Informationssäkerhet

Ledningens genomgång år 2024

Skärholmens stadsdelsförvaltning

Ledningens genomgång
Bilaga till Verksamhetsplan 2024
Dnr: 2023/1055
Kontaktperson: David Jansson

Ledningens genomgång är ett begrepp inom informationssäkerhet som syftar till att de som ansvarar för informationssäkerheten inom en organisation, minst årligen ska informera sig om hur arbetet går.

Enligt Stockholms stads tillämpningsanvisning för informationssäkerhet ska förvaltningschef inhämta en rapport, så kallad ”Ledningens genomgång” från informationssäkerhetssamordnaren. Rapporten bör exempelvis redogöra för om det finns lokala rutiner för incidenthantering, för utbildning av medarbetare eller om informationsklassningar och registerförteckning är genomförda.

Denna rapportering ska ge information och underlag till förvaltningschef att årligen bedöma om det lokala informationssäkerhetsarbetet och dataskyddsarbetet är tillräckligt och har önskad verkan. Förvaltningschefen ska ta upp aktiviteter som rör informationssäkerhet och dataskydd i verksamhetsplaneringen och i det interna arbetet med att uppnå tillräcklig intern kontroll.[1]

I *Anvisningar för nämndernas arbete med verksamhetsplan 2024*[2] uppmanas samtliga nämnder och bolagsstyrelser att ta fram en Ledningens genomgång med en planering för informationssäkerhetsarbetet under de kommande tre åren. Denna ska biläggas verksamhetsplan. Planeringen för de kommande tre åren ska utgå från nämndens verksamhetsuppdrag i budget och följa *Riktlinje för informationssäkerhet* i Stockholms stad.

Dessa aktiviteter ska redovisas både i Ledningens genomgång samt i nämndens verksamhetsplan under mål 3.5. Inventering och informationsklassning är grunden i informationssäkerhetsarbetet. För 2024 är därför området registerförteckning och informationsklassning särskilt prioriterat i Ledningens genomgång.

Alla nämnder ska prioritera att ta fram en plan för att inventera och klassa information som används i verksamheten alternativt se över och uppdatera genomförda klassningar.

[1] Tillämpningsanvisning till stadens riktlinje för informationssäkerhet
[2] anvisningar-for-namndernas-arbete-med-verksamhetsplan-2024.pdf (stockholm.se)

Innehållsförteckning

1. Ledningssystem för informationssäkerhet, LIS

Stockholms stads arbete med informationssäkerhet utgår från en så kallad ISO standard, ISO 27001. Det är en global standard för informationssäkerhet som hjälper organisationer att skydda sin känsliga information från hot och risker. Standarden ger ett ramverk för hur man implementerar ett ledningssystem för informationssäkerhet, LIS, som skyddar informationstillgångarna och ger en IT-process som är lättare att hantera, mäta och förbättra.

Stockholms stads informationssäkerhetsarbete regleras i en tillämpningsanvisning som är en bilaga till stadens Kvalitetsprogram[3]. Till riktlinjen finns tillämpningsanvisningar som är fastställda av stadsdirektören.

Tillämpningsanvisningarna reglerar ansvar och roller sett till Stockholms stads systematiska informationssäkerhetsarbete. För Skärholmens räkning kommer en så kallad lokal anvisning tas fram under 2024 som beskriver hur stadens övergripande ledningssystem för informationssäkerhet omhändertas inom förvaltningen.

1.1 Vad påverkar förvaltningens informationssäkerhetsarbete?

För att upprätthålla ett informationssäkerhetsarbete som är aktuellt över tid ska förvaltning ha ett riskbaserat förhållningssätt i sitt informationssäkerhetsarbete. Det innebär att verksamheten ska arbeta med att identifiera, bedöma och följa upp de informationssäkerhetsrisker som kan uppstå i verksamhetens informationshantering.

1.1.1 Finansborgarrådets förslag till budget 2024

Intern kontroll

Syftet med intern kontroll är att skapa förutsättningar för en ändamålsenlig och effektiv användning av skattemedel samt för att upprätthålla service med hög kvalitet till kommuninvånarna.

Genom en tillräcklig intern kontroll skapas förutsättningar att förebygga, upptäcka och åtgärda oönskade händelser och därmed minimera risker i verksamheten samt säkra tillgångar och förhindra förluster och oegentligheter som skadar stadens anseende. Arbetet med intern kontroll är en del av stadens kvalitetsarbete.

[3] Stockholms stads kvalitetsprogram (start.stockholm)

Utöver förvaltningens egna identifierade processer ska förvaltningen, enligt stadens anvisning, ha med den obligatoriska stadsövergripande processen *Systematiskt informationssäkerhetsarbete* i sin väsentlighets- och riskanalys och bedöma om de ska med i internkontrollplanen.

Förvaltningen har bedömt att två av de fem obligatoriska arbetssätten, *behörighetshantering, implementering av lokal anvisning, incidenthantering, informationsklassning* och *informationssäkerhet inom upphandlingsförfarandet,* ska ingå i intern kontrollplanen för 2024. De två arbetssätten är incidenthantering och informationsklassning.

1.1.2 Risk och sårbarhetsanalys

Stadens arbete med risk- och sårbarhetsanalys (RSA) bedrivs i en tvåårscykel. En ny cykel inleds under 2024.
Förvaltningen har i sin risk- och sårbarhetsanalys 2022 identifierat ett antal processer som är beroende av informationstillgångar, vilket har bäring på informationssäkerhet. För att tillse att processerna så långt som möjligt kan bedrivas även vid störningar i informationstillgångarna finns kontinuitetsplaner, vilka kontinuerligt förbättras. Förvaltningen följer stadens risk- och sårbarhetscykel och instruktioner.

1.1.3 Resultatet från egen uppföljning (IKP)

I förvaltningen tertialrapport 2 2023 rapporterades följande;

- Kontroll incidenthantering – lokal rutin saknas, stadsövergripande finns på intranätet.

- Kontroll informationsklassning – stickprov visade att informationsklassningsprotokollet för systemet Embrace var bristfällig och bör göras om.

- Kontroll informationssäkerhet inom upphandlingsförfarande – vid kontroll visade det sig att det inte alltid fungerar enligt rutin att involvera informationssäkerhetssamordnaren när så behövs vid upphandlingar.

I årets internkontrollplan ska kontroll göras av att alla upphandlingar har beaktat informationssäkerhetskrav. De stöddokument som används vid upphandlingar behöver förtydligas med punkter om informationssäkerhet. Ett arbete med att identifiera vilka delar i upphandlings- och avtalsprocessen som måste kompletteras med checklista för informationssäkerhet bör

genomföras. Denna checklista bör först införas i upphandlingsprocessen för att sedan införas i avtalsprocessen.

I syfte att förtydliga förvaltningens förteckning av personuppgiftsbehandling har den kompletterats enligt rekommendationer från dataskyddsombudet som denne lämnat i sin årsrapport för 2022.

1.1.4 Risker som identifierats i GDPR-årsrapport

Dataskyddsombudet har i senaste årsrapporten tagit upp följande som sina huvudsakliga rekommendationer:

- Involvera förvaltningens DSO och informationssäkerhetssamordnare i samband med upphandling av tjänster och system.

- Förstå vikten av konsekvensbedömning av personuppgiftsbehandlingar samt utse vem som ska hålla i konsekvensbedömningar.

- Fortsätt arbetet med registerförteckningen.

- En uppföljning av kunskapsläget inom dataskydd och informationssäkerhet behöver göras, samt repetition av de digitala utbildningarna på utbildningsplattformen.

- Nästa år planerar de europeiska dataskyddsmyndigheterna att granska dataskyddsombudens roll och ställning. Ett mycket välkommet initiativ som förhoppningsvis kommer att underlätta såväl för den som innehar rollen som DSO som den verksamhet DSO är satt att granska.

2.1 Förvaltningens lokala anvisning för informationssäkerhet

I förvaltningens Handlingsplan för informationssäkerhets- och dataskyddsarbete i Skärholmens stadsdelsförvaltning 2024-2026 finns fastslaget att en lokal anvisning för informationssäkerhet ska tas fram under 2024.

Enligt handlingsplanen ska förvaltningen även ta fram ett årshjul för arbetet med informationssäkerhet.

I samband med verksamhetsberättelse och bokslut tar förvaltningen del av dataskyddsombudets årsrapport och stor hänsyn tas till

eventuella rekommendationer till personuppgiftsansvarig som lämnas i rapporten.

3 Prioritering av åtgärder

3.1 Under 2024 ska Skärholmens stadsdelsförvaltning

Under 2024 ska förvaltningen prioritera;

- Informationssäkerhetssamordnaren ska ta fram och implementera årshjul för informationssäkerhet efter godkännande av förvaltningsledningen.
- Förvaltningens medarbetare ska genomföra utbildningar för grundläggande informationssäkerhet och dataskydd. På så vis främjas en säkerhetskultur inom organisationen
- Informationssäkerhetssamordnaren ska påbörja arbetet med att ta fram lokal anvisning av Riktlinje för informationssäkerhet
- Under 2023 påbörjade Dataskyddsombud (DSO) tillsammans med Grupp för informationssäkerhet och dataskydd en kartläggning som ska identifiera sina informationstillgångar och dokumentera detta i förvaltningens registerförteckning. Kartläggningen leder till en kunskap om vilken information som kan behöva genomgå en informationsklassning. Informationen ska sedan genomgå en riskanalys och därefter tas åtgärdsplaner, regler och riktlinjer fram under det fortsatta informationsklassningsarbetet.

3.2 Under 2025 ska Skärholmens stadsdelsförvaltning

Under 2025 ska förvaltningen prioritera;

- Informationssäkerhetssamordnaren ska leda och stötta arbetet med att göra årliga genomgångar av informationsklassningarna tillsammans med Grupp för informationssäkerhet och dataskydd. Under år 2025 kommer gruppen träffas med högre frekvens.
- Informationssäkerhetssamordnaren skapar en årlig rapport ‘Ledningens genomgång’ som överlämnas till förvaltningschef.
- Förvaltningens medarbetare ska genomföra utbildningar för grundläggande informationssäkerhet och dataskydd. På så vis främjas en säkerhetskultur inom organisationen

3.3 Under 2026 ska Skärholmens stadsdelsförvaltning

Under 2026 ska förvaltningen prioritera:

- Förvaltningens medarbetare ska genomföra utbildningar för grundläggande informationssäkerhet och dataskydd. På så vis främjas en säkerhetskultur inom organisationen
- Se över behov och revidera den lokala processen för hantering av informationssäkerhetsincidenter
- Informationssäkerhetssamordnaren skapar en årlig rapport ‘Ledningens genomgång’ som överlämnas till förvaltningschef.