Stockholms stad

Ledningens genomgång år 2024

Stockholms Stadshus AB

Beslutad 2024-01-09
Reviderad [datum]

Ledningens genomgång

Dnr: SSAB 2023/136

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.

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.

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

Innehållsförteckning

1 Vad är Ledningens genomgång? 2

2 Ledningssystem för informationssäkerhet, LIS 4

2.1 Vad påverkar Stockholms Stadshus ABs informationssäkerhetsarbete? 4

2.1.1 Omvärldsbevakning 4

2.1.2 Risk och sårbarhetsanalys 6

2.1.3 Väsentlighets- och riskanalys (VOR) och internkontrollplan (IKP) 6

2.1.4 Risker som identifierats i GDPR-årsrapport 7

3 Förbättringar för verksamhetens LIS 8

3.1 Stockholms Stadshus ABs lokala anvisning för informationssäkerhet 8

4 Åtgärder 2023 8

5 Åtgärder 3-årsplan 9

5.1 Under 2024 ska Stockholms Stadshus AB prioritera att: 9

5.2 Under 2025 ska Stockholms Stadshus AB prioritera att: 10

5.3 Under 2026 ska Stockholms Stadshus AB prioritera att: 10

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 har 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.

- 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

- Under året kommer årsredovisningslagen att anpassas 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. Eventuellt behöver även systemstöd utvecklas för denna redovisning.

- I slutet av 2023 kommer nya gallringsbeslut att fattas av Stadsarkivet vad gäller personalhandlingar. Dessa kommer 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.

- 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 Draft it 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.

2.1.2 Risk och sårbarhetsanalys

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

Stockholms Stadshus ABs övergripande slutsatser av analysen av risk- och sårbarhetsarbetet 2022 är att bolaget inte har någon samhällskritisk verksamhet men däremot kritisk verksamhet vad gäller styrning, uppföljning och beslutsfattande för bolagskoncernen. Bolaget genomförde steg 1-4 av RSA med bedömningen att verksamheten inte kräver vidare åtgärder för att upprätthållas, dvs bolaget har accepterat eller hanterat alla sina risker. Denna analys innebar att bolaget inte gjorde resterade steg inom RSA-modellen (kontinuitetshantering).

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 kommer under RSA-analysen 2024 ta 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.

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

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 (Behörighetshantering, Implementering av lokal anvisning, Incidenthantering, Informationsklassning och Informationssäkerhet inom upphandlingsförfarande) har låga riskvärden på bolaget och dessa tas inte med i internkontrollplanen för 2024. Däremot tas *Översyn av registerförteckningen över bolagets personuppgiftsbehandlingar* med i internkontrollplanen för 2024. Ställningstagande för vilka kontrollaktiviteter som tas med gällande informationssäkerhet för 2025-2026 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 2022 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 registerförteckningen justeras så att den kan förstås av en utomstående person.
- DSO rekommenderar att verksamheten säkerställer att samtlig personuppgiftsbehandling informationklassas.
- DSO rekommenderar bolaget att göra en sammanställning över vilka system de använder i sin verksamhet och vilka av

dessa som föranleder en riskanalys/konsekvensbedömning för att säkerställa att alla nödvändiga bedömningar genomförs.
- DSO rekommenderar bolaget att lägga särskilt fokus på att sprida kunskap i personalgruppen om vad personuppgiftsincidenter är och hur de ska hanteras.

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 25 mars 2024.

3 Förbättringar för verksamhetens LIS

3.1 Stockholms Stadshus ABs lokala anvisning för informationssäkerhet

Den 12 september 2023 fastställde vice vd bolagets Lokala anvisning för informationssäkerhet. Anvisningen är förmedlad till medarbetare, diarieförd och finns tillgänglig för alla medarbetare på bolagets gruppdisk.

4 Åtgärder 2023

Under året har bland annat nedan arbete utförts:
- Informationsklassningar av lönehanteringssystemet Visma Agda och det digitala videokonferensverktyget ZoomX genomfört
- Lokal anvisning för informationssäkerhet framtagen
- Genomgång av bl.a. lokal anvisning för informationssäkerhet samt rutin för incidenthantering med medarbetare
- Översyn av hanteringsrutin för informationssäkerhetsincidenter påbörjad
- Ställningstagande gjort gällande bolagens användande av IA och möjligheten att dela upp incidenter i arbetsmiljö-IA. Bolagen behåller IA som verktyg även för arbetsmiljö-incidenter (förvaltningar delar upp incidentrapporteringen)
- PUB-avtal framtaget med leverantör inför styrelseenkät
- Behörighetshanteringsrutin framtagen

- Revidering av rutin för registrerades rättigheter genomförd
- Rutin för hantering av offentlighetsprincipen i relation till dataskyddsförordningen framtagen och förmedlad till medarbetare
- Interna rutiner har tagits fram för såväl säkra meddelanden som digitala signaturer
- Medarbetare har genomfört Stadens utbildningar i informationssäkerhet och dataskydd
- Då bolaget främst använder centrala system pågår ett arbete med att säkerställa att centrala systemägare gjort normerande informationssäkerhetsklassningar för de system bolaget nyttjar i enlighet med DSOs rekommendationer
- Genomgång av behörigheter i ekonomisystemet och bolagets övriga verksamhetssystem har genomförts under året
- Bolaget har gjort en genomgång av registerförteckningen i syfte att uppdatera och förenkla i enlighet med DSOs rekommendationer

5 Åtgärder 3-årsplan

5.1 Under 2024 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
- genomföra stadens nya digitala utbildningar inom informationssäkerhet för medarbetare och chefer
- uppdatera och förenkla bolagets register över personuppgiftsbehandlingar
- inventera och dokumentera vilka informationsklassningar av de centrala system som bolaget nyttjar som är genomförda centralt
- göra årlig översyn av Lokal anvisning för informationssäkerhet
- uppdatera och kommunicera lokal rutin för informationssäkerhetsincidenter på bolaget
- inom ramen för RSA-arbetet ta ställning till om bolaget bör upprätta åtgärds/kontinuitetsplaner
- 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 rutiner/avtal för arkivering/gallring av personalhandlingar enligt nytt gallringsbeslut

5.2 Under 2025 ska Stockholms Stadshus AB prioritera att:

- etablera en rutin för regelbundna informationsklassningar
- säkerställa att informationssäkerhetsfrågorna lyfts fram och ingår i det interna utvecklingsarbetet.
- Utifrån ställningstagande gällande om bolaget bedriver samhällsviktig verksamhet, ta fram kontinuitetsplaner/åtgärdsplaner inom prioriterade verksamhetsområden
- 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
- uppföljningar av övrig rutindokumentation t ex avbrottsplan, hanteringsrutin för informationssäkerhetsincidenter och behörighetsrevision utförs
- 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 2026 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 2024-01-09