§ 346
Revisionsrapport Uppföljning IT-säkerhet och införande av dataskyddsförordningen - svar
Dnr KS/2018:384

Beslut
Kommunstyrelsen beslutar:

1. Avge svar enligt kommunledningskontorets förslag.
2. Uppdra till kommunledningskontoret att följa upp beslutade åtgärder enligt genomförd GAP-analys hösten 2016, och säkerställa att dessa blir åtgärdade.
3. Uppmana samtliga nämnder att se över åtgärder enligt samma GAP-analys.
4. Uppmana samtliga nämnder att implementera de nya uppdaterade VROB gällande förvaltning och drift.
5. Uppmana samtliga nämnder att arbeta in en handlingsplan för det fortsatta arbetet med GDPR/Dataskyddsförordningen

---

Ärendet
På uppdrag av kommunens revisorer har KPMG upprättat en revisionsrapport på ”Uppföljning av IT-säkerhet och granskning av införandet av dataskydds-förordningen” samt ”införandet av dataskyddsförordningen”. Rapporten har faktakontrollerats av IT-samordnare och IT-chef.

Beslutsunderlag
Svar revisionsrapport ” Uppföljning av IT-säkerhet och granskning av införandet av dataskyddsförordningen”

Vision 2025

Protokollsutdrag till
Kommunchefen
Samtliga förvaltningschefer

Exp / 2018

TIMRÅ KOMMUN
Kommunledningskontoret

Svar på revisionsrapport "Uppföljning av IT-säkerhet och granskning av införandet av dataskyddsförordningen"

KPMG har på uppdrag av kommunens revisorer genomfört en uppföljning av tidigare granskning av IT-säkerhet samt granskning av införandet av dataskyddsförordningen. Samtliga nämnder och kommunstyrelsen ska lämna svar på de slutsatser som redovisas och åtgärder senast 21 januari 2019.

Säkerställande av beslutade åtgärder vidtas enligt genomförd GAP- och riskanalys

GAP analys gjordes hösten 2016 och riskutvärdering gjordes 2017 på kommunens prioriterade system. Dessa visar på brister i olika system. Bland annat;

Saknas handlingsplaner för analys och hantering av risker för verksamhetssystemen.

- *Planerna saknas fortfarande. Centrala IT har 4 gånger per år förvaltningsmöten där kommande arbeten tas upp för respektive verksamhetssystem. I de uppdaterade riktlinjerna står även att en systemplan ska göras årligen.*

LIS system skulle införas.

- *LIS system har införts. Systemet har dock inte varit så enkelt som det utlovades från leverantören. Två analyser är gjorda 2017 och 2018.*
- *Mall för en enklare riskanalys har tagits fram och kommer spridas/informeras om till systemförvaltarna på decembermötet.*

Uppdragsbeskrivning av Centrala IT.

- *Omorganisation med ny chef som rekryterats och tillträder 1 januari 2019.*

Saknas strategi, tex processdokumentation och övrig systemrelaterad information.

- *En IT-arkitekt genomför en dokumentation av kommunens nätverk under 2018. Utöver detta arbete måste varje systemägare ta sitt ansvar och dokumentera hur just deras system är uppsatt och med vilka kopplingar.*

Utbildning i informationssäkerhet.

- *Både Informationssäkerhet samt GDPR/Dataskyddsförordningen har pågått i flera omgångar, under 2017-18 till alla medarbetare.*

Postadress: 861 82 Timrå
Besöksadress: Köpmangatan 14
Telefon: 060-16 31 00
Bankgiro: 5672-9387
Organisationsnummer: 212000-2395
Fax: 060-16 31 05
Hemsida: www.timra.se
E-post: info@timra.se

TIMRÅ KOMMUN
Kommunledningskontoret

IT-infrastruktur *– Kraftförsörjningen*

- *Ansvaret internt på Kultur- o teknikförvaltningen. Centrala IT har säkerhetsställt viss säkerhet i kommunhuset under 2017-18 genom en ny UPS.*

Kommunikationsnivåer till prioriterade arbetsplatser.

- *Ingen brist i dagsläget. Inga synpunkter har heller kommit från verksamheten att det ska vara någon brist någonstans.*

Kommunens telefonväxel *– Tillgänglighet och test regelbundet. Huvudansvaret ligger på leverantören Sundsvalls kommun. Gemensamma förvaltningsmöten ca 4 gånger per år.*

WWW.TIMRA.SE –Tillgänglighet, prio ett vid en kris.

- *Omfattande arbete genomförts för att säkra upp tillgängligheten under 2017-18. Servrar har flyttats och uppgraderats. Samt att under 2018 driftsätts en helt ny webbportal.*

Mailsystemet *– Flera mailsystem används inom kommunen vilket också bör tydliggöras. De höga SLA nivåer som finns på Outlook omfattas inte Firstclass inom skolan av. Förslaget i rapporten var att enas om ett system med lika hög tillgänglighet.*

- *Under 2018 har projekt inletts för att försöka lösa den frågan. Dessutom genomförs en sammanslagning av de två olika IT-enheterna under 2019.*

Det föreslogs en utbildning för medarbetarna om hur man hanterar mail och klickar på länkar.

- *Det har gjorts 2017 i en omgång, och görs löpande just nu i en annan omgång, november 2018.*

Det föreslogs en handlingsplan när kommunen skulle byta mailsystem och uppgradera.

- *När det gäller systemet för adminnätet har detta redan gjorts under 2017-18 till nyaste versionen, och arbetet fortsätter som sagt under 2019 med att försöka lösa ett gemensamt system för alla medarbetare.*

Teis *– Saknas en bedömning om vad som ska övervakas. Och vilka kriterier och larm som ska kräva åtgärd.*

- *Här krävs det insatser från alla håll. Först från systemägare som är de som ska sätta nivåerna för just sitt system. Sedan måste Centrala IT dokumentera detta på ett pedagogiskt sätt. Det har under flera års tid gått larm via mail, till två*

TIMRÅ KOMMUN
Kommunledningskontoret

ansvariga på Centrala IT och till vissa systemförvaltare. Detta måste tydliggöras under 2019 till systemförvaltarna vad dessa mail innebär.

LEX *– Inför framtiden med integration mot e-tjänster bör en godkänd process för varje integration göras, så att hänsyn tas till alla säkerhetsrisker.*

- *Detta görs i varje projekt för varje enskild e-tjänst. Detta har löpande pågått under 2018 och fortsätter under 2019.*

eCompanion/Besched *– Här planeras upphandling och införande av nytt system. Detta system agerar master för all personal och alla behörigheter i nätet. Eftersom detta system har särskilt höga krav just vid utbetalningstillfällena föreslås att kommunen har goda rutiner för ett eventuellt bortfall de dagarna i månaden.*

- *Det finns reservrutin med banken och har funnit sedan start 2004. Detta måste också säkerställas inför ett nytt system att rutinerna funkar.*

Aditro (Visma) ekonomisystem *– Här pågår införandet av helt nytt system. Planeras vara klart kring årsskiftet 2018-19.*

Styrdokument efterlevs samt omprövas

Nya Vägledande Råd Och Bestämmelser är gjorda och anpassade efter nya Dataskyddsförordningen. Ärende hos Kommunstyrelsen den 4 december 2018. Dokumentet för Drift och förvaltning har utökats med ännu mer detaljerad och tydligare information för systemägare och systemförvaltarens ansvar. En mall för systemförvaltningsplan har gjorts och informerats om på gemensamt möte i december 2018.

Fastställda riktlinjer för behörigheter finns där ansvarig chef tilldelar behörigheter. Dessa rutiner och blankett finns på intranätet. Ett stort arbete med förbättrad säkerhet har genomförts som innebär att medarbetarens behörigheter stängs i och med sista anställningsdagen i kommunen har passerat. Centrala IT har också gjort en e-tjänst för beställning av behörigheter. Den är nästan klar och ligger ute för test. Förväntas kunna publiceras Q1 2019.

Under hela 2017 genomfördes en löpande internkontroll som omfattade alla de prioriterade systemen. Fokus låg på att kolla behörigheter och loggar. Dessutom gjordes internkontroller av Centrala IT på konsultkonton, VPN-koppling för distansarbetsplats, växelanknytningar, mobilabonnemang, surfmängder som också indirekt hör till behörigheter. Dessa kontroller görs hela tiden löpande. Frågan har under oktober 2018 tagits med ansvariga för internkontrollen för att få till ytterligare stående kontrollpunkter.

TIMRÅ KOMMUN
Kommunledningskontoret

Centrala IT har sedan 2010 gjort ett internt dokument som kallats ”Året som gått 20xx”. I detta dokument kommer från och med 2019 att införas rapport från varje förvaltning om vilka kontroller som genomförts hos dem. Dokumentet kommer framöver anmälas till KS som informationsärende.

Åtgärder	Genomförda
Nya VROB anpassade efter GDPR	KS 4 dec 2018
2 systemförvaltare	KLK v 43-44 2018
GDPR Handlingsplan	Uppdateras löpande från CIT. Lämnas till KS som informationsärende 4 dec 2018
Förteckning behandlingar	Uppdateras löpande
Personuppgiftsbehandlingsavtal	Skrivs löpande
Beställning behörigheter	Riktlinjer för grundbeställning finns på intranätet. Den styrs helt utifrån om du har en anställning eller inte. Utan den får man inte tillgång till andra system. E-tjänst är under utveckling och planeras vara klar och testad Q1 2019.
Information på decembers IT-råd/Rond	•Alla internkontroller som görs i systemen måste rapporteras till Informationssäkerhetssamordnaren senast 1 mars årligen •Riktlinjer för beställning av behörighet i respektive verksamhetssystem måste göras •Förvaltningsplan med budget, för vhtsystem •Systemdokumentation för vhtsystem •GAP-analys/LIS system – informeras nämnden något? •Enklare mall för riskanalys kommer användas i stället •Hur hanteras brister i den, handlingsplan? •Övervakning o larm i Teis för respektive VHTsystem? •Kraftförsörjning på respektive arbetsplats? Kommunikationsnivåerna på respektive arbetsplats?

TIMRÅ KOMMUN
Kommunledningskontoret

Dataskyddsförordningen efterlevnad

Timrå kommun har ett dataskyddsombud tillsammans med Ånge och Sundsvalls kommuner, samt deras bolag. Detta innebär ett gemensamt nätverk, att arbetssätt, riktlinjer osv är mycket lika i dessa kommuner. Vilket innebär att det är fler medarbetare som kommer med kloka inlägg så att eventuella risker upptäcks lättare.

Dataskyddssamordnaren för Kommunledningskontoret har under 2018 skapat en handlingsplan för det genomförda arbetet med införandet av dataskyddsförordningen. Detta dokument har skickats ut som ett stöd till samtliga förvaltningar, med ett tips om att göra ett liknande dokument för sin nämnd. Alla rutiner, riktlinjer och mallar samlas på intranätet. Handlingsplanen lämnas som informationsärende till Kommunstyrelsen i slutet av året.

Arbetet med nya dataskyddsförordningen är inget arbete som tar slut. Det är ständigt ett pågående arbete. Register som ska hållas aktuellt, personuppgiftsbiträdesavtal ska skrivas med leverantörer, incidenter ska anmälas, samtycken ska underhållas osv.

Under oktober/november 2018 har även kommunens dataskyddsombud genomfört revision hos nämnderna enligt Datainspektionens riktlinjer.