Göteborgs Stad

Tjänsteutlåtande
Utfärdat 2024-06-12
Diarienummer 0197/24

Handläggare
Fredrik Andersson
Telefon: 031-367 83 41
E-post: fredrik.andersson@intraservice.goteborg.se

Nämnden för Intraservices anvisning för informationssäkerhet

Förslag till beslut

I nämnden för Intraservice:

Intraservice anvisning för informationssäkerhet fastställs

Sammanfattning

Kommunfullmäktige fastställde i maj 2023 stadens riktlinjer för informationssäkerhet. I riktlinjen definieras två roller kopplat till informationssäkerhet dessa är informationsägare samt systemägare.

2023-02-22 § 43 uppdrog nämnden för Intraservice förvaltningen att ta fram en handlingsplan med tidplan för att omhänderta brister i kontrollområden som framkommer i dataskyddsenhetens årsrapport 2022.

Dataskyddsombuds årsrapport 2022 innehåller förbättringsförslag kopplade till de brister som årsrapporten redovisar gällande förvaltningens informationssäkerhetsarbete och följsamhet mot dataskyddsförordningen.

2023-06-01 startade projektet Etablera processer och arbetssätt tillhörande styrning och uppföljning av informationssäkerhet. Projektets mål är att omhänderta brister som redovisas i dataskyddsombuds årsrapport 2021 och 2022 och Stadsrevisionens rapport 2022 genom att etablera ett systematiskt informationssäkerhetsarbete.

I återrapporteringen till nämnden i ärende 0104/23 återges status på arbete, men också förslag på etablering av en informationssäkerhets- och dataskyddsorganisation inklusive förtydligande av roller och ansvar. Då vi ser dataskydd, skyddandet av personuppgifter, som en del av det totala informationssäkerhetsarbetet blir den anvisning som finns bilagd till detta TU ett första steg i att förtydliga roller och ansvar, gemensamma definitioner inom området samt hur undantag inom området informationssäkerhet skall hanteras. Anvisningen kommer också att bli paraply för alla de anvisningar och rutiner som är tänkta att ingå i ledningssystemet kring informationssäkerhet.

Bedömning ur ekonomisk dimension

Förvaltningens förslag till etablering av det som i dataskyddsombuds årsrapport 2023 benämns som dataskyddsorganisation innefattar förslag till ett antal åtgärder. Åtgärderna inkluderar att befintliga roller får utökade och nya ansvar kopplade till aktiviteter tillhörande dataskydd, arkivansvar, tekniskt arkivansvar, informationsägarskap, riskägarskap, systemägarskap, informationsklassning och riskhantering. Denna typ av ansvar utgör grunden till uppbyggnad av en organisationsstruktur med processer och arbetssätt som styr och stödjer arbetet med informationssäkerhet, och därinom dataskydd, arkivansvar och tekniskt arkivansvar. Åtgärderna har presenterats för Intraservice ledningsgrupp och chefer, och riskanalys har genomförts med ett perspektiv på arbetsmiljö. Riskanalysen har identifierat risk för att det finns åtgärder som behöver vidtas inom förvaltningen som medför kostnader kopplade till rekryteringsbehov. Fortsatt analys och framtagande av förslag till åtgärder kommer att ske under perioden juli – december, där även hänsyn tas till behovet av att ytterligare ansvar kopplas till roller inom förvaltningen. Ytterligare ansvar kopplade till det systematiska informationssäkerhetsarbetet.

Bedömning ur ekologisk dimension

Förvaltningen har inte funnit några särskilda aspekter på frågan utifrån denna dimension

Bedömning ur social dimension

I arbetet med att förankra de föreslagna ändringarna kring ansvar, roller och till dess knutna arbetssätt har riskanalys ur ett arbetsmiljömässigt perspektiv genomförts. Det arbetsmiljömässiga perspektivet kan delas in i två delar; social arbetsmiljö organisatorisk arbetsmiljö.

Social arbetsmiljö

Riskanalysen har identifierat risk för att personer som innehar roller som verksamhetschef, enhetschef och förvaltningsledare kan komma att uppleva negativ stress. Detta utifrån att dessa roller utifrån förslag om åtgärder får utökade och nya ansvar, respektive ökat antal arbetsuppgifter.

Organisatorisk arbetsmiljö

Riskanalysen har identifierat att det utifrån hur förvaltningen är organiserad idag finns risker kopplade till ledning och styrning och fördelning av arbetsuppgifter utifrån utökade och nya ansvar. Risker som ger svar om ett behov av ökat antal resurser.

Riskanalysen med perspektiv på arbetsmiljö påvisar även risker som finns idag, risker som kommer att finnas även efter att föreslagna åtgärder vidtagits. Det gäller risker tillhörande samverkan med andra myndigheter inom Göteborgs Stad. Riskerna avser otydlighet i ansvarsfördelning. Ett exempel på otydlighet i ansvarsfördelning tas även upp i dataskyddsombuds årsrapport; otydlighet kring vilka parter som är att anse som personuppgiftsansvarig, personuppgiftsbiträde, eller om det råder delat personuppgiftsansvar för de personuppgiftsbehandlingar som utförs inom Intraservices leveranser av gemensamma tjänster och digital infrastruktur. Ett annat exempel på otydlighet rör arkivansvaret kopplat till dessa leveranser.

Fortsatt analys och framtagande av förslag till åtgärder kommer att ske under perioden juli – december, där även hänsyn tas till behovet av att ytterligare ansvar kopplas till roller inom förvaltningen. Ytterligare ansvar kopplade till det systematiska informationssäkerhetsarbetet.

Samverkan

Samverkan sker med de fackliga representanterna i FSG 2024-06-19

Bilagor

Nämnden för Intraservices anvisning för informationssäkerhet

Ärendet

Utgå ifrån att det är kopplat till etablering av dataskyddsorganisation och beskriv de första stegen som tas med anvisningen

Beskrivning av ärendet

Bakgrund

Systematiskt informationssäkerhetsarbete är något som ska och bör ske på alla nivåer inom en organisation.

På strategisk, taktisk och operativ nivå i form av samordning, rådgivning, efterlevnad och verkställande. Det ställer krav på tydlighet i processer och arbetssätt samt roller och ansvar kopplat till detta. Det är inte något som sker vid sidan av ordinarie arbete utan skall vara en integrerad del av det ordinarie arbetet och de processer och arbetssätt som guidar medarbetarna.

Området regleras av flera olika lagar, till detta kommer stadenövergripande styrdokument som definierar vidare hur arbetet skall bedrivas inom organisationen. Ett av de styrande dokumenten är Göteborgs stads riktlinje för informationssäkerhet. I detta definieras två roller enligt nedan.

”Ansvar och roller i informationssäkerhet i enlighet med vad som gäller för övrig verksamhet, är ansvaret för informationssäkerheten kopplat till ordinarie verksamhetsansvar. Det innebär att ansvarig nämnd/styrelse för en verksamhet också är ansvarig för att informationssäkerheten upprätthålls och efterföljs i denna verksamhet.

Informationsägare är den nämnd/styrelse som ansvarar för den information som skapas och hanteras. Ansvaret för informationen och dess säkerhet följer med ansvaret för verksamheten.

Informationssägaren klassificerar och beslutar om informationshantering inom ramen för befintlig lagstiftning och verksamhetskrav.

Systemägare är den som har ett överordnat ansvar för administration, drift och säkerhet för ett system. Ett system kan innehålla information som tillhör en eller flera informationsägare.

Systemägaren ansvarar för att system uppfyller lagkrav och verksamhetskrav som fastställts av informationsägare.”

Utöver definitionen av rollerna beskrivs också ett antal ansvar kopplat till rollerna kring områden så som organisatoriska, tekniska, fysiska och personella skyddsåtgärder.

Roller och ansvar

För att skapa förutsättningar för detta ansvar och arbete som det innebär behöver förvaltningen ha en inbyggd systematik kring informationssäkerhet. Detta i form av en tydlig informationssäkerhets- och dataskyddsorganisation med tillhörande ledningssystem som beskriver hur arbetet knyts an till ordinarie uppdrag att leverera gemensamma tjänster och digital infrastruktur till staden. Det krävs också en tydlighet vilket ansvar som ligger på ordinarie roller inom organisationen. Utifrån detta tydliggör anvisningen det ansvar som ligger på verksamhetschefer och enhetschefer specifikt kopplat till

informationssäkerhet. Detta blir komplement till de befattningsbeskrivningar beskriver övrigt ansvar som chef.

Det finns andra roller som får förtydligat ansvar, i första versionen fokuserar detta på förvaltningsledare, systemförvaltare och medarbetare. I arbetet vidare i projektet och i samarbete med liknande arbete inom förvaltningen kan ytterligare roller behöva beskrivas och befintliga kompletteras.

För att stötta förvaltningens medarbetare och chefer i det systematiska informationssäkerhetsarbetet kommer det finnas utpekade informationssäkerhetsamordnare. Detta är medarbetare med uppdrag att ta fram de styrande dokument och anvisningar som gäller för området samt stötta de medarbetare som skall genomföra arbetet. Informationssäkerhetssamordnarna kommer också ha ansvar som dataskyddskontakt för organisationen och i detta stötta och agera kontaktyta mot förvaltningens dataskyddsombud.

Informationssäkerhetssamordnarna är samlade i den föreslagna informationssäkerhets- och dataskyddsfunktion som föreslås, och leds och samordnas av förvaltningens CISO.

CISO rollen får också ett tydligare uppdrag och med det ansvar kopplat till sig som ansvarig för det ledningssystem för informationssäkerhet som tas fram.

Definitioner

För att undvika missförstånd i arbetet finns behov av ett gemensamt språkbruk, av den anledningen finns en definitionslista framtagen och är en del av anvisningen. Denna har sin utgång i vedertagna standarder och följer både INERA och MSB. Den kommer att kompletteras vid behov och samordnas med andra begrepp inom förvaltningen. Detta för att säkerställa att rätt begrepp används men också att de har samma betydelse överallt.

Undantag

I informationssäkerhetsarbetet kan situationer uppstå när tidsbegränsade undantag kan behöva ske. För att se till att detta hanteras på ett korrekt sätt behöver det finnas en tydlighet som vem som får fatta beslut och vilka förutsättningar som gäller för att beslut skall kunna tas. Det handlar om hur undantaget skall dokumenteras, vem som ansvarar för uppföljning av att undantaget och vilka planer som finns för att undantaget inte längre skall behövas.

Tekniskt arkivansvar

Informationssäkerhet skall beaktas genom hela livscykeln för informationen, från att den skapas, hanteras, distribueras till att den till slut antingen bevaras eller gallras. Detta påvisar en stark koppling till arkivering och det ansvar som förvaltningen fått av arkivnämnden i form av tekniskt arkivansvar[1].

Samråd har genomförts med Regionarkivet på tjänstepersonsnivå för att få bild över hur arbetet skulle kunna organiseras. Genom samråd och dialog har bland annat följande uppgifter identifierats ligga inom förväntade leveranser som tekniskt arkivansvarig.

[1] *2 kap. 19 § Göteborgs Stads föreskrifter och riktlinjer om arkiv- och informationshantering*

- ansvar för att bevara, verkställa gallring och leverera information som hanteras och förvaras i IT-lösningen, på uppdrag av arkivbildaren/informationsägaren
- val av lagringsmetod och skydd för lagrad information, exempelvis konvertering till arkivgodkända format
- att säkerställa att Arkivnämndens krav för arkivering följs vid upphandling eller utveckling av IT-lösningar
- samordning av leveransarbete till mellanlagringstjänster och system för bevarande
- kontakter med leverantörer när det gäller systemfunktioner som berör arkiveringen
- att upprätta den plan för bevarande av elektroniska handlingar som avses i 4 kap. 25 § Föreskrifter och riktlinjer om arkiv- och informationshantering på egen hand eller tillsammans med arkivbildaren/informationsägaren
- att lämna ut information ur IT-lösningen till den myndighet som äger informationen om den inte har direktåtkomst till informationen. I det tekniska arkivansvaret ingår inte det som varje myndighet ansvarar för.

Intraservice har två perspektiv kopplat till arkivhantering. Dels den som skall ske utifrån det egna förvaltningsarbetet. Här kommer ansvar att placeras hos kanslichef. Det andra perspektivet är utifrån leverantör av gemensamma tjänster och digital infrastruktur till stadens förvaltningar och bolag. Här föreslås Intraservices CISO utses till tekniskt arkivansvarig och de informationssäkerhetssamordnare som finns inom förvaltningen också få ansvar som teknisk arkivsamordnare. Dessa kommer sedan att stötta primärt förvaltningsledare som har det mer operativa ansvaret för att se till att planera för arkivhantering inom alla de tjänster som förvaltningen levererar.

Fortsatt arbete

I och med fastställande av anvisning för informationssäkerhet tas första steget mot att ska de förutsättningar för systematiskt informationssäkerhetsarbete som krävs för att svara upp mot revisionsrapporternas kritik men också att möta förändringar inom området utifrån kommande lagar och styrande dokument. Då projektet pågår fram till 2026 kommer anvisningen uppdateras kontinuerligt i de fall vi ser behov av att tydliggöra andra rollers ansvar och mandat när det gäller att realisera nämndens uppdrag kring informationssäkerhet.

Förvaltningens bedömning

För att en organisation skall kunna sägas ha ett systematiskt informationssäkerhetsarbete bygger det på flera delar. Tydliga och etablerade processer, arbetssätt där säkerhet är inbyggt och en tydlighet kring vilket ansvar som ligger på medarbetare och chefer i organisationen. Genom att börja skapa tydlighet kring rollerna och vilka ansvar som finns på varje roll skapar vi förutsättningar att bygga vidare på det ledningssystem som till slut ligger till grund för systematiskt informationssäkerhetsarbete. Här ser förvaltningen denna anvisning som en startpunkt och förutsättning för det fortsatta arbetet.

Stina Hall Hellqvist
Avdelningschef för styrning och stöd

Peter Söderström
Förvaltningsdirektör