Fastighets- och servicenämnden
Serviceförvaltningen

TJÄNSTEUTLÅTANDE
2026-04-29

FSN 2026–0304

Fastighets- och
servicenämnden

Svar på skrivelse av Fredrik Wallén (KD) avseende att införa globala standarden för ledningssystem för informationssäkerhet

Ärendebeskrivning

Fredrik Wallén (KD) har lämnat en skrivelse till fastighets- och servicenämnden avseende att införa den globala standarden för ledningssystem för informationssystem för informationssäkerhet.

Beslutsunderlag

Förvaltningschefens tjänsteutlåtande

Förslag till beslut

Fastighets- och servicenämnden beslutar följande.

1. Skrivelse av Fredrik Wallén (KD) avseende att införa globala standarden för ledningssystem för informationssäkerhet anses besvarad med hänvisning till förvaltningschefens tjänsteutlåtande.

Förvaltningens förslag och motivering

Sammanfattning

Fredrik Wallén (KD) har den 25 mars 2026 inkommit med en skrivelse till fastighets- och servicenämnden med förslag om att införa den globala standarden ISO/IEC 27001 för ledningssystem för informationssäkerhet (ISMS). I skrivelsen föreslår Kristdemokraterna att fastighets- och servicenämnden att besluta om att ge förvaltningschef vid serviceförvaltningen i uppdrag att utreda och ta fram förslag på hur Region Stockholm eller relevanta utförande verksamheter ska certifieras enligt internationell standard som bekräftar att vi systematiskt hanterar och skyddar information genom ett ledningssystem för informationssäkerhet (ISMS).

Fastighets- och servicenämnden konstaterar att det regionövergripande ansvaret för informationssäkerhet är placerat på regionstyrelsen. Nämnden har ansvar för den tjänsteleverans som sker inom serviceverksamheten och

för eget arbete med informationssäkerhet. Anvisningar som rör andra nämnder kan inte utfärdas av fastighets- och servicenämnden.

Region Stockholm ledningssystem bygger på de gemensamma standarderna, samt att det finns såväl självskattning från nämnderna som uppsikt från regionstyrelsen som fyller den roll en extern certifiering har för andra organisationer. Såväl regionstyrelsen som fastighets- och servicenämnden bedömer att en utomstående certifiering medför ökade kostnader och utökad administrativ börda utan att självklart leda till ökad informationssäkerhet.

Däremot avser förvaltningen att framgent på ett tydligare sätt involvera nämnden i beslut om ledningssystem och regelbunden återkoppling om arbetet inom området.

Bakgrund
Fredrik Wallén (KD) har den 25 mars 2026 inkommit med en skrivelse till fastighets- och servicenämnden med förslag om att införa den globala standarden ISO/IEC 27001 för ledningssystem för informationssäkerhet (ISMS). Av skrivelsen framgår bland annat att:

” (…) Revisionskontoret har granskat IT-säkerhetsarbetet i regionens nätverksmiljö med fokus på hantering av rekommendationer om skyddsåtgärder. Revisionskontorets har identifierat flera brister och bedömer att akutsjukhusnämnden behöver stärka sin styrning och kontroll för att säkerställa att CERT:s identifierade IT-relaterade risker åtgärdas i tid, och bedömer vidare att fastighets- och servicenämnden bör stärka sina processer kopplade till meddelanden från CERT. /…/. ISO 27001 är den globala standarden för ledningssystem för informationssäkerhet (ISMS). Den beskriver hur du systematiskt kan arbeta med att identifiera, hantera och minska risker kopplade till information och IT-system. Standarden är framtagen av ISO och IEC och används av företag, kommuner och organisationer världen över. Syftet med ISO/IEC 27001 är att skapa ett tryggt ramverk för att skydda information mot obehörig åtkomst, manipulation och förlust.

Mot denna bakgrund föreslår Kristdemokraterna i sin skrivelse att fastighets- och servicenämnden beslutar:

1. Uppdra åt chefen för serviceförvaltningen att utreda och ta fram förslag på hur Region Stockholm eller relevanta utförande verksamheter ska certifieras enligt internationell standard som

bekräftar att vi systematiskt hanterar och skyddar information genom ett ledningssystem för informationssäkerhet (ISMS).”

Överväganden
I skrivelsen omnämns såväl akutsjukhusnämnden som fastighets- och servicenämnden. I relation till detta har fastighets- och servicenämnden endast möjlighet att yttra sig i förhållande till nämndens ansvarsområde. Utifrån detta kan konstateras att Region Stockholm har ett övergripande ledningssystem för informationssäkerhet enligt Region Stockholms riktlinje för informationssäkerhet och dataskydd (RS 2025–0418). Riktlinjen och tillhörande metodstöd gäller för hela Region Stockholm och är anpassad efter ISO/IEC 27000-serien och omfattar i huvudsak de krav som ställs i ISO/IEC 27001 samt tillämplig lagstiftning, inklusive den nya cybersäkerhetslagen (2025:1506) om att uppnå en hög nivå av cybersäkerhet i samhället. Riktlinjen är även anpassad efter Region Stockholms styrningsstruktur enligt policyn för ledning och styrning.

Region Stockholm har valt att inte certifiera det regionövergripande ledningssystemet för informationssäkerhet enligt ISO 27001, trots att ledningssystemet bygger på ISO 27001. Skälet till att Region Stockholm valt att inte certifiera sig, det vill säga att inte låta en oberoende part (certifieringsorgan) granska och bekräfta att arbetssätt, processer och rutiner uppfyller standardens krav är att minska den administrativa bördan samt att i stället styra resurser till införandet av skyddsåtgärder som bidrar till ökad informations- och cybersäkerhet.

Granskning och bekräftelse sker i stället genom intern kontroll och uppföljning enligt Region Stockholms process och verktyg för regelefterlevnad och interna resurser, däribland respektive förvaltnings informationssäkerhetssamordnare. Utifrån gällande riktlinje har regionstyrelsen också ett särskilt utpekat ansvar för uppsikt över samtliga nämnders arbete med informationssäkerhet för analys, ledning och samordning inom området.

Serviceförvaltningen har, inom ramen för Region Stockholms övergripande ledningssystem för informationssäkerhet och dataskydd, etablerat ett lokalt anpassat ledningssystem i syfte att säkerställa ett strukturerat, enhetligt och systematiskt arbete med informationssäkerhet (FSN 2024–0213).
Sedan det lokala ledningssystemet fastställdes har Region Stockholm genomfört revideringar av den övergripande riktlinjen. Mot denna bakgrund planeras en översyn och uppdatering av det lokalt anpassade

ledningssystemet i syfte att säkerställa fortsatt överensstämmelse med gällande styrdokument. Arbetet kommer att återrapporteras till nämnden.

Förvaltningen delar i övrigt Region Stockholms bedömning, att extern certifiering av serviceförvaltningens lokala ledningssystem inte är nödvändig, eftersom såväl självskattning som uppsikt genomförs inom ramen för den tillsyn som regionstyrelsen bedriver. Detta sker utan det dubbla uppföljningsarbete som en extern certifiering skulle medföra. En sådan certifiering har sitt primära värde om en organisation återkommande behöver kunna uppvisa externt att det finns ett fungerande informationssäkerhetsarbete, exempelvis för att man återkommande deltar i anbudsprocesser där detta är ett krav. Skrivelsen anses härmed besvarad.

Miljömässiga och/eller sociala konsekvenser
Beslutet i enlighet med förvaltningschefens tjänsteutlåtande bedöms inte medföra några miljömässiga eller sociala konsekvenser.

Ekonomiska konsekvenser
Beslut i enlighet med förvaltningschefens tjänsteutlåtande bedöms inte medföra några ekonomiska konsekvenser.

Stefan Schildt
Förvaltningschef

Beslutsexpediering:
Akt