Landstingsstyrelsens förvaltning
Informationssäkerhet

TJÄNSTEUTLÅTANDE
2014-02-18

LS 1311-1449

Handläggare:
Vesna Lucassi

Landstingsstyrelsens
arbetsutskott

Genomlysning av rutiner, direktiv och policy om informationssäkerhet

Ärendebeskrivning

Arbetsutskottet gav i slutet av år 2013 landstingsdirektören i uppdrag att genomföra en genomlysning av rutiner, direktiv och policy om informationssäkerhet. I tjänsteutlåtandet rapporterar landstingsdirektören genomlysningen och de aktiviter som är kopplade till uppdraget.

Beslutsunderlag

Landstingsdirektörens tjänsteutlåtande den 18 februari 2014

Förslag till beslut

Arbetsutskottet föreslås besluta

att godkänna återrapporteringen.

Förvaltningens förslag och motivering

Sammanfattning
I slutet av år 2013 gav arbetsutskottet landstingsdirektören i uppdrag att göra en genomlysning av rutiner, direktiv och policy om informationssäkerhet (LS 1311-1456). Stockholms läns landsting står inför stora satsningar både inom trafik och inom vård. För att uppnå satta mål och hålla en god informationssäkerhet som står i paritet med kommande utmaningar är det nödvändigt att landstinget har en god styrning av och tydliga arbetssätt för informationssäkerheten i verksamheten. Landstingsdirektörens genomlysning pekar på de centrala områden till vilka är kopplade rutiner, direktiv och policy, och pekar ut de förbättringar som behöver genomföras under år 2014.

Bakgrund
Informationssäkerhet är idag en stor utmaning, både nationellt och globalt. Den snabba IT-utvecklingen, komplexa systemberoenden och ökad informationsdelning påverkar alla samhällsprocesser och ställer allt högre krav på informationshantering. Samtidigt innebär den höga förändringstakten och behovet av exponering mot internet att hotbilden ständigt förändras. Under de senaste åren har hotbilden kopplad till informationssäkerhet kraftigt ökat i samhället och de ekonomiska konsekvenserna av incidenterna ökar. En tydlig styrning och uppföljning av informationssäkerhetsarbetet inom landstinget är därför en nödvändighet. Arbetsutskottet gav den 5 november 2013 landstingsdirektören i uppdrag att genomföra en genomlysning av landstingets rutiner, direktiv och policy om informationssäkerhet.

Överväganden
Stockholm läns landsting ansvarar för den offentligt finansierade hälso- och sjukvården, kollektivtrafiken, regionplaneringen och andra viktiga uppgifter i Stockholms län. Verksamheten är omfattande och komplex, med många olika intressenter och med ett stort beroende av information. En effektiv och säker användning av information är en förutsättning för landstingets verksamhet och för förtroendet för förmågan att leverera service till medborgarna. För att uppnå satta mål och samtidigt säkerställa säkerheten i olika perspektiv, t.ex. patientsäkerhet och patientintegritet, i en komplex och integrerad miljö där IT är verksamhetskritisk, krävs att landstinget har en tydlig styrning av sin informationssäkerhet. Nödvändigheten av att skydda landstingets information varierar för olika typer av information och processer.

Arbetet med informationssäkerhet inom landstinget styrs genom lagbestämmelser och regler, där de grundläggande kraven på skydd anges i landstingets styrdokument för informationssäkerhet. Skydd av landstingets information uppnås främst av att verksamheterna uppfyller de i styrdokumenten fastställda kraven.

I början av år 2013 antog landstingsfullmäktige och landstingsstyrelsen en ny informationssäkerhetspolicy och nya riktlinjer för informationssäkerhet (LS 1112-1733). Landstingets informationssäkerhetspolicy är baserad på bl.a. standarderna i SS-ISO/IEC 27000-serien. I policyn anges att målet för landstingets informationssäkerhetsarbete är att skydda informationen inom verksamheten, och att skyddet ska vara anpassat till skyddsvärde, risk och lagkrav och därigenom möjliggöra för landstingets verksamheter att uppnå sina mål. I policyn anges de principer som ska gälla vid val av relevant

skyddsnivå. Dessa principer förtydligas i riktlinjerna, men behöver konkretiseras ytterligare för att öka regelefterlevnaden.

Arbete pågår därför med att ta fram konkretiserande tillämpningsanvisningar för hälso- och sjukvården samt för övrig verksamhet. Detta planeras bli klart under år 2014. För att åstadkomma en tydligare styrning av informationssäkerheten kommer exempelvis momentet "ledningens genomgång" införas, en obligatorisk, regelbundet återkommande del som ingår i standarden för informationssäkerhet. Momentet, som blir obligatoriskt för samtliga bolag och förvaltningar inom landstinget, syftar till att säkerställa ledningssystemets fortlöpande lämplighet, tillräcklighet och verkan. Förtydliganden kommer även införas gällande exempelvis klassificering av information, riskanalys och hanteringsregler för information såsom patientuppgifter inom hälso- och sjukvården.

I anslutning till beslutet om nya styrdokument för informationssäkerhet byggdes strukturen i landstingets ledningssystem för informationssäkerhet om. I de landstingsövergripande målen för år 2014, som är fastställda av landstingsfullmäktige, finns en indikator för informationssäkerhet. Indikatorn ger möjlighet till en landstingsövergripande målstyrning för informationssäkerhetsarbetet och alla förvaltningar och bolag ska följa upp samt rapportera sitt arbete i årsbokslutet.

Under år 2014 kommer ett förslag på handlingsprogram för informations-säkerhet att tas fram, som kommer syfta till att säkerställa ett strukturerat och långsiktigt arbete inom landstinget. Handlingsprogrammet kommer att kompletteras med en kommunikationsplan för informationssäkerhet.

Ett antal utvecklingsarbeten är påbörjade och bedrivs i nära samverkan med landstingets verksamheter. Det mest övergripande av dessa är den samlade inriktningen för landstingets informationssäkerhetsarbete som innefattar stöd för regelefterlevnad och riskbedömning. Arbete pågår med att införa ett process-stöd för systematiskt informations-säkerhetsarbete, s.k. compliance management, för kravställning, kontroll av regelefterlevnad och riskhantering. Processen förväntas bidra till ett decentraliserat och systematisk arbetssätt inom landstinget, samt till att viktiga informationssäkerhetsfrågor hanteras och följs upp på ett bättre och mer strukturerat sätt. Det förväntas även bidra till att landstingets informationssäkerhet kan följas upp och rapporteras genom nyckeltal.

Under år 2013 inträffade ett antal uppmärksammade IT-relaterade incidenter. Förbättringsområden har identifierats för att förebygga och

säkerställa en effektiv hantering av framtida it-säkerhetsincidenter. Ett av behoven som har identifierats är en ökad tydlighet i besluts- och kommunikationskedjorna gällande IT-säkerhetsrelaterade incidenter. Åtgärder planeras genomföras bl.a. genom att införa en ökad tydlighet i de till riktlinjerna hörande tillämpningsanvisningarna för informationssäkerhet. En ökad tydlighet behöver införas även i landstingets krishanteringsplan som är beslutad av landstingsfullmäktige, liksom i kriskommunikationsplanen, som är beslutad av landstingsstyrelsen (LS 0902-0185). I arbetet med att uppdatera dessa är det angeläget att informationssäkerhetsperspektivet omhändertas fullt ut.

Väsentliga informationssäkerhetsindicenter rapporteras via landstingets informationssäkerhetschef till landstingsdirektören i enlighet med gällande rutiner. Under året har rapporteringsvägar och arbetssätt förtydligats och förbättrats och kommer stärkas ytterligare genom de aktiviteter som beskrivits i landstingsdirektörens genomlysning.

Ekonomiska konsekvenser av beslutet

Det uppstår inga ekonomiska konsekvenser av beslutet. Kostnaderna för ovan beskrivna aktiviteter ryms inom ordinarie budget.

Miljökonsekvenser av beslutet

I enlighet med landstingets Miljöpolitiska program 2012-2016 har hänsyn till miljön beaktats och slutsatsen är att det inte är relevant med en miljökonsekvensbedömning i detta ärende.

Toivo Heinsoo
Landstingsdirektör

Anders Nyström
Biträdande förvaltningschef