Ledningens genomgång år 2025

Idrottsförvaltningen

Beslutad 16 december 2025

Ledningens genomgång

Dnr: 1.2.2/2025/1877

Kontaktperson: Omar Farjani

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 2026 uppmanas samtliga nämnder och bolagsstyrelser att de ska ta fram en ”Ledningens genomgång” med en planering för informationssäkerhetsarbetet under de kommande tre åren. Den ska biläggas verksamhetsplanen. Planeringen för de kommande tre åren ska utgå från nämndens verksamhetsuppdrag i budget och följa riktlinjen för informationssäkerhet i Stockholms stad.

Aktiviteterna ska redovisas både i ”Ledningens genomgång” samt i nämndens verksamhetsplan under mål 3.5.

Under perioden 2026–2028 ska förvaltningens arbete med informationssäkerhet fokusera på att tydliggöra organisation, ansvarsfördelning och arbetssätt inom dataskydd och informationssäkerhet.

Ett centralt område i arbetet är att genomföra informationsklassningar. Förvaltningen ska inventera befintliga informationsklassningar, säkerställa att dessa är dokumenterade samt vid behov revidera dem för att upprätthålla aktuell och korrekt informationshantering.

Arbetet ska även omfatta framtagande och implementering av rutiner för informationssäkerhet samt säkerställande av att

utbildningsinsatser inom området planeras och genomförs för berörd personal.

Därutöver ska säkerhetshöjande åtgärder genomföras i förvaltningens verksamhetssystem för att stärka skyddet av information och minska risken för incidenter.
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

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[1]. Till riktlinjen finns tillämpningsanvisningar som är fastställda av stadsdirektören.

Tillämpningsanvisningarna reglerar ansvar och roller sett till Stockholms stads systematiska informationssäkerhetsarbete. Idrottsnämnden har färdigställt en lokal anvisning för informationssäkerhet som fastställs under 2025.

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

[1] Stockholms stads kvalitetsprogram (start.stockholm)

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 inleddes under 2024 och förvaltningen följer stadens instruktioner. I RSA finns informationssäkerhet med och under 2025 gjordes en fördjupad analys där risker och sårbarheter identifierades med förslag på åtgärder.

2.1.2 Resultatet från egen uppföljning (VoR och IKP)

I förvaltningens tertialrapport 2 2025 rapporterades inga väsentliga avvikelser. Under 2025 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

Under året har förvaltningen, i två omgångar, utsett nya Dataskyddsombud. Första delen av året har kompetensen och rollen tillsetts av en konsult, för att från och med september bemannas genom stadens egen organisation (serviceförvaltningen). Dessa har därför haft kort tid på sig att sätta sig in i förvaltningens arbete med personuppgiftshantering. En GDPR-årsrapport för 2025 håller på att färdigställals. Förvaltningen utgår från att denna kommer gå i jämförbar linje med 2024-års årsrapport, då arbetet med att omhänderta upptäckta risker och brister fortfarande är pågående hos förvaltningen.

Förvaltningen har under året arbetat med att gå igenom personuppgiftshantering kopplat till processerna som berör det nya bokningssystemet, Idrottsportalen. Förvaltningen har genomfört en konsekvensbedömning av personuppgiftshanteringen kopplat till systemet som innebar att ytterliga tekniska skyddsåtgärder så som tydligare behörighetsstyrning för information infördes i systemet. Förvaltningen undersöker även om det finns ytterligare möjligheter till uppgiftsminimering eller skyddsåtgärder i processerna. Det innebär ex. om pseudonymisering och gallring av personuppgifter efter viss tid kan genomföras.

Förvaltningen har ett pågående arbete att uppdatera hanteringsanvisningarna, med stöd av konsult från stadsarkivet. Det arbete kommer sedan ligga till grund för en revidering av nämndens registerförteckning.

3. Prioritering av åtgärder

3.1 Plan för 2026

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:

- Bevaka hur förvaltningen påverkas av NIS2-direktivet och hur arbetet därefter ska ske
- Förstärka samt förtydliga organisationen kring arbetet med dataskydd och informationssäkerhet i samarbete med DSO
- Genomföra ett penetrationstest i Idrottsportalen
- Bevaka utvecklingen av generativ AI och syntetisk media utifrån ett informationssäkerhetsperspektiv
- Höja kompetens och kunskap inom informationssäkerhet genom utbildningar och informationsinsatser inom förvaltningen
- Arbeta med registerförteckning samt ta fram en rutin för arbetet med registerförteckning
- Ta fram och fastställa en lokal rutin för incident-hantering
- Med utgångspunkt från GDPR-årsrapport 2025 genomföra föreslagna åtgärder
- Säkerställa att hänsyn tas till informationssäkerhetskrav vid upphandlingar
- Ta fram en normerande rutin för behörighetshantering samt revidera befintliga

3.2 Plan för 2027

- Uppföljning av arbetet som har genomförts inom Generativ AI.
- Följa upp och utvärdera arbetet inom NIS2-direktivet
- Följa upp, utvärdera och revidera rutiner och förteckningar inom informationssäkerhetsområdet
- Följa upp utbildnings- och informationsinsatser

3.3 Plan för 2028

- Revidera genomförda informationsklassningar som ska ske vartannat år
- Granska att de lokala rutinerna som togs fram 2026 inom informationssäkerhetsområdet efterlevs

Dokumenttyp Rapport	*Dokumentnamn* Ledningens genomgång 2025.docx	
Godkänd av Marina Högland	*Datum* 2025-11-12	*Version* 1.0