Södertälje kommun

SÖDERTÄLJE KOMMUN
Kommunstyrelsen
2017 -09- 13
Dnr | Rnr

14

TJÄNSTESKRIVELSE
2017-09-05
Kommunstyrelsens kontor

Kommunstyrelsen

KS 20170929

Informationssäkerhetspolicy

Dnr KS 17/256

Sammanfattning av ärendet

Informationssäkerhetsarbetet utgår i första hand från lagar, andra författningar och föreskrifter, men också från kommunens egna krav och ingångna avtal mellan kommunen och annan part. Information är en av kommunens viktigaste tillgångar och hanteringen av den är en viktig del i arbetet. Med informationstillgångar avses all information oavsett om den behandlas manuellt eller automatiserat och oberoende av dess form eller i vilken miljö den förekommer. Informationssäkerhet reglerar alltså inte bara hur vi arbetar med våra IT-baserade system utan gäller för alla former av information. Det är betydelsen av informationen som är styrande, inte systemen, organisationen eller tekniken. Med informationssäkerhet avses att vissa definierade krav säkerställs beroende på vilken information som avses.

Informationssäkerheten är en integrerad del av verksamheten. Alla som hanterar information och informationstillgångar har ett ansvar att upprätthålla informationssäkerheten. Det är också ett ansvar för chefer på alla nivåer att aktivt verka för en positiv attityd till informationssäkerhetsarbetet.

Policyn utgör högsta nivån i nedanstående styrande dokument som beskriver hur vi ska arbeta med informationssäkerhet. Strukturen är enligt följande;

- Informationssäkerhetspolicy. Beskriver den övergripande inriktningen.
- Anvisningar för olika användarkategorier som fastställs av Informationssäkerhetsansvarig. Detta tar sin utgångspunkt ifrån informationssäkerhetspolicyn.
- Tillämpningar, rutiner och checklistor. Dessa kan beslutas av Informationssäkerhetsansvarig, eller i samråd med denne av respektive kontor.

Informationssäkerhetspolicyn är utarbetad utifrån ett samarbete inom Kommunförbundet Stockholms Län (KSL) och baserade på riktlinjer från Myndigheten för Samhällsskydd och Beredskap (MSB), ISO standard 27001, samt de modeller som tillämpas av Stockholms stad och Stockholms läns landsting.
Förändringarna i aktuell uppdaterad policy innehåller en tillagd rubrik om uppföljning och revidering. I övrigt är det övergripande ansvaret för informationssäkerhet överfört från funktionen IT-strateg till säkerhetschef efter beslut av förre t f stadsdirektören per den 1 januari 2017.

Rollfördelning för informationssäkerhetsarbetet:

- Kommunstyrelsens kontor är övergripande ansvarigt för att samordna arbetet och följa upp tillämpning.
- Informationssäkerhetsansvarig är operativt ansvarigt för att driva och följa upp arbetet och skall bistå verksamheterna i informationssäkerhetsarbetet.
- IT-enheten utgör tekniskt stöd.
- Respektive kontor ansvarar för informationshantering och informationssäkerhet inom sitt respektive område.

Arbetet med informationssäkerhet ska integreras med det löpande arbetet när det gäller informationshantering samt i förekommande fall system- och informationsförvaltning.

Beslutsunderlag

Kommunstyrelsens kontors tjänsteskrivelse 5 september 2017
Bifogat förslag till uppdaterad Informationssäkerhetspolicy

Ekonomiska konsekvenser och finansiering

Arbetet med informationssäkerhet är en integrerad del av verksamheternas informations- och systemförvaltning. Eventuella utbildningsinsatser samt hanteringen av den nya dataskyddsförordningen, GDPR som vinner laga kraft 2018-05-25, hanteras i tilldelad budget under 2018.

Kommunstyrelsens kontors förslag till kommunstyrelsen:

1. Framlagt förslag till uppdaterad informationssäkerhetspolicy fastställs
2. Informationssäkerhetsansvarige i enlighet med Informationssäkerhetspolicyn ges i uppdrag att utarbeta och besluta om anvisningar och handledningar som bygger på informationssäkerhetspolicyn.

Rickard Sundbom
Stadsdirektör

Per Tegel
Säkerhetschef

Handläggare: Per Tegel
Säkerhetschef
Telefon (direkt): 08-523 03131
E-post: per.tegel@sodertalje.se

Södertälje kommun

Informationssäkerhetspolicy

Dokumentets syfte
Beskriver Södertälje kommuns arbete med informationssäkerhet på en övergripande nivå.

Dokumentet gäller för
Nämnder, kontor, verksamheter och medarbetare. I tillämpbara delar även för andra användargrupper som får tillgång till kommunens informationstillgångar genom användarkonton och liknande (t ex privata utförare, bolag, leverantörer, inhyrd personal eller andra användare av Södertäljes IT-miljö).

Information är en av Södertälje kommuns viktigaste tillgångar och hanteringen av den är en mycket viktig del i arbetet. Med informationstillgångar avses all information oavsett om den behandlas manuellt eller automatiserat och oberoende av dess form (muntlig, skriftlig, digital etc.), eller miljön den förekommer i. Informationssäkerheten omfattar kommunens alla informationstillgångar. Vi behöver skydda vår information på ett sätt som gör att allmänhet, uppdragsgivare, samarbetspartners och anställda har förtroende för vår verksamhet och våra sätt att hantera information.

Struktur

I denna *Informationssäkerhetspolicy* fastställer kommunstyrelsen Södertälje kommuns syn på informationssäkerhet samt övergripande mål och intentioner med kommunens informationssäkerhetsarbete.

Södertälje kommuns mål är att skydda och stödja alla medborgares intressen; kontinuiteten i verksamheten, samt möjliggöra samarbete både nationellt och internationellt. Information ska även vara tillgänglig i enlighet med medborgarnas behov, utifrån verksamhetens behov och i enlighet med grundlagen, samt gällande nationella och internationella bestämmelser. Informationssäkerhetspolicyn kompletteras med riktlinjer och anvisningar för olika grupper/ansvar som beskriver vad som måste göras för att uppfylla informationssäkerhetspolicyn. Sammantaget utgör dessa kommunens styrdokument för informationssäkerhet.

Informationssäkerhetsarbetet kännetecknas av att

- all information värderas efter sin känslighet och den som anses kritisk av verksamheten ska klassificeras efter den modell som finns
- det med administrativa och tekniska skyddsåtgärder säkerställs att informationen är tillgänglig när den behövs, att den är korrekt och att obehöriga inte kan få tillgång till informationen
- krav på spårbarhet uppfylls – det ska i efterhand kunna avgöras vem som tagit del av informationen, vilka förändringar som skett och av vem dessa utförts.
- kunskap finns om hur informationssäkerheten säkerställs
- krishanteringsförmågan fortlöpande analyseras och upprätthålls
- hotbilden mot vår information analyseras fortlöpande

- händelser som kan leda till negativa konsekvenser förebyggs, och
- arbetet med informationssäkerhet är en naturlig del i verksamheten

Organisation av informationssäkerhetsarbetet

- *Kommunstyrelsen* har det yttersta ansvaret för kommunens informationssäkerhetsarbete och uttrycker sin viljeinriktning genom kommunens informationssäkerhetspolicy.
- *Informationssäkerhets ansvarig* (i dagsläget är kommunens säkerhetschef av stadsdirektören utsedd att vara informationssäkerhets ansvarig) har det övergripande och strategiska ansvaret att leda, utveckla och samordna informationssäkerhetsarbetet bl.a. genom anvisningar. I uppdraget ingår även att genomföra oberoende informationssäkerhetsrevisioner inom verksamheten, samt att samordna kommunens personuppgiftsombud.
- *Informationsägarna* har det övergripande och yttersta ansvaret för den information som används inom en avgränsad verksamhet och att nödvändiga resurser avsätts för informationssäkerheten. Informationsägaren fattar de avgörande besluten om hur, av vem och vilken information som ska registreras samt om informationen behöver revideras och i vilken form informationen ska bevaras för att tillgänglighet, riktighet, sekretess och spårbarhet ska säkerställas över tid.
- För information som lagras eller bearbetas i IT-system har *systemägarna* ett övergripande ansvar för respektive system och hur information hanteras i systemet, samt systemets användning. System ska uppfylla informationssäkerhetskraven i förhållande till verksamhetens behov så som dess innehåll klassificerats enligt anvisningar för informationsklassificering.
- För information som lagras eller bearbetas i IT-system har *systemförvaltarna* det funktionella (dagliga) helhetsansvaret för ett system. Systemförvaltaren fungerar i hög grad som systemägarens utförare och ser till att systemets funktionalitet samt planerade och beslutade aktiviteter genomförs och upprätthålls.
- Chefer på alla nivåer har ett ansvar att dess medarbetare är medvetna om och lever upp till denna policy, samt skall aktivt verka för en positiv attityd till och förståelse för syftet med säkerhetsarbetet.
- Alla som hanterar informationstillgångar har ett ansvar för att informationssäkerheten upprätthålls.

Sanktioner

Hela den kommunala organisationen skall följa denna informationssäkerhetspolicy, samt de anvisningar som berör respektive individ. Det finns inte utrymme att fatta beslut som strider mot denna policy eller de centralt beslutade anvisningarna, vid behov kan särskilda anvisningar beslutas av informationssäkerhetsansvarig. Den som använder kommunens informationstillgångar på sätt som strider mot dessa och därigenom äventyrar informationssäkerheten kan bli föremål för disciplinära eller rättsliga åtgärder.

Anvisningar för verksamheten

Kommunstyrelsen ger kommunens informationssäkerhetsansvarige i uppdrag att utifrån denna beslutade informationssäkerhetspolicy dels utarbeta riktlinjer och dels anvisningar för de olika roller som finns inom Södertälje kommun, samt uppdrag att ta fram och löpande aktualisera anvisningar för bl.a. "IT-organisation, roller- och ansvar", "Anvisning för informationsklassning", "Handledning för risk- och sårbarhetsanalys" och "Anvisning för krishantering".

Uppföljning och revidering

Uppföljning och revidering av denna policy ska ske regelbundet. I samband med revideringska tillhörande riktlinjer och anvisningar samt handlingsplanen för informationssäkerhet revideras på motsvarande sätt.