Informationssäkerhet

- Ledningens genomgång år 2024

Stockholm Globe Arena Fastigheter AB

Ledningens genomgång
Bilaga till SGA Fastigheters Verksamhetsplan 2024
Dnr: 2023/74
Kontaktperson: Sara Feinberg

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 VD 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 VD att årligen bedöma om det lokala informationssäkerhetsarbetet och dataskyddsarbetet är tillräckligt och har önskad verkan. VD ska ta upp aktiviteter som rör informationssäkerhet och dataskydd i verksamhetsplaneringen och i det interna arbetet med att uppnå tillräcklig intern kontroll.

I *Anvisningar för arbete med verksamhetsplan 2024* 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 bolagets uppdrag i budget och följa *Riktlinje för informationssäkerhet* i Stockholms stad.

Dessa aktiviteter ska redovisas både i Ledningens genomgång samt i bolagets 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 och bolagsstyrelser ska prioritera att ta fram en plan för att inventera och klassa information som används i verksamheten alternativt se över och uppdatera genomförda klassningar.

Innehållsförteckning

1. Ledningssystem för informationssäkerhet, LIS 4
1.1 Vad påverkar SGAFs informationssäkerhetsarbete? 4
1.1.1 Finansborgarrådets förslag till budget 2024 4
1.1.2 Risk och sårbarhetsanalys 5
1.1.3 Penetrationstest 5
1.1.4 Risker som identifierats i GDPR-årsrapport 5
2.1 Förbättringar för verksamhetens LIS 6
2.1.1 SGAFs lokala anvisning för informationssäkerhet 6
3 Prioritering av åtgärder 6
3.1 2024 6
3.2 2025 6
3.3 2026 7

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. Till riktlinjen finns tillämpningsanvisningar som är fastställda av stadsdirektören, tillika VD för Stockholms Stadshus AB.

Tillämpningsanvisningarna reglerar ansvar och roller sett till Stockholms stads systematiska informationssäkerhetsarbete. För Stockholm Globe Arena Fastigheters (SGAF) räkning har VD fastställt en så kallad lokal anvisning som beskriver hur stadens övergripande ledningssystem för informationssäkerhet omhändertas inom bolaget

1.1 Vad påverkar SGAFs informationssäkerhetsarbete?

För att upprätthålla ett informationssäkerhetsarbete som är aktuellt över tid ska SGAF 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

Budgetuppdrag

SGAF har i budget 2024 som uppdrag, tillsammans med övriga verksamheter inom staden, att fortsätta öka beredskapsförmågan, exempelvis genom att analysera och hantera risker- och sårbarheter samt genom bl.a. systematiskt informationssäkerhetsarbete.

Intern kontroll

Enligt kommunfullmäktiges beslut ska bolagsstyrelser (och nämnder) i samband med att budget och verksamhetsplan utarbeta en internkontrollplan, baserad på risk- och väsentlighetsanalys samt risk- och sårbarhetsanalys.

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.

Utöver SGAFs egna identifierade processer ska bolaget, enligt stadens anvisning, ha med den obligatoriska stadsövergripande processen *Systematiskt informationssäkerhetsarbete* i sin väsentlighets- och riskanalys och bedöma vad som ska med i internkontrollplanen.

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

1.1.2 Risk och sårbarhetsanalys

Stadens arbete med risk- och sårbarhetsanalys (RSA) bedrivs i en tvåårscykel. En ny cykel inleds under 2024.

SGAF har i tidigare risk- och sårbarhetsarbete samt interkontrollplan, med tillhörande väsentlighet- och riskanalys, identifierat ett antal processer som kan ha risker inom informationssäkerhet och har kontroller och åtgärdsplaner för de delar som bolaget kan arbeta med.

1.1.3 Penetrationstest

SGAF genomförde 2021 ett penetrationstest av utvalda delar av IT-miljö tillsammans med säkerhetsföretag. Resultatet från det testet har legat till grund för det informationssäkerhetsarbete som SGAF därefter genomfört under de följande åren. I detta har PM3 och informationsklassning varit värdefulla verktyg.

1.1.4 Risker som identifierats i GDPR-årsrapport

Dataskyddsombudet har i årsrapporten för 2022 skrivit att *Det finns inga direkta brister i hantering eller rutiner. Bolaget hade under 2021 en fördjupad granskning från Stadsrevisionen gällande dataskydd. Granskningen visade att det finns utmaningar kopplade till DSO:s oberoende då denne är operativ vid bland annat uppdatering av registerförteckning. I en liten organisation är det ständiga utmaningar med att bemanna alla roller. Det beslutades då att arbetet fortsätter enligt tidigare då det anses fungerat tillfredsställande under förutsättningarna. Detta kan komma att ses*

över under 2023, genom att tillsammans med andra systerbolag undersöka möjligheten att anlita och dela på extern DSO.

Under 2023 har SGAF har tillsammans med ett antal systerbolag påbörjat upphandling av en gemensam DSO.

2.1 Förbättringar för verksamhetens LIS

2.1.1 SGAFs lokala anvisning för informationssäkerhet

I november 2023 fastställde VD Mats Viker SGAFs Lokala anvisning för informationssäkerhet. Anvisningen är diarieförd och finns tillgänglig för alla medarbetare på bolagets gruppdisk.

I samband med verksamhetsberättelse och bokslut tar styrelsen och bolagsledningen del av dataskyddsombudets årsrapport. Personuppgiftsansvarig tar hänsyn till eventuella rekommendationer som lämnas i rapporten.

3 Prioritering av åtgärder

3.1 2024

Bolaget ska under 2024 prioritera att:

- följa upp att den lokala anvisningen hanteras
- följa upp att incidenthanteringsrapporteringsrutinen hanteras
- fortsätta informationsklassningar med fokus på kritiska system enligt bolagets riskanalys
- fortsätta implementera förvaltningsorganisationer för de tekniska systemen enligt PM3
- arbeta enligt processer och kontroller i internkontrollplanen för 2024 gällande delar som rör informationssäkerhet
- fortsätta tillse att medarbetare genomfört stadens obligatoriska utbildningar i informationssäkerhet och dataskydd

3.2 2025

Under 2025 ska SGAF prioritera att:

- fortsätta klassning av bolagets informationstillgångar
- fortsätta arbetet med de tekniska systemen utifrån PM3-modellen
- öva och finjustera utifrån framtagna rutiner och planer för att kunna hantera incidenter

3.3 2026

Under 2026 ska SGAF prioritera att:

- fortsätta klassning av bolagets informationstillgångar
- Arbeta utifrån RSA framtagna riskanalysområden gällande informationssäkerhet
- Arbeta utifrån internkontrollplanens områden gällande informationssäkerhet

Fastställd av VD Mats Viker 2023-11-22