Stockholms stad

Ledningens genomgång år 2025

Stockholms Stadshus AB

Beslutad 2024-01-09
Reviderad [2024-11-19]

Ledningens genomgång

Dnr: SSAB 2024/194

Kontaktperson: Ingrid Storm

1 Vad är Ledningens genomgång?

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/bolagschef 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 och om informationsklassningar och registerförteckning är genomförda.

Denna rapportering ska ge information och underlag till förvaltningschef/bolagschef att årligen bedöma om det lokala informationssäkerhetsarbetet och dataskyddsarbetet är tillräckligt och har önskad verkan. Förvaltnings- och bolagschefer 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] samt i motsvarande *Anvisningar budget/VP 2024 koncernen Stockholms Stadshus AB* som tas fram till bolagen uppmanas samtliga nämnder och bolagsstyrelser ta fram en Ledningens genomgång med en planering för informationssäkerhetsarbetet för de kommande tre åren. Denna ska biläggas verksamhetsplanen. Planeringen för de kommande tre åren ska utgå från nämndens/bolagets verksamhetsuppdrag i budget och följa *Riktlinje för informationssäkerhet* i Stockholms stad.

I anvisningarna för budget/VP 2025 finns ingen motsvarande uppmaning men ledningens genomgång ska fortsatt tas fram enligt *Riktlinje för informationssäkerhet* och Funktionen för stadsövergripande informationssäkerhet på stadsledningskontoret. Enligt styrelsens arbetsordning föreläggs denna för koncernstyrelsen årets första ordinarie sammanträde.

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

Innehållsförteckning

2 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 Stockholms Stadshus ABs räkning har vice vd fastställt en lokal anvisning som beskriver hur stadens övergripande ledningssystem för informationssäkerhet omhändertas inom bolaget.

2.1 Vad påverkar Stockholms Stadshus ABs informationssäkerhetsarbete?

För att upprätthålla ett informationssäkerhetsarbete som är aktuellt över tid ska Stockholms Stadshus AB 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. Bolaget har ingen direkt operativ verksamhet gentemot medborgare, kunder, hyresgäster men hanterar information vad gäller styrning, stöd och uppföljning av bolagen inom koncernen. Bolaget använder nästan enbart stadens centralt upphandlade verksamhetssystem.

2.1.1 Omvärldsbevakning

Budgetuppdrag

- Moderbolaget Stockholms Stadshus AB har som uppgift att bl.a. svara för övergripande utveckling, strategisk planering, löpande översyn och omprövning, utöva ekonomisk kontroll och uppföljning, samt att utveckla styrformer och samspelet

[3] Stockholms stads kvalitetsprogram (start.stockholm)

mellan ägare, koncernledning och dotterbolag. I detta arbete samverkar bolaget med bland annat stadsledningskontoret vad gäller anvisningar och strategiska frågor inom informationssäkerhet. Samarbetet bör utvecklas den kommande treårsperioden.

- I budget 2024 hade samtliga förvaltningar och bolag i uppdrag att fortsätta öka beredskapsförmågan, exempelvis genom att analysera och hantera risker och sårbarheter samt genom krisledningsplanering, kontinuitetshantering, systematiskt informationssäkerhetsarbete, krigsorganisation samt årliga, obligatoriska krisledningsövningar. Detta uppdrag ligger kvar 2025.

- Moderbolaget ska delta i arbetet inom stadens sektorsorganisation för civil beredskap genom deltagande i de två sektorerna *energiförsörjning* och *finansiella tjänster* samt deltagande i deras motsvarande stadsövergripande beredskapsråd samt i styrgruppen för civil beredskap.

Övrigt

- NIS2-direktivet (Network and Information Systems Directive 2 - Cybersäkerhetslagen) kommer att genomföras i Sverige genom en lag som börjar gälla tidigast under sommaren 2025.

  NIS2 är en uppdatering av det tidigare NIS-direktivet. Stockholms Stadshus AB har inte omfattats av det tidigare NIS-direktivet men några bolag inom koncernen har gjort det.

  Syftet med NIS2 är att säkerställa en hög nivå av informationssäkerhet i hela EU genom att stärka skyddet av samhällsviktiga tjänster som en följd av den ökade digitaliseringen och hotbilden av cyberhot.
  Juridiska avdelningen på stadsledningskontoret har under 2024 tittat på frågan om kommunala bolag omfattas av NIS2. I utredningen anges att kommunen ”i dess helhet” ska omfattas av sektorn offentlig förvaltning, men att i de fall verksamheten bedrivs genom kommunala bolag är det inte kommunen som är verksamhetsutövare. För nämndernas och de kommunala bolagens del, omfattas samtliga förvaltningar inom staden i dess helhet samt de kommunala bolagen i de fall de anses vara verksamhetsutövare, som t.ex. S:t Erik Kommunikation AB för digital infrastruktur. Analys pågår

nu i stadens bolag kring om de omfattas av någon sektor. För vissa bolag är det tydligt att de omfattas utifrån att de tidigare träffats av NIS eller att kärnverksamheten ingår i någon av sektorerna i NIS2. Utmaningar i tolkningen består bland annat i tolkning av sektorer som digital infrastruktur och elektricitet där t.ex. fiber och solceller finns i vissa fastighetsbolag. Enligt analysen som gjorts hittills omfattas inte moderbolaget Stockholms Stadshus AB av någon av sektorerna.

- Centralt i staden pågår ett utvecklingsarbete med processen för leverantörsuppföljning av centrala avtal med fokus på informationssäkerhetsfrågorna.

- Årsredovisningslagen har under året anpassats till nya EU-direktiv om hållbarhetsredovisning. De nya kraven är väsentligt mer långtgående och kommer kräva utökade resurser men också mer insamling och redovisning av jämförbar och transparent data/information från dotterbolagen till bolagskoncernens redovisning. Systemstöd behöver utvecklas för denna redovisning och utredning pågår kring detta. Om ett nytt system ska upphandlas/utvecklas behöver informationssäkerhets- och arkivperspektivet ingå vid utformningen av systemet.

- I slutet av 2023 antogs ett nytt gallringsbeslut av Stadsarkivet vad gäller personalhandlingar. Stockholms Stadshus ABs avsikt var att dessa skulle användas som grund för arbetet med att ta fram tilläggsavtal till extern löneadministratör vad gäller gallring och arkivering av personalhandlingar i enlighet med det föreläggande bolaget fick vid den inspektion som gjordes av Stadsarkivet hösten 2022. Efter vidare utredning med hjälp av arkivkonsult på Stadsarkivet och avstämning med extern löneadministratör finns det dock begränsningar i att genomföra gallring i enlighet med beslutet. Utredningen har istället föreslagit att en särskild gallringsframställan för de bolag som gemensamt använder detta system tas fram och hemställas till Stadsarkivet 2025.

- Stadens centrala informationssäkerhetsfunktion har tidigare rekommenderat Stockholms Stadshus AB att ansluta sig till registerförteckningsverktyget Draftit Privacy Records. Efter resonemang med bolagets externa dataskyddsombud är bolagets bedömning att det finns många fördelar med att

använda Draftit men att Stockholms Stadshus AB som relativt litet bolag med nio anställda i dagsläget uppfyller kraven med den registerförteckning som finns upprättad idag i Excel. Argumenten är att bolaget har en relativt liten verksamhet som inte motiverar ett systemstöd, det skulle vara resurskrävande att föra över informationen i ett nytt system och det skulle skapa sårbarheter att uppgifterna finns i ett externt system som endast en medarbetare har utbildning i och tillgång till. Det finns i dagsläget inget ägardirektiv om att systemet måste användas.

- Stadens centrala informationssäkerhetsfunktion har tidigare rekommenderat förvaltningar/bolag att ansluta sig till Klassa för systematisk informationsklassning av verksamhetens tillgångar. Bolaget använder nästan enbart stadens centralt upphandlade verksamhetssystem. Bolagets bedömning är att det finns många fördelar med att använda Klassa men att Stockholms Stadshus AB som relativt litet bolag med tio anställda och endast ett system som inte är centralt upphandlat uppfyller kraven på informationsklassning genom att säkerställa att centrala systemägare gjort normerande informationssäkerhetsklassningar för de system bolaget nyttjar i enlighet med DSOs rekommendationer.

  Argumenten är att bolaget har en relativt liten verksamhet som inte motiverar användandet av Klassa, det skulle vara resurskrävande att utbildas i och införa ett nytt system och det skulle skapa sårbarheter att endast en medarbetare har kunskap tillgång till systemet. Det finns i dagsläget inget ägardirektiv om att systemet måste användas.

2.1.2 Risk och sårbarhetsanalys

Stadens arbete med risk- och sårbarhetsanalys (RSA) bedrivs i en tvåårscykel. En ny cykel inleddes under 2024. Bolaget följer stadens risk- och sårbarhetscykel och instruktioner.

Stockholms Stadshus ABs övergripande slutsatser av analysen av risk- och sårbarhetsarbetet 2022 var att bolaget inte har någon samhällsviktig verksamhet men däremot kritisk verksamhet vad gäller styrning, uppföljning och beslutsfattande för bolagskoncernen.

I budgeten för 2023 fanns uppdrag om att ta fram en krigsledningsplan samt prioritera de verksamhetsområden som skulle bedrivas i händelse av höjd beredskap. I samband med detta utreddes även bolagens förutsättningar för beslutsfattande. Bolaget

har under RSA-analysen 2024 tagit ställning till om slutsatsen som tidigare gjordes 2022 gäller än eller om åtgärdsplan och kontinuitetshanteringsplaner behöver tas fram för de prioriterade verksamhetsområdena som identifierades i samband med framtagandet av krigsledningsplanen för bolaget. Efter genomförandet av steg 1-4 av RSA 2024 är bedömningen att bolaget saknar samhällsviktig verksamhet men har däremot prioriterad verksamhet vad gäller styrning och beslutsfattande för bolagskoncernen samt faktura- och lönehantering för bolaget. Analysen har landat i ett antal åtgärdsförslag och kontinuitetshanteringsplaner att hantera under 2025 bl.a. vad gäller bortfall av infrastruktur, antagonistiskt hot samt sociala risker.

Utöver bolagets egen risk- och sårbarhetsarbete kommer arbete ske inom områden som behandlas i stadens sektorsorganisation där Stadshus AB deltar i två sektorer.

Bolaget har uppfattat att staden ser över hur styrdokument och RSA-metoden kan utvecklas för att anpassas till de krav som ställs i NIS2/Cybersäkerhetslagen/CER.

2.1.3 Väsentlighets- och riskanalys (VOR) och internkontrollplan (IKP)

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.

Utöver bolagets egna identifierade processer ska bolaget, enligt stadens anvisning, ha med den obligatoriska stadsövergripande processen Systematiskt informationssäkerhetsarbete i sin väsentlighets- och riskanalys och bedöma om de ska med i internkontrollplanen. Stockholms Stadshus AB har bedömt att nämndernas obligatoriska arbetssätt (Implementering av lokal anvisning, Incidenthantering, Informationsklassning och Informationssäkerhet inom upphandlingsförfarande) har låga riskvärden på bolaget och dessa tas inte med i internkontrollplanen för 2025. Däremot tas *Behörighetshantering* och *Översyn av registerförteckningen över bolagets personuppgiftsbehandlingar* med i internkontrollplanen för 2025. Ställningstagande för vilka kontrollaktiviteter som tas med gällande informationssäkerhet för 2026-2027 tas i samband med kommande års internkontrollplaner.

2.1.4 Risker som identifierats i GDPR-årsrapport

GDPR-årsrapport är ett medel för styrelsen att ta emot de råd och rekommendationer som dataskyddsombudet (DSO) är skyldig att ge till ansvarig enligt dataskyddsförordningen samt för att få insyn i vad DSO:ns granskande arbete av verksamhetens status avseende integritet och dataskydd visar. Årsrapporten syftar till att nämnd/bolagsstyrelse ska kunna fatta beslut om prioriteringar, resurser och initiativ framåt. Detta samspel resulterar i att det blir enklare för ansvarig nämnd/bolagsstyrelse att visa hur de som personuppgiftsansvarig efterlever dataskyddslagstiftningen.

I GDPR-årsrapport 2023 konstaterar DSO att verksamhetens dataskyddsarbete håller en hög nivå och att majoriteten av förra tillsynsårets föreslagna åtgärder har åtgärdats på ett lämpligt sätt.

DSO har granskat de sex obligatoriska granskningsområdena samt ett antal områden utöver de obligatoriska. Inledningsvis konstaterar DSO att verksamheten i hög utsträckning uppfyller de krav som ställs enligt dataskyddsförordningen och enligt den aktuella rapporten. Ett antal förbättringsåtgärder har dock identifierats av bolagets DSO, bland annat:

- DSO rekommenderar att verksamheten fyller i alla tomma fält i registerförteckningen. Tomma fält kan för utomstående framstå som att registerförteckningen är ofullständig.
- DSO rekommenderar att verksamheten kontrollerar att samtliga genomförda informationsklassningar är aktuella, relevanta och har en arbetsgång som säkerställer att verksamheten vid behov reviderar klassningarna.
- DSO rekommenderar att bolaget gör en inventering av samtliga pågående personuppgiftsbehandlingar som kan tänkas innebära hög risk för fysiska personers rättigheter och friheter för att säkerställa att alla nödvändiga bedömningar genomförs.
- DSO rekommenderar att bolaget lägger särskilt fokus på att sprida kunskap i sin organisation om vad personuppgiftsincidenter är och hur de ska hanteras om de inträffar.
- DSO rekommenderar att de anställda får tydlig information om hur de ska hantera sin e-post i förhållande till dataskyddsförordningen och allmänna handlingar.

I samband med verksamhetsberättelse och bokslut tar bolaget del av dataskyddsombudets årsrapport och stor hänsyn tas till eventuella rekommendationer till personuppgiftsansvarig som lämnas i rapporten. Nästa GDPR-årsrapport tas upp på koncernstyrelsemötet 24 mars 2025.

3 Förbättringar för verksamhetens LIS

3.1 Stockholms Stadshus ABs lokala anvisning för informationssäkerhet

Den 4 november 2024 fastställde vice vd bolagets reviderade version av Lokal anvisning för informationssäkerhet. Anvisningen är förmedlad till medarbetare, diarieförd och finns tillgänglig för alla medarbetare på bolagets gruppdisk.

4 Åtgärder 2024

Under året har bland annat nedan arbete utförts:

- Översyn av Lokal anvisning för informationssäkerhet.
- Genomgång av bl.a. lokal anvisning för informationssäkerhet med medarbetare.
- Reviderad version av hanteringsrutin för informationssäkerhetsincidenter framtagen men inte fastställd arbete fortgår 2025
- Ställningstagande gjort gällande bolagens användande av IA och möjligheten att dela upp incidenter gällande arbetsmiljö i systemstödet Stella. Bolagen behåller IA som verktyg även för arbetsmiljö-incidenter (förvaltningar delar upp incidentrapporteringen). Bolagen kan överväga att dela upp i senare skede.
- Behörighetshanteringsrutin efterlevd och dokumenterad.
- Genomgång av rutin för hantering av offentlighetsprincipen i relation till dataskyddsförordningen med medarbetare
- Utvecklat arbete med såväl säkra meddelanden som digitala signaturer
- Medarbetare har genomfört Stadens utbildningar i informationssäkerhet och dataskydd
- Bolaget använder främst centrala system, ett arbete med att säkerställa att centrala systemägare gjort normerande informationssäkerhetsklassningar för de system bolaget nyttjar i enlighet med DSOs rekommendationer pågår
- Bolaget har fortsatt genomgången av registerförteckningen i syfte att uppdatera och förenkla i enlighet med DSOs rekommendationer
- Bolaget har inte genomfört stadens nya digitala utbildningar inom informationssäkerhet för medarbetare och chefer då

dessa dragits tillbaka av funktionen för stadsövergripande informationssäkerhet
- Inom ramen för RSA-arbetet har bolaget tagit ställning till att åtgärds/kontinuitetsplaner bör upprättas inom några områden
- Uppdaterat, förenklat och kommunicerat avtalshanteringsrutinen med medarbetare
- Utrett möjligheten att ta fram rutiner/avtal för arkivering/gallring av personalhandlingar enligt nytt gallringsbeslut – ej möjligt.

5 Åtgärder 3-årsplan

5.1 Under 2025 ska Stockholms Stadshus AB prioritera att:

- säkerställa att informationssäkerhetsfrågorna lyfts fram och ingår i det interna utvecklingsarbetet
- säkerställa att samtliga medarbetare genomför stadens obligatoriska e-utbildningar för informationssäkerhet och dataskydd
- etablera en rutin för regelbundna informationsklassningar
- göra årlig översyn av Lokal anvisning för informationssäkerhet
- fastställa och kommunicera lokal rutin för informationssäkerhetsincidenter inklusive personuppgiftsincidenter på bolaget
- följa och vid behov uppdatera avtalshanteringsrutin
- följa och vid behov uppdatera behörighetshanteringsrutin
- se över behovet av en konsekvensanalys vid eventuellt införande av systemstöd för redovisning av hållbarhetsrapportering inom bolagskoncernen
- ta fram gallringsframställan till Stadsarkivet för hantering av personaluppgifter i lönesystem
- Se över och vid behov uppdatera bolagets hanteringsanvisningar för hantering av allmänna handlingar
- ta fram kontinuitetsplaner/åtgärdsplaner inom prioriterade verksamhetsområden utifrån RSA-analys
- Utföra stickprovskontroller enligt internkontrollplan

5.2 Under 2026 ska Stockholms Stadshus AB prioritera att:

- säkerställa att informationssäkerhetsfrågorna lyfts fram och ingår i det interna utvecklingsarbetet.

- se till att samtliga medarbetare genomför stadens obligatoriska e-utbildningar för informationssäkerhet och dataskydd
- gå igenom och uppdatera registret över personuppgiftsbehandlingar
- årlig översyn av Lokal anvisning för informationssäkerhet
- årlig uppdatering av Lokal incidenthanteringsrutin
- årlig behörighetsrevision (identitet och åtkomst)
- följa den framtagna rutinen för regelbundna informationsklassningar
- ta fram plan/rutin för hantering av digitala personalhandlingar/digital personalakt

5.3 Under 2027 ska Stockholms Stadshus AB prioritera att:

- säkerställa att samtliga medarbetare genomför stadens obligatoriska e-utbildningar för informationssäkerhet och dataskydd
- säkerställa att genomgång av registret över personuppgiftsbehandlingar utförs
- genomföra årlig översyn av Lokal anvisning för informationssäkerhet
- genomföra årlig behörighetsgenomgång
- genomföra uppföljningar av övrig rutindokumentation t ex avtalshanteringsrutin, incidenthanteringsrutin m.m. utförs.
- följa den framtagna rutinen för regelbundna informationsklassningar

Fastställd av vice vd 2024-11-19