Informationssäkerhet

- Ledningens genomgång år 2024

Kulturhuset Stadsteatern

Kontaktperson: Andreas Eriksson, Infrastrukturchef
Beslutad av: Malin Dahlberg, VD
Datum: 2024-12-18

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 5

2.2 Risk och sårbarhetsanalys 6

3 Faktorer som påverkar 6

3.1 Tredjelandsöverföring 6

3.2 Finansborgarrådets förslag till budget 2025 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 2024 har flera framsteg gjorts inom informationssäkerhet och dataskydd i bolaget. Här följer en sammanfattning av de viktigaste insatserna:

Utbildning och medvetenhet: Bolagets medarbetare har fortsatt att informeras och utbildas i informationssäkerhet, bland annat genom stadens obligatoriska e-utbildningar. Chefer har fått fördjupad information om bolagets incidentrutin för informationssäkerhet. Detta för att säkerställa en hög beredskap.

Strategiskt arbete: Informationssäkerhet har integrerats i bolagets AI-strategi under året. Detta säkerställer att säkerhetsfrågor beaktas i takt med att bolaget utvecklar nya teknologiska initiativ.

Intern utveckling: Informationssäkerhets- och dataskyddsfrågor har lyfts fram som centrala komponenter vid internt utvecklingsarbetet.

Systemklassificering: Det kontinuerliga arbetet med att klassa alla relevanta system har fortsatt, vilket stärker bolagets kontroll över sina digitala tillgångar.

Incidenthantering: Alla anmälda incidenter har följts upp och utretts enligt bolagets etablerade incidentrutin, vilket bidrar till lärande och förbättring. Ingen incident har bedömts som allvarlig, mycket allvarlig eller katastrofala utan har hanterats som en del av det systematiska incidenthanteringsarbetet.

Revisioner: Årlig revision av den *Lokala anvisningen för informationssäkerhet och dataskydd* samt den *Lokala rutinen för incidenthantering (informationssäkerhet)* har genomförts, vilket säkerställer att styrdokumenten är uppdaterade och relevanta.

Inköpsprocesser: Informationssäkerhetens roll i inköpsprocessen har tydliggjorts genom en revidering av upphandlings- och inköpsdokument, i nära samarbete med bolagets upphandlare.

Dessa insatser har tillsammans stärkt bolagets informationssäkerhet och dataskydd, och lagt en stabil grund för fortsatt arbete inom området.

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.

2.1 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.

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

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 genomföra steg 1 (kartläggning och analys) och steg 2 (riskbedömning) enligt RSA-metodiken 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 2025

Stockholms stads budget 2025 fastställer att de kommunala bolagen ska fortsätta öka beredskapsförmågan, exempelvis genom att analysera och hantera risker och sårbarheter samt genom krisledningsplanering, kontinuitetshantering, systematiskt informationssäkerhetsarbete, krigsorganisation samt årliga, obligatoriska krisledningsövningar.

4 Resultatet från egen uppföljning

4.1 Internkontrollplan (IKP)

Under 2024 har bolaget endast behandlat processen *Systematiskt informationssäkerhetsarbete* i Väsentlighets- och Riskanalys-processen (VoR) och därmed inte följt upp några specifika kontrollpunkter i IKPn.

Som ett delområde i det systematiska informationssäkerhetsarbetet skall informationssäkerhetsrelaterade krav beaktas vid upphandling av nya system och tillhörande tjänster. Detta görs genom att informationssäkerhetssamordnaren involveras i samband med upphandlingsförfarandet. Informationssäkerhetssamordnaren säkerställer att stadens metodstöd för informationsklassning, eller motsvarande, har använts vid identifikation av relevanta informationssäkerhetskrav.

Det har under året noterats att de stöddokument som används vid upphandlingar behöver förtydligas med kontrollpunkter relaterade till informationssäkerhet. Stöddokumenten har uppdaterats under tertial 3 med relevanta kontrollpunkter.

4.2 Revisionsresultat

I de revisionsrapporter som bolaget mottagit under 2024, 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 2024.

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 2025 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
- Se över om en gemensam incidenthanteringsprocess för bolagets olika typer av incidenter skall skapas (informations/IT-säkerhet, dataskydd, arbetsmiljö)
- Behörighetshantering
- Informationsklassning
- Årlig revision av styrande dokument

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