



Svar till Inspektionen för vård och omsorg IVO

Bakgrund

IVO genomförde 21:a november 2019 en tillsyn vid stadsdelsnämnden Örgryte Härlanda avseende stadsdelsnämndens systematiska informationssäkerhetsarbete i egenskap av leverantör av samhällsviktig tjänst inom hälso- och sjukvårdssektorn enligt NIS (Europaparlamentets och rådets direktiv (EU) 2016/1148 av den 6 juli 2016 om åtgärder för en hög gemensam nivå på säkerhets- och informationssystem i hela unionen)

IVO konstaterar i sitt beslut daterat 2020-02-28 Dnr 8.5-33807/2019-13 att de ”anser att Örgryte Härlanda stadsdelsnämnd inte bedriver något systematiskt och riskbaserat informationssäkerhetsarbete. IVO har identifierat följande brister vid tidpunkten för inspektionen.”

- Örgryte Härlanda stadsdelsnämnd har inte genomfört någon övergripande riskanalys och hade inte någon plan för genomförandet av en övergripande riskanalys som ska utgöra grund för beslut om lämpliga säkerhetsåtgärder.
- Ledningens och övriga organisationens ansvar för det systematiska informationssäkerhetsarbetet är inte tydliggjort i tillräcklig omfattning.
- Örgryte Härlanda stadsdelsnämnd bedriver inte informationssäkerhetsarbetet enligt internationella standarder.

IVO begär att nämnden redovisar sin inställning till de konstaterade bristerna. Redovisningen ska även innehålla de eventuella åtgärder som nämnden har vidtagit eller planerar att vidta för att komma tillrätta med bristerna. Redovisningen ska avslutas med uppgifter om när åtgärden genomfördes eller kommer att genomföras.

Stadsdelsnämnden Örgryte-Härlandas inställning till de konstaterade bristerna

Stadsdelsnämnden har för avsikt att åtgärda samtliga brister som framkommit vid IVO:s inspektion. Detta arbete har påbörjats i februari 2020 och planeras att vara avslutat och redovisat till Stadsdelsnämnden i december 2020.

Nedan beskrivs de åtgärder nämnden har vidtagit eller kommer att vidta under de olika punkterna i IVO:s beslut.

Stadsdelen genomför inte en årlig riskanalys på övergripande nivå.

Inspektionen gäller specifikt samhällsviktiga tjänster inom Hälso- och sjukvården. Eftersom stadsdelsnämnden är ansvarig för fler verksamheter är de åtgärder som nu genomförs riktade till alla stadsdelens verksamheter.

När det gäller arbetet med utbildning, informationsklassning och riskanalys tog förvaltningen under våren 2019 fram en planering för detta. Detta utifrån den kritik stadsrevisionen riktade mot hur förvaltningen arbetade med informationssäkerheten. Detta arbete var inte möjligt att genomföra som planerat under hösten 2019 och kom inte igång förrän efter årsskiftet 2020.

Under 2020 har förvaltningen startat ett arbete med att genomföra en informationsklassning, informationsvärdering och riskanalys utifrån samtliga kriterier som anges av IVO och som framgår av lagstiftningen det vill säga:

- Tillgänglighet
- Konfidentialitet
- Riktighet
- Spårbarhet

Åtgärden innebär att förvaltningens säkerhetsansvarige träffar samtliga enhetschefer i förvaltningen vid tre till fyra tillfällen:

Tillfälle 1 – utbildning i informationssäkerhet, vad det innebär, vilket ansvar som åvilar olika nivåer i organisationen, vad lagstiftningen säger. Enhetscheferna ges då också ett uppdrag att inventera sina informationstillgångar. Tillfälle ett genomförs under våren och hösten 2020.

Tillfälle 2 – workshop för att tillsammans genomföra en informationsklassning och värdering av informationstillgångarna. Tillfälle två genomförs under våren och hösten 2020.

Tillfälle 3 – workshop för att tillsammans genomföra en riskanalys och ta fram förslag på åtgärder. Om det är möjligt, ta fram en åtgärdsplan vid detta tillfälle. Annars genomförs detta vid tillfälle fyra. Tillfälle tre och fyra genomförs senare under hösten 2020 (oktober - november).

Åtgärdsplanen kommer att sammanställas och dokumenteras på den förvaltningsövergripande nivån och redovisas till stadsdelsnämnden på sammanträdet i december. Av åtgärdsplanen kommer det att framgå när det är lämpligt att uppföljning sker.

Göteborgs stad organiserar om sina nämnder inom delar av välfärdssektorn den 1 januari 2021. Det innebär att stadsdelsnämnderna avvecklas och verksamheten övergår till nya nämnder. Det kommer att inrättas en nämnd för äldreomsorg och hälso- och sjukvård, en nämnd för funktionsstöd och en eller flera nämnder för individ och familjeomsorg. Eftersom uppföljning av åtgärdsplanen inte kan genomföras förrän tidigast under hösten 2021 kommer denna fråga att behöva lämnas över till de nämnder som ska ansvara för verksamheten i framtiden.

Detaljerad tidplan framgår av bilaga 1

Ledningens och organisationens ansvar för det systematiska informationssäkerhetsarbetet är inte tydliggjort

Utifrån inspektionen menar IVO att det inte finns ”någon sakkunnig eller stödfunktion på central nivå dit stadsdelen kunde vända sig med informationssäkerhetsfrågor”. Detta

måste bero på ett missförstånd eftersom det vid inspektionen och i samband med de synpunkter förvaltningen lämnade i faktagranskning fördes ett resonemang kring det stöd som finns att få från Stadsledningskontoret och informationssäkerhetschefen där Jan A Svensson.

Förvaltningen har arbetat med att förtydliga ledningens och övriga organisationens ansvar för det systematiska informationssäkerhetsarbetet (bilaga 2), detta dokument är beslutat av stadsdelsdirektören.

Vid inspektionen framförde företrädare för stadsdelen att stadens organisation innebär att stadsdelsnämnden inte själv äger alla de system som hanterar information. Detta var i huvudsak en beskrivning av hur Göteborgs stad är organiserad. Stadsdelsnämndens myndighetsansvar är reglerat i det reglemente som finns för stadsdelarna och som är beslutat av kommunfullmäktige. Stadsdelsorganisationen innebär att det finns ett behov av stöd och samordning från staden centralt. I detta sammanhang är nämnden för Intraservice den enda möjliga tjänsteleverantören. Det finns i staden tydliga riktlinjer ”Göteborgs Stads generella regler för kommungemensamma interna tjänster” (bilaga 3) som beskriver ansvarsfördelningen mellan nämnden för Intraservice och stadsdelsnämnden, bland annat när det gäller att rapportera avvikelser och incidenter i de kommungemensamma systemen. Stadsdelsnämnden följer denna riktlinje och samarbetar tätt med nämnden för Intraservice.

Stadsdelen bedriver inte informationssäkerhetsarbetet enligt internationella standarder för informationssäkerhet

Förvaltningen har förtydligat dokumentet Örgryte-Härlandas riktlinjer för informationssäkerhet (bilaga 4), detta dokument är beslutat av stadsdelsdirektören.

Förvaltningens riktlinjer följer Göteborgs stads riktlinje för informationssäkerhet (bilaga 5). Som framgår av skrivelse från Göteborgs stads informationssäkerhetschef Jan A Svensson (bilaga 6) är stadens riktlinje uppdaterad i december 2019 i enlighet med gällande internationella standarder.

Med hänvisning till ovanstående bedömer förvaltningen att internationella standarder följs i förvaltningens informationssäkerhetsarbete.

Övrigt

Förvaltningen har i samband med förtydligandet av riktlinjen för informationssäkerhet (bilaga 4) daterat upp hänvisningen till gällande lagstiftning.