Tyresö kommun
Kommunstyrelseförvaltningen
Sara Vikslund
Enhetschef Verksamhetsstöd och utveckling
sara.vikslund@tyreso.se

TJÄNSTESKRIVELSE
2022-01-23

Diarienummer
2021/REV 0009

Kommunledningsutskottet

Svar på revisionsrapport om fördjupad granskning inom Cybersäkerhet

Kommunstyrelseförvaltningens förslag till kommunledningsutskottet för beslut i kommunstyrelsen

- Kommunstyrelseförvaltningens skrivelse antas som kommunstyrelsens svar på revisionsrapporten ”Fördjupad granskning inom cybersäkerhet”

Kommunstyrelseförvaltningen

Elin Waltersson
Tf. Kommundirektör

Antonios Arvanitidis
Stabschef IT och digitalisering

Sammanfattning

På uppdrag av de förtroendevalda revisorerna har EY genomfört en fördjupad granskning av kommunens arbete med IT- och informationssäkerhet. Granskningens syfte har varit att följa upp och fördjupa den granskning som gjordes januari-mars 2019 och bedöma om det finns brister i kommunens arbete med IT- och informationssäkerhet. Vidare har syftet också varit att bedöma i vilken omfattning kommunstyrelsen och nämnderna styr och följer upp arbetet på området.

Beskrivning av ärendet

Granskningen genomfördes under augusti till oktober 2021 och baserades på intervjuer med identifierade nyckelpersoner i kommunens informationssäkerhetsarbete och genomgång av insamlade styrdokument. Granskningen har fokuserat på fem utvalda fördjupningsområden: Åtkomsthantering, Styrning och organisation, Medvetenhet och utbildning, Policyer och rutiner samt Tredjepartshantering.

Granskningen har genomförts utifrån EYs ramverk för granskning av IT- och informationssäkerhet. Utifrån valda områden har kommunens nivå bedömts på en skala från 1 (begynnande) till 5 (optimerad) inom respektive område.

Nivån bedöms vara som högst inom identitetshantering och ledningssystem. Lägst anses nivån vara inom kontinuerlig utbildning, policyer och rutiner relaterade till tredjeparter samt granskning och genomgång av behörigheter.

Revisorernas rekommendationer till kommunstyrelsen utifrån granskningens resultat

Kommunen delar uppfattningen om granskningens fyra förbättringsområden och föreslår åtgärder i tabellen längre ned i tjänsteskrivelsen. Utifrån granskningens resultat rekommenderas kommunstyrelsen att:

- Upprätta lämpliga rutiner för att IT incidenter och säkerhetsrisker rapporteras till kommunstyrelsen.
- Etablera tydliga processer och riktlinjer kring hur arbetet med granskning och uppföljning ska genomföras. Detta inkluderar både efterlevnad av styrdokument, samt tredjeparters efterlevnad av på förhand definierade säkerhetskrav.
- Säkerställa att styrdokument förblir aktuella över tid, samt kommunicerade till kommunens anställda.
- Förbättra arbetet med utbildning och medvetenhet hos personalen. Detta genom att arbeta utefter en tydligt definierad plan som säkerställer att regelbundna och obligatoriska utbildningar genomförs och utvärderas.

Nr	Rekommendation	Kommentar	Start	Slut
1	Upprätta lämpliga rutiner för att IT incidenter och säkerhetsrisker rapporteras till kommunstyrelsen.	**A.** Planera in och genomföra "Ledningens genomgång" från MSB som innefattar hotbild, incidenter etc. på KS. - Säkerställer att incidentrutinerna är relevanta och etablera rapporteringsrutiner till KS - Tar fram och inför en palett/verktygslåda med olika mätmöjligheter för informationssäkerhetsrisker. Mätningarna delas in i organisatoriska och tekniska risker. Där MSB:s InfoSäkKollen utgör ett fundament i mätningen för organisatorisk risk. Tekniska mätningar innehåller exempelvis penetrationstester. - Dokumentera helheten i en riktlinje	2022 Q3	2023 Q1

2	Etablera tydliga processer och riktlinjer kring hur arbetet med granskning och uppföljning ska genomföras. Detta inkluderar både efterlevnad av styrdokument, samt tredjeparters efterlevnad av på förhand definierade säkerhetskrav.	**A.** Tar fram en palett/verktygslåda med olika granskningsmöjligheter av hur styrdokument efterlevs i den interna organisationen. Utgångspunkt är exempelvis tillämpning av informationssäkerhetspolicy, även konkretiserat i exempelvis status för informationssäkerhetsklassning av verksamhetssystem. **B.** Tar fram en palett/verktygslåda med olika granskningsmöjligheter av hur leverantörers uppfyller säkerhetskraven. Verktygslådan förväntas innehålla alternativa metoder för granskning såsom - Brett med relativt enkla grundläggande frågor - mer omfattande till prioriterade leverantörer utifrån risk - Granskning på plats **C.** Resultatet dokumenteras i en riktlinje	2022 Q4	2023 Q2
3	Säkerställa att styrdokument förblir aktuella över tid, samt kommunicerade till kommunens anställda.	**A.** Identifiera årshjul för varje styrande dokument inom informations- och datasäkerhet, samt koppla roller med ansvar för revision. **B.** Kommunikation till medarbetare att styrdokument ändras - Passiv sökning, såsom sida på intranätet med varje dokuments årshjul och ansvariga. - Uppsökande, ingår i årlig utbildning (live) av nya chefer,	2022 Q2	2022 Q4

		dataskydd- och säkerhetssamordnare, samt den inspelade versionen (PPT med berättarröst) **C.** Resultatet dokumenteras i en riktlinje **D.** Säkerställa att alla medarbetare årligen tar del av inspelade PPT med berättarröst t.ex. på APT**.**		
4	Förbättra arbetet med utbildning och medvetenhet hos personalen. Detta genom att arbeta utefter en tydligt definierad plan som säkerställer att regelbundna och obligatoriska utbildningar genomförs och utvärderas.	**A.** Identifiera obligatoriska och frivilliga utbildningar per relevant roll samt form, inordna i systematisk planering. Exempel på former och kunskapsområden är; - Nya chefer, dataskydds- och säkerhetssamordnare Årlig liveutbildning erbjuds 2ggr/år - Samtliga medarbetare Webbutbildning för GDPR och informationssäkerhet Inspelad årlig utbildning, PPT med berättarröst. **B.** Ta fram krav för utbildningar inom informationssäkerhet och dataskydd för ev. upphandling av Lärplattform. **C.** Resultatet dokumenteras i en riktlinje	2022 Q3	2023 Q2

Prövning av barnets bästa

Sveriges riksdag fattade beslut om att ratificera FN konventionen om barnets rättigheter den 1 juni 1990. Den 1 januari 2020 blev barnkonventionen svensk lag, Barnrättslagen. Det innebär bland annat att barnets bästa ska prövas innan olika beslut fattas och att medborgare har rätt att överklaga beslut med hänvisning till den nya lagen.

Föreliggande ärende gällande IT- och informationssäkerhet berör inte barn direkt och därför görs ingen fördjupad prövning av barnets bästa. Planerade insatser som rutin vid IT-incident, tydliga processer, aktuella styrdokumentation, utbildning och medvetenhet hos personal säkerställer IT- och informationssäkerhet och är kvalitetshöjande för kommunens arbete. Konsekvensen av föreliggande granskning, gynnar därmed indirekt barn genom hantering av uppgifter som rör barn och deras integritet.

Ärendets karaktär kan indirekt hänvisas till artikel 4 som handlar om att varje stat ska nyttja sina resurser till fullo för att uppfylla barns rättigheter, samt artikel 8 om barns rätt till sin identitet och artikel 16 om barns rätt till privatliv.

Ekonomisk kalkyl

Kalkylen innefattar de timmar som uppskattas kräva en konsult och således generera en direkt kostnad. Utöver dessa timmar så tillkommer interna timmar från främst CISO/DSO (Stöd och servicekontoret) och enhetschef Infrastruktur och service (IT och digitaliseringsstaben). Interna timmar bedöms hanteras inom ordinarie linjearbete.
Finansiering av konsult skulle kunna finansieras av digitaliseringsmedel efter beslut av Kommunledningsgruppen. Den totala kostnaden för konsult uppgår till ca.1000 tsek. Fördelade på timmar enligt nedan tabell.

Åtgärd nr	Beskrivning	Timmar konsult	
Åtgärd 1	Upprätta lämpliga rutiner för att IT incidenter och säkerhetsrisker rapporteras till kommunstyrelsen	110	
Åtgärd 2	Etablera tydliga processer och riktlinjer kring hur arbetet med granskning och uppföljning ska genomföras. Detta inkluderar både efterlevnad av styrdokument, samt tredjeparters efterlevnad av på förhand definierade säkerhetskrav.	152	
Åtgärd 3	Säkerställa att styrdokument förblir aktuella över tid, samt kommunicerade till kommunens anställda.	103	
Åtgärd 4	Förbättra arbetet med utbildning och medvetenhet hos personalen. Detta genom att arbeta utefter en tydligt definierad plan som säkerställer att regelbundna och obligatoriska utbildningar genomförs och utvärderas.”	308	
		672	