# Informationssäkerhet

## - Ledningens genomgång år 2024

## Kulturhuset Stadsteatern



**Ledningens genomgång**
Bilaga till Kulturhuset Stadsteaterns Verksamhetsplan 2024
**Dnr:** xxxx/xxx
**Kontaktperson:** Andreas Eriksson, Infrastrukturchef
**Beslutad av:** Malin Dahlberg, VD
**Datum:**

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]

Rapporten skall också innehålla en planering för informationssäkerhetsarbetet under de kommande tre åren. Denna ska biläggas verksamhetsplan. Planeringen för de kommande tre åren ska utgå från 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

# Innehållsförteckning

# 1 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 som beskriver hur stadens övergripande ledningssystem för informationssäkerhet omhändertas inom bolaget.

## 1.1 Vad påverkar Kulturhuset Stadsteaterns informationssäkerhetsarbete?

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.

### 1.1.1 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)

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.

Kulturhuset Stadsteatern har bedömt att de fem obligatoriska arbetssätten, *behörighetshantering, implementering av lokal anvisning, incidenthantering, informationsklassning* och *informationssäkerhet inom upphandlingsförfarandet,* ska ingå i intern kontrollplanen även kommande tre år.

### 1.1.2 Risk och sårbarhetsanalys

Stadens arbete med risk- och sårbarhetsanalys (RSA) bedrivs i en tvåårscykel. En ny cykel inleds under 2024.
Kulturhuset Stadsteatern har i risk- och sårbarhetsarbetet 2022 identifierat ett antal processer som kan ha risker inom informationssäkerhet och har åtgärdsplaner och kontinuitetsplaner för de delar som bolaget har rådighet över. Bolaget följer stadens risk- och sårbarhetscykel och instruktioner.

### 1.1.3 Resultatet från egen uppföljning (IKP)

I årets internkontrollplan ska kontroll göras av att alla upphandlingar av nya system och tillhörande tjänster har beaktat informationssäkerhetsrelaterade krav. 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 noterats att de stöddokument som används vid upphandlingar behöver förtydligas med kontrollpunkter relaterade till informationssäkerhet. Exempelvis har det identifierats att en kontrollpunkt måste införas vilken gör gällande att informationssäkerhetssamordnaren har givit klartecken på att informationssäkerhetsrelaterade krav är omhändertagna innan upphandlingen publiceras.

### 1.1.4 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 och 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

Nedan följer en sammanställning över identifierade brister som bedömts vara omfattande eller allvarliga;

- Bristande incidentrapportering. Under granskningen noterades det att endast en personuppgiftsincident hade rapporterats vilket är orealistiskt för en organisation av KHSTs storlek.
- Bristande i behandlingen av känsliga personuppgifter. Under granskningen noterades det att behandlingarna av känsliga uppgifter saknade ett angivet undantag för att behandlingen ska vara laglig.
- Bristande process beträffande granskning av den som beställer mailloggar, dvs. en granskning av granskaren.
- Brister i det systematiska dataskyddsarbetet

En detaljerad beskrivning av identifierade risker och rekommenderade åtgärdsförslag återfinns i GDPR-rapporten för 2022.

### 1.1.5 Kompetenslyft ledningsgrupp

Under 2023 genomför Stadsledningskontoret, SLK, en kompetenshöjande satsning inom området informationssäkerhet. En del av denne omfattar aktiviteten *Kompetenslyft Ledningsgrupp*, genom vilken stadens ledningsgrupper erbjuds en kompetenshöjande workshop av Deloitte.

Under 2023 kommer en sådan workshop att genomföras hos Kulturhuset Stadsteaterns ledningsgrupp. Förutom att bidra till ett kompetenslyft inom området så kommer leverantören också att identifiera ett antal förslag på fortsatt arbete.

## 2.1 Förbättringar för verksamhetens LIS

### 2.1.1 Kulturhuset Stadsteaterns lokala anvisning för informationssäkerhet

Den 13 december 2022 fastställde bolagschef Malin Dahlberg Kulturhuset Stadsteaterns Lokala anvisning för informationssäkerhet och dataskydd. Anvisningen finns tillgänglig för alla medarbetare på bolagets intranät.

Enligt anvisningen är informationssäkerhetsarbetet nära sammanlänkat med arbetet kring dataskyddsarbetet samt väsentlighets- och riskanalys samt risk- och sårbarhetsanalys. Arbetet planeras och rapporteras till staden enligt ordinarie rutiner.

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.

## 2.2 Prioritering av åtgärder

### 2.2.1 Under 2024 ska Kulturhuset Stadsteatern

Bolaget ska under 2024 följa upp att den lokala anvisningen följs, främst med fokus på att;

- chefer;
  - årligen ser till att samtliga medarbetare och konsulter genomför stadens obligatoriska e-utbildningar för informationssäkerhet och dataskydd
  - känner till och anammar bolagets incidentrutin för informationssäkerhet och dataskydd
  - följer upp och utreder de incidenter som verksamheten anmäler enligt bolagets incidentrutin

- objektledare;
  - tillser att informationstillgångar är klassade och att handlingsplaner från klassning tas om hand för systemet.

Under 2024 ska Kulturhuset Stadsteatern prioritera;

- fortsätta utveckla rutiner för att tydliggöra informationssäkerhet i inköps- och upphandlingsprocesserna
- säkerställa att informationssäkerhet är beaktat i den AI-strategi som bolaget skall ta fram under 2024
- säkerställ att informationssäkerhets- och dataskyddsfrågorna lyfts fram och ingår i det interna utvecklingsarbete som pågår inom bolaget

### 2.2.2 Under 2025 ska Kulturhuset Stadsteatern

Under 2025 ska Kulturhuset Stadsteatern prioritera;

- att etablera en rutin för regelbundna informationsklassningar
- att ta fram en gemensam incidenthanteringsprocess för så många typer av incidenter som möjligt (informations/IT-säkerhet, dataskydd, arbetsmiljö) som bidrar till snabb identifiering, bedömning, hantering och återställning.
- Utifrån RSA säkerställa att kontinuitetsplaner finns för alla relevanta system.

### 2.2.3 Under 2026 ska Kulturhuset Stadsteatern

Under 2026 ska Kulturhuset Stadsteatern prioritera:

- Revidering av lokal anvisning.
- Granska hur väl lokal rutin för regelbundna informationsklassningar följs.
- Öva utifrån kontinuitetsplaner.