Informationssäkerhet

- Ledningens genomgång år 2025

Kulturhuset Stadsteatern

Kontaktperson: Andreas Eriksson, Infrastrukturchef
Beslutad av: Malin Dahlberg, VD
Datum: 2025-11-18

KULTURHUSET
stadsteatern

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 eller 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]

Planerade aktiviteter ska redovisas i Ledningens genomgång och i bolagets verksamhetsplan under mål 3.5 *Hög beredskap och stark rådighet ska råda i alla verksamhetsområden*.

[1] Tillämpningsanvisning till stadens riktlinje för informationssäkerhet

Innehållsförteckning

1 Status för åtgärder från ledningens tidigare genomgångar 4

2 Ledningssystem för informationssäkerhet, LIS 5

2.1 Intern kontroll 6

2.2 Risk och sårbarhetsanalys 6

3 Faktorer som påverkar 7

3.1 Tredjelandsöverföring 7

3.2 Finansborgarrådets förslag till budget 2026 7

4 Resultatet från egen uppföljning 7

4.1 Internkontrollplan (IKP) 7

4.2 Revisionsresultat 7

4.3 Risker som identifierats i GDPR-årsrapport 7

5 Möjligheter till förbättring av verksamhetens LIS 8

5.1 Prioritering av fortsatt arbete 8

1 Status för åtgärder från ledningens tidigare genomgångar

Under 2025 har bolaget fortsatt att stärka sitt arbete inom informationssäkerhet och dataskydd. Här följer en sammanfattning av årets viktigaste insatser:

Utbildning och medvetenhet: Bolagets medarbetare har även under 2025 deltagit i stadens obligatoriska e-utbildningar inom informationssäkerhet och dataskydd. Chefer och systemansvariga har fått fördjupad information kring incidenthantering, personuppgiftshantering och riskbedömning. Syftet har varit att ytterligare höja medvetenheten och beredskapen i hela organisationen.

Strategiskt arbete: Informationssäkerhet har fortsatt att vara en integrerad del i bolagets digitala och teknologiska utveckling, inklusive det fortsatta arbetet med AI-strategin. Säkerhets- och integritetsaspekter har beaktats i planering, införande och uppföljning av nya initiativ.

Intern utveckling: Frågor kopplade till informationssäkerhet och dataskydd har under året varit en naturlig del i bolagets interna utvecklingsprojekt. Fokus har legat på att säkerställa att nya system och processer uppfyller gällande krav och bidrar till en trygg informationshantering.

Systemklassificering: Arbetet med systemklassificering har fortsatt enligt plan. Genom uppdateringar och kompletteringar har bolaget förbättrat sin överblick över digitala tillgångar och säkerställt att system hanteras utifrån rätt skyddsnivå.

Incidenthantering: Bolaget har fortsatt att hantera och följa upp samtliga inkomna incidenter i enlighet med gällande rutin. Ingen incident under året har bedömts som allvarlig, mycket allvarlig eller katastrofal. Erfarenheter från inträffade händelser har använts för lärande och förbättring.

Revisioner: Årlig revision av den *Lokala anvisningen för informationssäkerhet och dataskydd* samt den *Lokala rutinen för incidenthantering (informationssäkerhet)* har genomförts. Dokumenten har uppdaterats i enlighet med förändrade krav och erfarenheter från verksamheten.

Inköpsprocesser: Informationssäkerhetens roll i upphandling och inköp har ytterligare förstärkts genom fortsatt samarbete mellan

informationssäkerhetsfunktionen och bolagets upphandlare. Arbetet har bidragit till att krav på informationssäkerhet beaktas redan i ett tidigt skede.

Dessa insatser har tillsammans bidragit till att ytterligare stärka bolagets informationssäkerhet och dataskydd, samt lagt grunden för ett långsiktigt och systematiskt förbättringsarbete även framöver.

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

Tillämpningsanvisningarna reglerar ansvar och roller sett till Stockholms stads systematiska informationssäkerhetsarbete. För Kulturhuset Stadsteaterns räkning har bolagschef fastställt en så kallad lokal anvisning[3] som beskriver hur stadens övergripande ledningssystem för informationssäkerhet omhändertas inom bolaget.

För att upprätthålla ett informationssäkerhetsarbete som är aktuellt över tid ska Kulturhuset Stadsteatern 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.

[2] Stockholms stads kvalitetsprogram (start.stockholm)
[3] Lokal anvisning för informationssäkerhet och dataskydd

2.1 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 och därmed minimera risker i verksamheten samt säkra tillgångar och förhindra förluster och oegentligheter som skadar bolagets anseende. Arbetet med intern kontroll är en del av stadens kvalitetsarbete.

Den interna kontrollen ska vara utformad för att med rimlig grad av säkerhet kunna uppnå följande:

- att verksamheten är ändamålsenlig och effektiv
- att information om verksamhet och ekonomi är tillförlitlig och rättvisande
- att lagar, förordningar, föreskrifter och styrdokument följs.

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 någon av de fem arbetssätten, *behörighetshantering, implementering av lokal anvisning, incidenthantering, informationsklassning* och *informationssäkerhet inom upphandlingsförfarandet*, ska ingå i internkontrollplanen.

För 2025 har bolaget bedömt att *implementering av lokal anvisning* och *informationssäkerhet inom upphandlingsförfarandet* skall följas upp i internkontrollplanen.

2.2 Risk och sårbarhetsanalys

En viktig del av stadens övergripande krisberedskapsarbete är processen för risk- och sårbarhetsanalys (RSA), vilken ska stärka stadens förmåga att hantera extraordinära händelser och arbetet med civil beredskap.

Stadens arbete med risk- och sårbarhetsanalys (RSA) bedrivs i en tvåårscykel. Bolaget följer stadens risk- och sårbarhetscykel och dess instruktioner. Enligt dessa instruktioner är bolaget inte ålagd att genomföra en RSA, då bolaget inte anses vara en samhällsviktig verksamhet. Bolaget har trots detta valt att använda delar i denna metodik i syfte att höja bolagets beredskaps- och krishanteringsförmågor.

3 Faktorer som påverkar

3.1 Tredjelandsöverföring

I juli 2023 fattade EU-kommissionen ett beslut om adekvat skyddsnivå för USA, förutsatt att organisationen/leverantören omfattas av EU-U.S. Data Privacy Framework. Det nya EU-beslutet ger kommuner större möjligheter att använda USA-ägda molntjänster. Stadens styrgrupp för informationssäkerhet uppmanar fortsatt till återhållsamhet kring amerikanska molntjänster och har tagit fram ett nytt inriktningsbeslut för molntjänster. Inriktningsbeslutet innebär bland annat att inga stora införanden av nya stadsgemensamma molntjänster kommer att genomföras i dagsläget som en följd av det senaste EU-beslutet.

3.2 Finansborgarrådets förslag till budget 2026

Stockholms stads förslag till budget 2026 fastställer att de kommunala bolagen ska fortsätta öka beredskaps- och krishanteringsförmågan, utveckla och stärka arbetet med informationssäkerhet, samt beakta risker och sårbarheter med generativ AI och syntetisk media.

4 Resultatet från egen uppföljning

4.1 Internkontrollplan (IKP)

Under 2025 har bolaget behandlat processen *Systematiskt informationssäkerhetsarbete* i Väsentlighets- och Riskanalysen (VoR) och följt upp *Implementering av lokal anvisning* och *Informationssäkerhet inom upphandlingsförfarande* specifikt i internkontrollplanen.

Vid uppföljningen av de två kontrollpunkterna har inga avvikelser noterats.

4.2 Revisionsresultat

I de revisionsrapporter som bolaget mottagit under 2025, har inga särskilda rekommendationer lämnats gällande informationssäkerhet förutom de som härrör till bolagets följsamhet till dataskyddsförordningen (GDPR). Se mer information under avsnitt 4.3.

4.3 Risker som identifierats i GDPR-årsrapport

För att Personuppgiftsansvarig skall kunna leda och styra dataskyddsarbetet så som dataskyddsförordningen avser genomförs ett antal granskningar under året av bolagets externt anlitade

dataskyddsombud. Resultatet sammanfattas i en årsrapport, upprättad av dataskyddsombudet, som spänner över sex obligatoriska rapporteringsområden. Dessa är registerförteckning, styrdokument, tekniska och organisatoriska åtgärder för personuppgiftsbehandlingar, konsekvensbedömningar, individens rättigheter samt personuppgiftsincidenter. Identifierade risker värderas enligt en fyrgradig skala baserat på deras allvarlighetsgrad.

- Allvarliga brister identifierade som omgående kräver insatser av ledning och/eller övriga verksamheten
- Brister identifierade som bedöms vara omfattande och/eller kräva omgående åtgärder
- Brister identifierade som bör åtgärdas men ej bedöms vara brådskande, omfattande eller allvarliga
- Inga brister av nämnvärd betydelse identifierade

En detaljerad beskrivning av identifierade risker och rekommenderade åtgärdsförslag återfinns i GDPR Årsrapport år 2025.

5 Möjligheter till förbättring av verksamhetens LIS

Bolaget ser kontinuerligt över och utvecklar det systematiska informationssäkerhetsarbetet. Utvecklingen sker med utgångspunkt i lagstiftning, verksamhetens behov och i eventuella brister.

5.1 Prioritering av fortsatt arbete

Under 2026 kommer Kulturhuset Stadsteatern särskilt fokusera på;

- Ökad andel medarbetare som har kunskap om informationssäkerhet genom bland annat stadens obligatoriska e-utbildningar
- Fortsätta utbilda bolagets chefer så de känner till och anammar bolagets incidentrutin för informationssäkerhet och dataskydd
- Säkerställa att kontinuitetsplaner finns för alla relevanta system.
- Behörighetshantering
- Informationsklassning
- Årlig revision av styrande dokument

Under 2027 kommer Kulturhuset Stadsteatern särskilt fokusera på;

- Ökad andel medarbetare som har kunskap om informationssäkerhet genom bland annat stadens obligatoriska e-utbildningar
- Fortsätta utbilda bolagets chefer så de känner till och anammar bolagets incidentrutin för informationssäkerhet och dataskydd
- Öva utifrån kontinuitetsplaner.
- Behörighetshantering
- Informationsklassning
- Årlig revision av styrande dokument

Under 2028 kommer Kulturhuset Stadsteatern särskilt fokusera på;

- Ökad andel medarbetare som har kunskap om informationssäkerhet genom bland annat stadens obligatoriska e-utbildningar
- Fortsätta utbilda bolagets chefer så de känner till och anammar bolagets incidentrutin för informationssäkerhet och dataskydd
- Fortsätta öva utifrån kontinuitetsplaner.
- Behörighetshantering
- Informationsklassning
- Årlig revision av styrande dokument