Vi har idag gemensam samverkansnämnd med Knivsta kommun med tillhörande IT-enheten som ska serva båda kommunerna gällande drift och IT-säkerhet. Gällande dataskydd (GDPR), verksamhetssystem och informationssäkerhet ligger ansvaret på respektive kommuner.
Den centrala resursen som Heby kommun i dagsläget har är en heltidsanställd datasamordnare, som just nu arbetar med samordningen av kommunens anpassning till GDPR, arbetet är omfattande och prioriterat fram till december 2018. Det mest prioriterade gällande GDPR förutom det intensiva och resurskrävande anpassningsarbetet som pågår är att vi måste ha ett dataskyddsombud helst med juristkunskap som aktivt arbetar de brister som framkommer i rapporten och det kommande dataskyddsarbetet som lagen kräver. Lagen kräver att kommunen har utsett dataskyddsombud senast 25 maj 2018. Det framgår även att dataskyddsombudet inte får granska sitt eget arbete eller ha en chefsroll.

Det omfattande arbetet med informationssäkerhet, GDPR och IT-säkerhet är en förutsättning för digitalisering, effektivisering och utvecklingen i kommunen som främjar tillväxt, Vi är idag helt beroende av att vår IT-miljö, IT-säkerhet och informationssäkerhet fungerar. Heby kommun har idag inga centrala resurser till att genomföra nödvändigt arbete inom informationssäkerhet och dataskydd. För att kunna leva upp till de lagstadgade kraven på dataskydd (GDPR) samt informationssäkerhetsarbetet bedömer förvaltningen att följande resurser behöver tillsättas:

I**nformationssäkerhetsansvarig/ dataskyddsombud 100%**
Informationssäkerhetsansvarig/dataskyddsombud. Arbeta som dataskyddsombud med anvisningar och rutiner, utbildningar, anmälningar till datainspektionen mm. uppdatera registerförteckningar. Systemansvarig för Draftit. Arbeta med informationssäkerhet, incidenter, revision mm. samt jobba med revisionsrapporten.

Karin Eljansbo
Administrativ chef

Till Kommunfullmäktige i Knivsta kommun

25 oktober 2017

Revisionsrapport, Granskning av IT- och informationssäkerhet inom Samverkansnämnden

I egenskap av förtroendevalda revisorer i Knivsta kommun har vi granskat Samverkansnämnden Knivsta/Heby arbete med IT- och informationssäkerhet. Den övergripande revisionsfrågan är om Samverkansnämnden på en övergripande nivå har ändamålsenliga rutiner och processer för att hantera IT- och informationssäkerhet. I granskningen har vi biträtts av sakkunniga från PwC.

Vår övergripande bedömning är att arbetet kring IT- och informationssäkerhet till viss del uppfyller revisionsfrågans innebörd. Arbete inom informationssäkerhet har påbörjats och medvetenhet om vikten av detta är hög inom ledningen hos både Knivsta och Heby kommun. Det krävs ett antal åtgärder för att säkerställa en god informationssäkerhet varav några behöver verkställas snarast.

- System- och informationsklassning har påbörjats i Knivsta men ej i Heby. Ur informationssäkerhetssynpunkt måste detta finnas på plats för att möjliggöra rätt nivå av säkerhet och skydd av känslig information, speciellt i ljuset av kommande dataskyddsförordning (GDPR), är det av vikt att detta arbete prioriteras och slutförs.

- Det saknas återkommande risk- och sårbarhetsbedömningar ur ett informationssäkerhetsperspektiv. Vi rekommenderar att samverkansnämnden etablerar en process för återkommande riskbedömningar för att möjliggöra upprättande av åtgärdsplaner för de prioriterade riskerna.

- Det saknas tydliga riktlinjer för hur man som medarbetare skall förhålla sig till informationssäkerhet och integritet och hur incidenter skall hanteras. Vi rekommenderar att samverkansnämnden snarast fastställer riktlinjer för informationssäkerhet och incidentrapportering samt en rutin för återkommande utbildning för samtlig personal.

- Det saknas processer för att säkerställa att medarbetare har rätt behörighetsnivå och därmed deras tillgång till skyddsvärd eller känslig information. Ansvaret för behörigheter ligger i dag på enhetscheferna. Vi rekommenderar att samverkansnämnden snarast inför en process för återkommande revision av behörigheter för att säkerställa att medarbetare som bytt tjänst inte har för hög behörighet och att medarbetare som lämnat sin tjänst också avslutas i systemen.

I rapporten lämnas även förslag på andra rekommendationer

Revisorerna överlämnar härmed granskningsrapporten för kännedom och yttrande. **Vi förväntar** oss att yttrandet innehåller en tidplan över vilka åtgärder som planeras att vidtas med anledning av de rekommendationer som lämnas i rapporten. Yttrande från Samverkansnämnden önskas senast den **15 december** 2017.

För Knivsta kommuns revisorer

Eva Enskär
Ordförande

Bilaga: Revisionsrapport "Granskning av IT-och informationssäkerhet inom Samverkansnämnden" PwC.

www.pwc.se

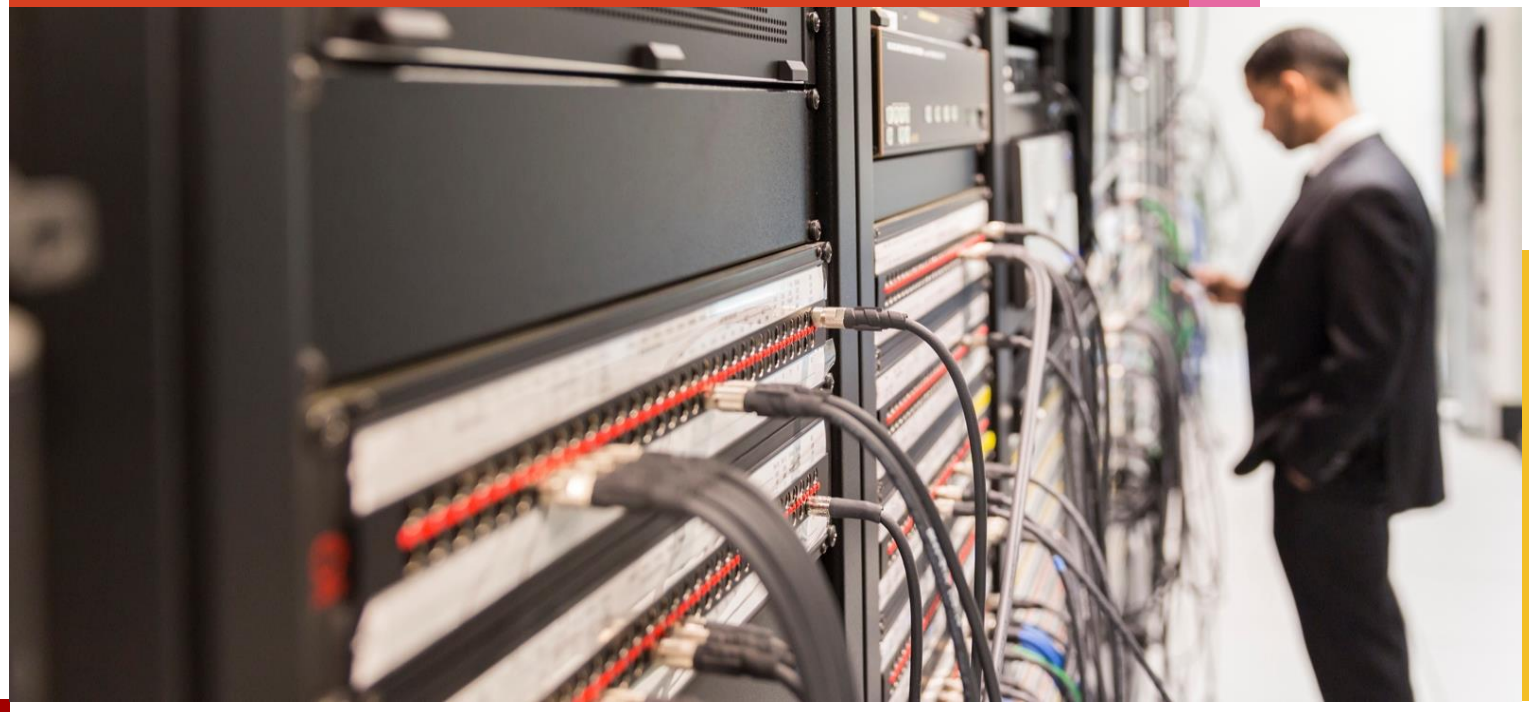
Knivsta och Heby kommun

Granskning av IT- och informations-säkerhet inom Samverkansnämnden Oktober 2017

Knivsta kommun

HEBY KOMMUN

10 oktober 2017



pwc

Innehåll

Sammanfattning

Under perioden augusti till oktober 2017 har PwC på uppdrag av revisorerna i Knivsta och Heby kommuner genomfört en översiktlig granskning av Samverkansnämndens arbete med IT- och informationssäkerhet. *Syftet har varit att granska om Samverkansnämnden på en övergripande nivå har ändamålsenliga rutiner och processer för att hantera IT- och informationssäkerhet.*

Vår övergripande bedömning är att arbetet kring informationssäkerhet till viss del uppfyller revisionsfrågans innebörd. Arbete inom informationssäkerhet har påbörjats och medvetenhet om vikten av detta är hög inom ledningen hos både Knivsta och Heby kommun. Det krävs ett antal åtgärder för att säkerställa en god informationssäkerhet varav några behöver verkställas snarast.

- System- och informationsklassning har påbörjats i Knivsta men ej i Heby. Ur informationssäkerhetssynpunkt måste detta finnas på plats för att möjliggöra rätt nivå av säkerhet och skydd av känslig information, speciellt i ljuset av kommande dataskyddsförordning (GDPR), är det av vikt att detta arbete prioriteras och slutförs.
- Det saknas återkommande risk- och sårbarhetsbedömningar ur ett informationssäkerhetsperspektiv. Vi rekommenderar att samverkansnämnden etablerar en process för återkommande riskbedömningar för att möjliggöra upprättande av åtgärdsplaner för de prioriterade riskerna.
- Det saknas tydliga riktlinjer för hur man som medarbetare skall förhålla sig till informationssäkerhet och integritet och hur incidenter inom området dessa skall hanteras. Vi rekommenderar att samverkansnämnden snarast fastställer riktlinjer för informationssäkerhet och incidentrapportering samt en rutin för återkommande utbildning för samtlig personal.
- Det saknas processer för att säkerställa att medarbetare har rätt behörighetsnivå och därmed deras tillgång till skyddsvärd eller känslig information. Ansvaret för behörigheter ligger i dag på enhetscheferna. Vi rekommenderar att samverkansnämnden snarast inför en process för återkommande revision av behörigheter för att säkerställa att medarbetare som bytt tjänst inte har för hög behörighet och att medarbetare som lämnat sin tjänst också avslutas i systemen.

Bakgrund, syfte och övergripande revisionsfråga

Inledning

Under perioden augusti till oktober 2017 har PwC på uppdrag av revisorerna i Knivsta och Heby kommuner genomfört en översiktlig granskning av Samverkansnämndens arbete med IT- och informationssäkerhet. Granskningen omfattar Samverkansnämndens gemensamma IT-enhet.

Resultatet av granskningen presenteras i denna rapport.

Syfte

Uppdraget innebar att inom ramen för revisionsarbetet inom kommunerna genomföra en övergripande granskning av den gemensamma nämndens arbete med IT- och informationssäkerhet för att förstå och analysera huruvida verksamheten på en övergripande nivå har ändamålsenliga rutiner och processer för att hantera informationssäkerhet. Granskningen har översiktligt fokuserat på; styrning och ledning av IT- och informationssäkerhet, samt rutiner, processer, uppföljning, samt personalaspekter såsom kompetens och bredd.

Syftet med granskningen är att klargöra vilka eventuella områden som Samverkansnämnden behöver utveckla för att uppnå ändamålsenliga rutiner och processer för att hantera IT- och informationssäkerhet på ett för kommunen lämpligt sätt.

Övergripande revisionsfråga

Rapporten avser att belysa följande övergripande revisionsfråga:

Har Samverkansnämnden på en övergripande nivå ändamålsenliga rutiner och processer för att hantera IT- och informationssäkerhet?

För att besvara den övergripande revisionsfrågan har sex områden definierats, bestående av totalt elva delfrågor, se nästa sida.

Revisionsfrågor

Har Samverkansnämnden på en övergripande nivå ändamålsenliga rutiner och processer för att hantera IT- och informationssäkerhet?

Revisionsfrågor delområden:

Styrning av IT

1. Finns det en etablerad styrmodell för IT-verksamheten avseende IT-relaterade prioriteringar inklusive informationssäkerhet?

Styrande dokument

2. Finns beslutade styrande dokument (t.ex. IT-strategi, IT-policy, IT/informationssäkerhetspolicy samt kontinuitetsplan kopplat till informationssäkerhet? Är dessa kommunicerade?)

Informationssäkerhet

3. Har informationssäkerhetsarbetet organiserats på ett ändamålsenligt sätt?
4. Kontrolleras efterlevnaden av riktlinjer för informationssäkerhet?
5. Sker informationsklassning enligt en systematisk metod?
6. Sker utbildning av medarbetare i IT- och informationssäkerhet?
7. Beaktas IT- och informationssäkerhetsrelaterade aspekter vid upphandling/anskaffning av system och applikationer?

IT-Processer

8. Finns det rutiner för rapportering och hantering av säkerhetsbrister och incidenter kopplade till IT och informationssäkerhet?

IT-säkerhet

9. Har risk- och systemsäkerhetsanalyser genomförts för verksamhetskritiska system?
10. Är åtkomstskydd till kritiska system och applikationer (behörighet och lösenord) lämpligt utformat? Genomförs periodisk granskning av tilldelade behörigheter?

IT-drift

11. Är IT-infrastrukturen uppbyggd enligt god praxis och skapar den förutsättningar för ett kvalitativt och säkert IT-stöd (t.ex. finns rutiner och processer för backup och återställning av data)?

Metod

Metod

PwC har baserat granskningen på följande arbetssätt och metodik.

- Intervjuer med identifierade nyckelpersoner i Knivsta och Heby kommuner, (se intervjulista, bilaga 1) samt inläsning och genomgång av tillgänglig dokumentation och styrande dokument.
- Granskningen baseras på PwC:s modell för IT-styrning och IT-mognad (ITM), etablerad god praxis, samt delar av ramverket för informationssäkerhet från National Institute of Standards and Technology (NIST).

Avgränsning

- Erhållet material har granskats på en övergripande nivå.
- PwC har endast granskat den information som tillgängliggjorts för oss.
- Vidare har PwC inte specifikt analyserat Samverkansnämndens externa IT-driftleverantör.
- Verksamhet inom olika kommunala bolag har inte granskats specifikt.

Revisionell bedömning

Övergripande revisionsfråga

Har Samverkansnämnden på en övergripande nivå ändamålsenliga rutiner och processer för att hantera IT- och informationssäkerhet?

Bedömning

Vår övergripande bedömning är att Samverkansnämndens arbete med IT- och informationssäkerhet till viss del uppfyller revisionsfrågans innebörd. Ett strukturerat arbete inom informationssäkerhet har påbörjats och det finns en medvetenhet inom respektive kommun och Samverkansnämnden att det krävs ett antal åtgärder för att optimera arbetet med informationssäkerhet. Vår bedömning är dock att kommunerna kommit olika långt i denna process, där Knivsta kommun uppfattas kommit längre i jämförelse med Heby kommun. Knivsta kommun, till skillnad från Heby kommun, genomför till exempel informationsklassning, har börjat uppdatera befintliga styrdokument kopplade till IT- och informationssäkerhet och utbildar nyanställda chefer inom området. Avseende förberedelse för GDPR, är vår bedömning dock att Heby kommun kommit något längre.

- Det finns en viss diskrepans i uppfattningen inom respektive kommun avseende Samverkansavtalets ansvarsområden och innebörd. Som exempel angavs det under intervjuerna att det tidigare funnits oklarheter kring vilken part som ansvarar för att ta framstyrande dokument.
- Uppdaterade och förnyade styrande dokument i form av IT-strategi, IT-policy, IT/informationssäkerhetspolicy samt kontinuitetsplan med tillhörande riktlinjer, anvisningar och användarvänliga instruktioner bör fastställas och tydligt kommuniceras till användare inom respektive kommun.
- Roller och ansvar kopplade till informationssäkerhet och integritet bör tydliggöras i allmänhet, men särskilt med anledning av kommande dataskyddsförordning (GDPR) som ersätter PUL.
- Kunskapsnivån och medvetenheten avseende IT- och informationssäkerhet varierar bland medarbetarna inom båda kommunerna. De medarbetare som aktivt arbetar med frågor relaterade till IT- och informationssäkerhet bedöms ha en högre grad av kunskap och medvetenhet inom området, i jämförelse med de medarbetare som inte har dessa frågor som primära arbetsområden. Därav är det av vikt att alla medarbetare erbjuds vidare utbildning inom dessa områden och bör ske regelbundet och återkommande.
- Även om respektive kommun är enskilt ansvarig för att tillgodose den egna verksamhetens efterlevnad av lagar, förordningar och regler kopplade till informationssäkerhet, kan detta arbete med fördel samordnas inom Samverkansnämnden. Ett samarbete avseende framtagning av rutiner, processer och dokument kan bland annat leda till högre effektivitet och samsyn avseende avtalets ansvarsområden och innebörd. Vidare bör även en gemensam process för återkommande och regelbundna riskanalyser införas.

Delfråga 1

Finns det en etablerad styrmodell för IT-verksamheten avseende IT-relaterade prioriteringar?

Observationer

- Den strategiska och driftsmässiga ledningen av IT delas mellan Knivsta och Heby. Det finns idag en IT-chef och en IT-driftschef med ansvar för bägge kommunerna.
- Den gemensamma samverkansnämnden för IT ansvarar för de båda kommunernas IT-drift och IT-strategiska frågor. Ansvaret för frågor kring förvaltning och verksamhetsutveckling samt organisation för LIS/informationssäkerhet och hantering av informationssäkerhetsfrågor ligger hos varje kommun. Den gemensamma nämnden kan ges i uppdrag att ta fram olika beslutsunderlag i dessa frågor*.
- Det framkommer under intervjuerna att det inte finns någon ”tydligt etablerad” styrmodell för IT-verksamheten. Det som finns i dagsläget är generella mål för IT (uttryckt i de kommunala målen).
- För löpande styrning & prioritering av IT-relaterade frågor finns i respektive kommun en eStyrgrupp som leds av kommunchefen i Heby kommun och av kanslichefen i Knivsta kommun.

Rekommendationer

- Kommunerna bör ta fram en detaljerad plan och övergripande strategi/styrmodell för sin respektive IT-verksamhet. Denna styrmodell bör utgå från respektive kommuns vision och långsiktiga strategiska mål, samtidigt som Samverkansnämndens gemensamma mål och prioriteringar bör beaktas. Vidare bör den beskriva hur IT ska bidra till att uppfylla dessa mål.
  - Styrmodell bör kompletteras med en handlingsplan med prioriterade aktiviteter. Den bör omfatta både egna och Samverkansnämndens gemensamma prioriteringar.
  - Styrmodellen bör beslutas inom kommunledning och ägas av IT- och informationsansvariga.
  - Arbetet med att planera och ta fram styrmodellerna, kan med fördel samordnas inom Samverkansnämnden för att nå högre effektivitet och transparens.

* Källa: Verksamhetsberättelse och årsbokslut för Samverkansnämnden 2016.

Delfråga 2

Finns beslutade styrande dokument (t.ex. IT-strategi, IT-policy, IT/informationssäkerhetspolicy samt kontinuitetsplan kopplat till informationssäkerhet? Är dessa kommunicerade?

Observationer

- Granskningen visar att det i dagsläget saknas uppdaterade styrdokument gällande IT-strategi, IT-policy samt handlingsplan. Det senast uppdaterade IT-strategidokumentet i Knivsta kommun är daterat 2008-02-28, dock visar intervjuerna att innehållet inte blivit tydligt kommunicerat till berörda medarbetare.
- Utöver ovannämnda dokument saknas aktuell IT-säkerhetspolicy och informationssäkerhetspolicy. I Knivsta kommun finns dock utkast som är under revidering. Planen är att uppdaterade policys ska kommuniceras till verksamheten efter årsskiftet 2017/2018.
- Övergripande kontinuitetsplan för IT-verksamheten saknas, även om det under intervjuerna angavs finnas mer utvecklade kontinuitetsplaner för vissa delar av verksamheten i båda kommunerna (t.ex. Socialförvaltningen).
- Inom Knivsta kommun pågår ett arbete med att uppdatera och komplettera de befintliga styrande dokumenten för informationssäkerhet. I Heby kommun har en medarbetare fått ansvar att påbörja arbetet med att ta fram relevanta styrdokument.

Rekommendationer

- Respektive kommun bör ta fram en plan för att komplettera IT-relaterade styrande dokument, där bland annat följande dokument för IT behöver utvecklas:
  - IT-strategi, IT-policy och handlingsplan.
  - IT-säkerhets- och Informationssäkerhetspolicy, kontinuitetsplan för IT-verksamheten.
  - Arbetet med att planera och ta fram dessa styrdokument, kan med fördel samordnas inom Samverkansnämnden för att nå högre effektivitet och transparens. Samt förbereda för den planerade utvecklingen av samverkansnämnden med fler kommuner.
- Vidare bör respektive kommun ta fram ändamålsenliga, användarvänliga och lättillgängliga riktlinjer, anvisningar och instruktioner kopplade till dessa styrande dokument.

Delfråga 3

Har IT- och informationssäkerhetsarbetet organiserats på ett ändamålsenligt sätt?

Observationer

- Under intervjuerna framkommer det att IT-organisationen har genomgått stora förändringar under senare tid, vilket har påverkat IT-och informationssäkerhetsarbetets framgång.
- Granskningen visar att arbetet med IT-och informationssäkerhet till viss del organiserats och påbörjats, där det under intervjuerna framkommer att t.ex. en person i respektive kommun anställts på heltid för att arbeta med frågor kopplat till dessa områden. Dock är detta arbete i ett initialt skede.
- Det saknas dokumenterade roll- och ansvarsbeskrivningar relaterade till IT-och informationssäkerhetsarbetet samt process för identifiering/tilldelning av informationsägarskap.
- Av intervjuerna framkommer det att det råder en brist i samarbetet och kommunikationen mellan verksamheten och IT. Det upplevs saknas tydliga kontaktpersoner och kommunikationsvägar.
- Vidare framkommer att det saknas tydliga och uppdaterade kontinuitetsplaner kopplade till informationssäkerhets-incidenter. Dock framkommer det att dessa planer är under bearbetning.
- Utifrån intervjuerna bedöms det finnas en medvetenhet bland medarbetarna kring fördelarna samt vikten av att börja av ett välorganiserat IT-och informationssäkerhetsarbete.

Rekommendationer

- Samverkansnämnden bör vidareutveckla den övergripande planen för hur arbetet med informationssäkerhet ska organiseras inom kommunerna. När en sådan plan är upprättad bör den på ett strukturerat sätt kommuniceras till verksamheten, i syfte att skapa en samsyn beträffande informationssäkerhetsarbetet.
- Vidare bör även roll- och ansvarsbeskrivningar fastställas för samtliga roller relaterade till informationssäkerhetsarbetet inom kommunernas verksamheter. Bland dessa roller bör den roll som omfattar ansvaret för att leda arbetet med att anpassa respektive kommuns verksamhet till den nya dataskyddsförordningen (GDPR*) ingå. För denna roll krävs, utöver en tydlig rollbeskrivning, mandat samt erforderlig kompetens då regelverket i den nya förordningen är mer komplext än Personuppgiftslagen (PuL).
- En process för identifiering och tilldelning av informationsägarskap bör tas fram.
- Vidare rekommenderas att kommunerna planerar och genomför återkommande kris- och katastrofövningar kopplade till IT/informationssäkerhet och integritet för att säkerställa en god beredskap för intrång med förlust av t.ex. känsliga persondata samt identifiera och rätta fel i processerna.

***) GDPR** – (General Data Protection Regulation). Ny dataskyddsförordning som är gemensam inom EU och ersätter Personuppgiftslagen. GDPR träder i kraft 25 maj 2018. I Sverige kommer Datainspektionen att vara tillsynsmyndighet

Delfråga 4

Kontrolleras efterlevnaden av riktlinjer för informationssäkerhet?

Observationer

- Granskningen visar att det inte finns några etablerade rutiner, strukturerade processer eller kontroller avseende uppföljning av medarbetarnas efterlevnad av riktlinjer inom IT- och informationssäkerhet eller övriga IT-relaterade styrande dokument.

Rekommendationer

- För att identifiera, hantera och förebygga eventuella incidenter relaterade till IT- och informationssäkerhet är det av vikt att respektive kommun tar fram en strukturerad plan som säkerställer medarbetarnas efterlevnad av policys, riktlinjer, anvisningar och instruktioner. Arbetet med att ta fram en sådan plan kan med fördel samordnas inom Samverkansnämnden för att nå högre effektivitet och transparens.

Delfråga 5

Sker informationsklassning enligt en systematisk metod?

Observationer

- I Knivsta kommun genomförs informationsklassning med hjälp av verktyget *KLASSA**. Dock framkommer det under intervjuerna att detta inte genomförs med regelbundenhet. Vidare framkommer att det saknas en övergripande och gemensam plan avseende vilka system som ska informationsklassificeras och under vilka omständigheter.
- I Heby kommun har arbetet med informationsklassning inte påbörjats i någon större omfattning. Intervjuerna visar dock att det finns en medvetenhet kring fördelarna samt vikten av att börja arbeta med informationsklassning.

Rekommendationer

- Vi rekommenderar respektive kommun att ta fram en strukturerad plan för hur arbetet gällande informationsklassificering ska genomföras. Planen bör innehålla en tydlig beskrivning av målen med informationsklassificeringen samt hur dessa mål ska uppfyllas inom respektive verksamhet.
  - Arbetet med att utveckla denna plan kan med fördel samordnas inom Samverkansnämnden för att nå högre effektivitet och transparens.
- Med bakgrund av den kommande dataskyddsförordningen (GDPR), är det av vikt att Knivsta kommun fortsätter arbetet med informationsklassning på ett mer strukturerat sätt samt att Heby kommun skyndsamt påbörjar arbetet med informationsklassning enligt en systematisk metod.

***) KLASSA** – En metod framtagen av SKL för att hjälpa verksamheten välja rätt åtgärder som skyddar informationen.

Delfråga 6

Sker utbildning av medarbetare i IT- och informationssäkerhet?

Observationer

- Det saknas en fastställd utbildningsplan för utbildning inom IT och informationssäkerhet hos båda kommunerna. Dock framkommer det att en plan är under framtagning inom vilken målet är att varje nyanställd ska få möjlighet att delta i relevanta utbildningar.
- Det finns en webbaserad utbildningsplattform hos båda kommunerna som främst är tillgänglig för nyanställda chefer. Plattformen nämns vara under vidareutveckling.
- I Knivsta kommun genomförs inte strukturerade utbildningar i IT och/eller informationssäkerhet i någon större omfattning, med undantag för nyanställda chefer som genomgår en sådan utbildning. För övriga medarbetare finns ingen motsvarande utbildning.
- I Heby kommun genomgår ingen medarbetare någon utbildning avseende IT- och/eller informationssäkerhet, med undantag för Socialförvaltningen där utbildning av nyanställda sker riktad mot information som skyddas av offentlighets- och sekretesslagen. Arbetet har dock påbörjats inom Heby kommun med att ta fram en kortare introduktionsutbildning, vilken planeras vara färdig under december 2017.
- Kunskapsnivån och medvetenheten avseende IT och informationssäkerhet varierar bland medarbetarna inom båda kommunerna. De medarbetare som aktivt arbetar med frågor relaterade till IT och Informationssäkerhet bedöms ha en högre grad av kunskap och medvetenhet inom området, i jämförelse med de medarbetare som inte har dessa frågor som primära arbetsområden. Det framkommer dock att det inom Socialförvaltningen bedöms föreligga en hög grad av kunskap och medvetenhet avseende information som skyddas av offentlighets- och sekretesslagen.

Rekommendationer

- Kommunerna rekommenderas fortsätta sitt påbörjade arbete med en mer strukturerad utbildningsplan inom IT- och informationssäkerhet. Detta arbete kan med fördel samordnas inom Samverkansnämnden för att nå högre effektivitet och transparens.
  - Utbildningsplanen bör omfatta alla anställda och innehålla information om vilken kunskapsnivå en viss roll kräver, samt vilken typ av kunskapshöjande aktiviteter som bör genomföras.
  - Vidare bör kommunerna tydliggöra ansvaret för att utbildning inom IT- och informationssäkerhet ska ske regelbundet och återkommande, i syfte att öka kunskapen och medvetenheten hos medarbetare inom ämnet. I ett initialt skede skulle detta ansvar kunna ligga på informationssäkerhetssamordnaren.
- För att tillfullo utnyttja de resurser som investerats i respektive kommuns utbildningsplattform, bör kommunerna säkerställa att dessa tillgängliggörs och nyttjas av fler medarbetare än enbart nyanställda chefer.
- Kommunerna bör även skyndsamt säkerställa att utbildning kring regelverket i den nya dataskyddsförordningen (GDPR) genomförs. Denna utbildning bör bland annat omfatta hur det skiljer sig från PUL samt vilka krav det ställer på hantering av personuppgifter.

Delfråga 7

Beaktas IT- och informationssäkerhetsrelaterade aspekter vid upphandling/anskaffning av system och applikationer?

Observationer

- Under intervjuerna framkommer det att upphandling normalt sker med hjälp av Kammarkollegiets ramavtal. Dessa avtal innehåller bland annat rekommendationer över vilka informationssäkerhetsrelaterade aspekter som bör beaktas vid upphandling.
- Granskningen visar dock att ramavtalen inte alltid används som underlag vid upphandling. Som exempel nämns bland annat att anskaffningen av den nya IT-leverantören (Advania) inte granskades i enlighet med ”utökade” informationssäkerhets-relaterade aspekter. Den nya leverantören anges enbart ha granskats i enlighet med de grundläggande krav gällande dataskydd, accesskontroll samt fysisk/logisk tillgång som IT-enheten har.
- Respektive förvaltnings/kontorschef är i dagsläget ansvarig för inköp av verksamhetssystem. Dock framkommer det under intervjuerna att IT inte är involverade i denna process.

Rekommendationer

- För att säkerställa en ändamålsenlig informationssäkerhet och god teknisk IT-säkerhet, är vår rekommendation att upphandling av kritiska system/applikationer/tjänster, ska ske i enlighet med de utökade krav på informationssäkerhet som bland annat ställs i relation till införandet av den nya dataskyddsförordningen.
- Vid upphandling av nya system och applikationer, bör IT användas som en rådgivande stödfunktion i tekniska frågor bland annat relaterade till IT- och informationssäkerhet. Genom detta tillvägagångssätt kan verksamheten få råd kring exempelvis det tilltänkta systemets eller applikationens lämplighet i relation till den nuvarande systemfloran samt kapacitetsplanering.

Delfråga 8

Finns rutiner för rapportering och hantering av säkerhetsbrister och incidenter kopplade till IT- och informationssäkerhet?

Observationer

- Av granskningen framkommer att ändrings-, incident och problemhantering avseende verksamhetskritiska IT-system och applikationer hos båda kommunerna är utlagt på extern leverantör.
- Det framkommer dock av intervjuerna att det saknas generella rutiner för rapportering och hantering av säkerhetsbrister och incidenter kopplade till IT- och informationssäkerhet inom båda kommunerna. Som exempel nämns att det råder en oklarhet bland medarbetarna avseende vem, vad, när och hur en säkerhetsbrist ska rapporteras.
- Dock visar intervjuerna samtidigt på att det inom Socialförvaltningen i respektive kommun finns dokumenterade rutiner och beskrivningar för incidenter avseende information som skyddas av offentlighets- och sekretesslagen.

Rekommendationer

- Rutiner för rapportering och hantering av säkerhetsbrister och incidenter kopplade till IT- och informationssäkerhet bör snarast upprättas, dokumenteras och anpassas till samtliga förvaltningar (kontor), samt kommuniceras och tillgängliggöras till verksamheten inom respektive kommun.

Delfråga 9

Har risk- och systemsäkerhetsanalyser genomförts för verksamhetskritiska system?

Observationer

- Granskningen visar att det i Knivsta kommun främst är en medarbetare som genomför riskanalyser avseende IT- och informationssäkerhet. Enligt intervjuerna finns det dock inte några strukturerade processer och rutiner för detta arbete.
- Avseende Heby kommun visar intervjuerna att det inte genomförs regelbundna riskanalyser avseende IT- och informationssäkerhet. Det saknas även strukturerade processer och rutiner för detta arbete.
- Det framgår av granskningen att det är respektive systemägare som är ansvarig för att genomföra systemsäkerhetsanalyser. Det saknas dock strukturerade processer och rutiner för att säkerställa att sådana analyser genomförs regelbundet.
- Vidare visar intervjuerna att uppdateringen av vissa verksamhetskritiska system varit bristfällig under de senaste åren. I samband med sammanslagningen mellan Knivsta/Heby kommuner har dock fler uppdateringar genomförts, även om det fortfarande uppges finnas ett behov av ytterligare uppdateringar.

Rekommendationer

- Risk- och systemsäkerhetsanalyser är en kritisk del i arbetet med att nå en ändamålsenlig hantering av IT- och informationssäkerhet då dessa bidrar i arbetet med att identifiera risker, som vid allvarliga händelser, kan få väsentlig påverkan på verksamhetskritiska system och processer. Vår rekommendation är därför att kommunerna tar fram tydliga processer och rutiner för att säkerställa att risk- och systemsäkerhetsanalyser genomförs på ett ändamålsenligt sätt. Samverkansnämnden bör samordna detta arbete för att nå en högre effektivitet och samsyn mellan kommunerna.
- För att säkerställa en god tekniskt IT-säkerhet och skydda verksamhetskritisk information, krävs ett aktivt arbete för att upptäcka/motverka intrångsförsök i system och applikationer. Vi rekommenderar därför att respektive kommun tar fram en strukturerad plan med rutiner och processer för vilka system och applikationer som ska uppdateras och med vilka tidsintervall. Samverkansnämnden bör samordna detta arbete för att nå en högre effektivitet och samsyn mellan kommunerna.

Delfråga 10

Är åtkomstskydd till kritiska system och applikationer (t.ex. behörighet och lösenord) lämpligt utformat? Genomförs periodisk granskning av tilldelade behörigheter?

Observationer

- Rent formellt är det respektive förvaltningschef (kontorschef) som är ansvarig att granska, registrera och avsluta medarbetares behörighet och tillgång till diverse verksamhetskritiska system och applikationer. Dock visar intervjuerna att det inte genomförs några strukturerade kontroller för om huruvida medarbetares behörigheter genomförs i enlighet med uppsatta rutiner eller ej.
- Vidare anges det inte finnas några dokumenterade riktlinjer, anvisningar eller instruktioner kopplade till behörighetskontroll (t.ex. upplägg/avslut av medarbetares tillgång till system och applikationer samt beskrivning för när behörigheter ska granskas).
- Av intervjuerna framkommer att tilldelning av behörigheter fungerar väl vid nyanställning. Vid internt byte och avslut av tjänst, upplevs behörighetskontrollen i vissa situationer som bristfällig.

Rekommendationer

- För att säkerställa ett välfungerande åtkomstskydd, behövs uppdaterade och mer organiserade rutiner och processer för respektive kommun avseende upplägg, avslut och granskning av tilldelade behörigheter. Samverkansnämnden kan bidra i detta arbete med syfte att skapa en samsyn mellan kommunerna inom detta område.

Delfråga 11

Är IT-infrastrukturen (kommunens interna nätverks-infrastruktur) uppbyggd enligt god praxis och skapar den förutsättningar för ett kvalitativt och säkert IT-stöd (t.ex. finns rutiner och processer för backup och återställning av data)?

Observationer

- Granskningen visar att Samverkansnämnden ska byta leverantör från Axians till Advania i november 2017. Detta omfattar alla tjänster kopplat till drift, nätinfrastruktur samt backup och återställning av data.
- Vidare ägs IT-plattformen av Samverkansnämnden, där IT-enheten ansvarar för driften av kommunernas interna nätverk.
- Den IT-infrastruktur som är utlagd på extern leverantör antas vara uppbyggd enligt grundläggande förutsättningar som finns för god praxis, dock inkluderas inte Axians/Advanias processer och rutiner avseende dessa områden i denna granskning.
- Den IT-infrastruktur som är kopplad till kommunernas interna nätverk uppfattas i vissa situationer vara av ”för hög säkerhetsnivå”, där medarbetare delger att nivån på säkerhet påverkar nätverkets användarvänlighet negativt. Det noteras dock att det inte har genomförts några återkommande riskanalyser som grund för nätverkets säkerhetsnivå eller några penetrationstester.
- Vidare framkommer det i granskningen att det genomförts återläsning av data vid incidenter (t.ex. om specifik information förlorats). Det har dock inte genomförts några planerade tester av leverantörens förmåga avseende backup- och återställning av data.

Rekommendationer

- För att fastställa ett säkert IT-stöd samt att leverantören uppfyller överenskommet SLA, bör kommunerna framta en rutin för återkommande tester avseende backup och återställning av data (så kallade ”disaster recovery tester”).
- För att säkerställa att leverantören levererar ett ändamålsenligt och säkert IT-stöd, bör Samverkansnämnden begära in styrande dokument relaterade till IT (t.ex. disaster reocvery-plan, kontinuitetsplan) samt karta över deras IT-infrastruktur.
- Vi rekommenderar att kommunerna implementerar en process för genomförande av återkommande riskanalyser och penetrationstester avseende kommunernas interna nätverks-infrastruktur.

Avslutning

Vi vill avslutningsvis ta tillfället i akt och tacka de personer som deltagit i intervjuer och bidragit med underlag till denna översyn för ett vänligt bemötande och ett gott samarbete.

Vid frågor om översynen kan Mikael Carinci eller Anders Gustafson kontaktas.

Stockholm, oktober 2017

Kontakt:

Mikael Carinci

E-post: mikael.carinci@pwc.com

Tel: 072 - 980 90 35

Anders Gustafson

E-post: anders.gustafson@pwc.com

Tel: 070 – 929 42 62

Bilagor

Bilaga 1
Intervjulista

Namn	Roll	Verksamhet
Anders Fredriksson	IT-säkerhetssamordnare	Knivsta kommun
Christina Björses	Samordnare IT	Heby kommun
Emma Burstedt	Kommunchef	Heby kommun
Karin Eljansbo	Administrativ chef	Heby kommun
Lars-Erik Andersson	IT-chef	Samverkansnämnden (Knivsta kommun & Heby kommun)
Lena Fransson	Kommundirektör	Knivsta kommun
Michael Von Essen	IT-driftschef	Samverkansnämnden (Knivsta kommun & Heby kommun)
Rojda Sjöö	Verksamhetsutvecklare	Knivsta kommun
Åsa Franzén	Kanslichef, Biträdande kommundirektör (GDPR)	Knivsta kommun
Åsa Johansson	Förvaltningschef, Vård och Omsorg	Heby kommun

Bilaga 2

Vad innebär en god informationssäkerhet och teknisk IT-säkerhet?

En god informationssäkerhet syftar till att säkra en effektiv informationsförsörjning och att undgå allvarlig fel som påverkar möjligheten att bedriva en ändamålsenlig verksamhet.

En ändamålsenlig informationssäkerhet innebär:

- Vidta preventiva åtgärder för att undvika att information kan förvanskas eller för att förhindra informationsläckage.
- Säkerställa att man alltid har tillgång till den information organisationen behöver för sin dagliga verksamhet, även om kris eller katastrof föreligger.
- Informationssäkerhetsnivån man är helt avhängig den riskaptit man har, samt den bedömda hotbilden.
- En organisation som hanterar mycket känslig information, exempelvis i form av personuppgifter i kundregister, lönelistor eller liknande, kan behöva mer skydd än en organisation som inte hanterar och lagrar liknande information.

En god teknisk IT-säkerhet innebär att organisationen har rutiner, processer och uppsatta kontrollpunkter som löpande följs upp och att organisationen har rutiner för att hålla sig uppdaterad kring omvärldshot och förändringar som kan påverka kritiska resurser.

En god teknisk IT-säkerhet innebär:

- att ha hög tillgänglighet till information och tjänster,
- att säkerställa informationens riktighet genom skydd mot oavsiktlig och avsiktlig förvanskning,
- att ha en behörighetskontroll baserad på klassificering av informationens känslighet, spårbarhet och konfidentialitet, samt möjlighet till skyddad kommunikation,
- ett aktivt arbete för att så tidigt som möjligt upptäcka och åtgärda intrångsförsök och identifiera eventuella sårbarheter i den interna och externa IT-miljön.