



Stockholms
stad

Ledningens genomgång år 2023

Idrottsförvaltningen

Beslutad 23 januari 2023

Ledningens genomgång

Dnr: 1.2.1/2023/2751

Kontaktperson: Johan Malmström

1. Sammanfattning

”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, en 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.

Rapporten ska ge information och vara ett underlag till förvaltningschef/bolagschef årliga bedömning 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.

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

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 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.	Sammanfattning	3
2.	Ledningssystem för informationssäkerhet, LIS	5
2.1	Informationssäkerhetsarbete	5
2.1.1	<i>Vad har verksamheten identifierat i RSA-arbetet Risk och sårbarhetsanalys</i>	<i>6</i>
2.1.2	<i>Resultatet från egen uppföljning (VoR och IKP).....</i>	<i>6</i>
2.1.3	<i>Risker som identifierats i GDPR-årsrapport</i>	<i>6</i>
3.	Prioritering av åtgärder.....	7
3.1	Plan för 2024	7
3.2	Plan för 2025	7
3.3	Plan för 2026	7

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 Kvalitetsprogram¹. Till riktlinjen finns tillämpningsanvisningar som är fastställda av stadsdirektören.

Tillämpningsanvisningarna reglerar ansvar och roller sett till Stockholms stads systematiska informationssäkerhetsarbete. Inom idrottsnämnden pågår ett arbete med att färdigställa en lokal anvisning som ska visa hur stadens övergripande ledningssystem för informationssäkerhet implementeras och förväntas vara klart under slutet av 2023 eller början av 2024

2.1 Informationssäkerhetsarbete

Idrottsförvaltningen ska alltid ha ett riskbaserat förhållningssätt i arbetet med informationssäkerhet. För att det ska fungera, behöver samtliga verksamheter i förvaltningen delta. Det är inom verksamheterna som bedömningar av uppkomna risker och sårbarheter kan identifieras och som senare kan lyftas internt för vidare hantering. Som stöd använder förvaltningen stadens övergripande dokument, rutiner och guider.

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. Därmed minskar risker för förluster och oegentligheter som skadar stadens anseende och till-

¹ [Stockholms stads kvalitetsprogram \(start.stockholm\)](https://start.stockholm/kvalitetsprogram)

gångarna säkras. Arbetet med intern kontroll är en del av stadens kvalitetsarbete.

Utöver nämndens egna identifierade processer har nämnden tagit med incidenthantering i internkontrollplanen.

2.1.1 Vad har verksamheten identifierat i RSA-arbetet Risk och sårbarhetsanalys

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

Fokus för stadens risk- och sårbarhetsarbetet under 2023 har varit på väsentlig funktion i samhället. Idrottsförvaltningen är inte av väsentlig funktion under en förhöjd beredskap, men kan bistå med resurser såsom maskiner och lokaler vid behov som kan användas av totalförsvaret.

Under 2024 ska en ny risk- och sårbarhetsanalys genomföras och då kommer även informationssäkerhet att ingå.

2.1.2 Resultatet från egen uppföljning (VoR och IKP)

I förvaltningens tertialrapport 2 2023 rapporterades inga väsentliga avvikelser. Under året har kontroller genomförts i förvaltningens verksamhetssystem för att säkerställa att rätt person har rätt behörighet. Vidare har kontroller genomförts inom områden såsom registerförteckning, informationsklassning och hantering av registerförteckning.

2.1.3 Risker som identifierats i GDPR-årsrapport

Dataskyddsombudets GDPR-årsrapport för 2022 visade att förvaltningen inte helt lever upp till de krav som ställs. Förvaltningen rekommenderas förbättringar inom områdena styrdokument samt några tekniska och organisatoriska åtgärder.

Dataskyddsombudets bedömning bygger helt på den information som lagts in i registerförteckningen. Påpekandet om att viss information saknades, stämmer inte eftersom information fanns dokumenterad, dock på annan plats än i förteckningen.

Under 2024 kommer förvaltningen fortsätta arbetet med att uppdatera registerförteckningen och tillse att dokumentationen finns i förteckningen.

3. Prioritering av åtgärder

3.1 Plan för 2024

Under året kommer nya samt uppdaterade informationsklassningar göras av de system som förvaltningen använder, det vill säga även centrala system som tidigare inte klassats.

Vidare kommer följande aktiviteter att ske:

- implementera en lokal anvisning för informationssäkerhet
- genomföra utbildningar och informationsinsatser för berörda målgrupper inom förvaltningen
- uppdatera registerförteckning samt ta fram en rutin för arbetet med registerförteckning
- ta fram och fastställa en lokal rutin för personuppgiftsincidenter samt en rutin för informationssäkerhetsincidenter
- säkerställa att samtliga medarbetare genomför stadens obligatoriska e-utbildningar för informationssäkerhet och dataskydd

3.2 Plan för 2025

- Följa upp, utvärdera och revidera rutiner inom informationssäkerhetsområdet

3.3 Plan för 2026

- Revidera genomförda informationsklassningar som ska ske vartannat år
- Granska att de lokala rutinerna som togs fram 2024 inom informationssäkerhetsområdet efterlevs