Ämne	Skapat av	Revision
Informationssäkerhet	Andreas Holmgren	1.0
Dokument	Skapat datum	Revisionsdatum
LIS (Ledningssystem) - Informationssäkerhet	2023-11-13	2023-12-19

Ledningssystem – Informationssäkerhet (LIS)

Lokal anvisning – Stockholmsmässan AB

Allmänt	
Dokumentägare	Carl-Johan Torssel (ISAM)
Författare	Andreas Holmgren (konsult)

Revisionshistoria			
0.1	2023-11-13	Andreas Holmgren	Avstämd med Dataskyddsombud (DSO)
0.2	2023-12-12	Andreas Holmgren	Uppdatering efter avstämning med Informationssäkerhetssamordnare (ISAM), Verksamhetscontroller, CFO och IT-chef.
1.0	2023-12-19	Andreas Holmgren	Fastställd av VD

Bilagor		
B1	2022-11-17	Stockholms stads standardmall för Lokal anvisning v1

Ämne	Skapat av	Revision
Informationssäkerhet	Andreas Holmgren	1.0
Dokument	Skapat datum	Revisionsdatum
LIS (Ledningssystem) - Informationssäkerhet	2023-11-13	2023-12-19

Innehåll

Ämne	Skapat av	Revision
Informationssäkerhet	Andreas Holmgren	1.0
Dokument	Skapat datum	Revisionsdatum
LIS (Ledningssystem) - Informationssäkerhet	2023-11-13	2023-12-19

1 Bakgrund

Denna ”Lokala anvisning” beskriver roller, organisation och arbetssätt för Stockholmsmässans informationssäkerhetsarbete.

Den kompletterar stadens centrala riktlinje och tillämpningsanvisning för informationssäkerhet och dokumenterar hur Stockholmsmässan systematiskt tillämpar och följer upp arbetet med informationssäkerhet.

Den förtydligar hur ansvarsfördelning och roller har anpassats för Stockholmsmässan – vem som ansvarar för vad, vilka styr-, stöd och granskningsroller som finns, och övriga roller som i sitt uppdrag arbetar med skydd av informationstillgångar.

1.1 Ägarens krav på ”Lokal anvisning”

Ägarens styrande krav på detta dokument är formulerat på följande sätt:

”Förvaltningschef/bolagschef ska för nämndens/styrelsens räkning fastställa en så kallad lokal anvisning som beskriver hur stadens övergripande ledningssystem för informationssäkerhet omhändertas i den egna verksamheten. Den lokala anvisningen ska gås igenom årligen och revideras vid behov. Den lokala anvisningen ska minst beskriva ansvarsfördelning inom den egna informationssäkerhetsorganisationen (roller och mandat), vilken effekt informationssäkerhetsarbetet ska leda till lokalt, specifik lagstiftning som gäller för verksamhetens informationshantering samt hur arbetet följs upp lokalt.”

Den mall för ”Lokal anvisning” som ägaren tillhandahållit utgör bilaga för att ge möjlighet att värdera vilka avsteg eller kompletteringar som Stockholmsmässan har gjort vid framtagandet av denna ”Lokala anvisning”.

1.2 Avgränsning

Ledningssystemet (LIS) och den ”Lokala anvisningen” berör endast HUR det systematiska informationssäkerhetsarbetet är organiserat. Det berör inte VAD för konkreta åtgärder som är etablerade eller planeras för. Dessa underhålls löpande och finns separat dokumenterade i olika dokument som t ex:

- Policy för IT- och telefonianvändning och för IT- och informationssäkerhet.
- Tekniska och organisatoriska skyddsåtgärder.
- Kontinuitetsplan IT.

- Informationsklassningsrapporter.

1.3 Påverkande lagrum

De lagrum som är styrande för Stockholmsmässans arbete med informationssäkerhet är:

- Dataskyddsförordningen (GDPR)
- Offentlighets- och sekretesslagen
- Arkivlagen

De lagrum som inte är styrande för Stockholmsmässans arbete med informationssäkerhet är:

- Lagen om informationssäkerhet för samhällsviktiga och digitala tjänster (NIS)
- Patientdatalagen (PdL)

2 Organisation och roller

Stockholmsmässans organisation för informationssäkerhet är indelad i tre olika nivåer.

- Den **styrande** nivån omfattar beslutande roller och funktioner i verksamheten.
  VD, Företagsledning (FL) och Chefer
- Den **stödjande** nivån omfattar specialistfunktioner som stödjer linjeverksamheten i informationssäkerhetsarbetet.
  Informationssäkerhetssamordnare (ISAM), GDPR Förvaltningsgrupp, Dataskyddsombud (DSO) och Systemledare.
- Den **granskande** nivån omfattar funktioner för kontroll av att lagar och beslutade policyer och rutiner efterlevs.
  Företagsledning, Dataskyddsombud (DSO), Verksamhetscontroller och Externa granskare.

2.1 Styrande

2.1.1 VD och Företagsledning (FL)

Företagsledningen (FL), med VD som ytterst ansvarig, är formellt informationsägare och personuppgiftsansvarig för Stockholmsmässan. Företagsledningen (FL) ansvarar för:

- Att det finns ett ändamålsenligt och effektivt informationssäkerhetsarbete inom verksamheten.
- Att verksamheten så långt det är möjligt strävar efter att arbeta i linje med stadsövergripande riktlinjer och vägledande dokument för informationssäkerhet.
- Att verksamheten tilldelas de resurser som behövs för att kunna upprätthålla god informationssäkerhet.
- Att utse Informationssäkerhetssamordnare (ISAM) och Dataskyddsombud (DSO).
- Att årligen inhämta rapporterna ”Ledningens genomgång” från Informationssäkerhetssamordnaren (ISAM) samt ”GDPR årsrapport” från Dataskyddsombudet (DSO).

VD godkänner och fastställer:

- Den ”Lokala anvisningen” (detta dokument).

- Rapporten ”Ledningens genomgång”.
- Rapporten ”GDPR årsrapport”.

2.1.2 Chefer

Ansvaret för att skydda informationen som hanteras inom verksamheten följer linjeansvaret. Varje chef har inom sin verksamhet ett särskilt ansvar för att informationen hanteras på ett korrekt sätt enligt gällande lagstiftning, riktlinjer och policyer. Chefen kan delegera och fördela ansvaret inom sin verksamhet men har fortsatt kvar det formella ansvaret för medarbetare inom den egna verksamheten – såväl anställda som konsulter, vikarier, praktikanter etc. Chefer ansvarar för:

- Att medarbetare får tillgång till och tar till sig tillgängliga policyer och instruktioner avseende informationshantering och personuppgiftsbehandling. Detta ska ske i samband med tillträde och därefter minst vartannat år, eller tätare om det särskilt anmodas.
- Att medarbetare genomgår de utbildningar kring informationssäkerhet och dataskydd som tillgängliggörs. Detta ska ske i samband med tillträde och därefter minst vartannat år, eller tätare om det särskilt anmodas.
- Att medarbetare ges de instruktioner och den utbildning som krävs för att på ett korrekt sätt använda de system och tjänster som innehåller informationstillgångar och som de förväntas använda i utförandet av sina arbetsuppgifter.
- Att faktiska eller potentiella incidenter som rör personuppgifter utan dröjsmål anmäls enligt beslutad rutin.

2.2 Stödjande

2.2.1 Informationssäkerhetssamordnare (ISAM)

Informationssäkerhetssamordnare (ISAM) ansvarar för att samordna, följa upp och rapportera om det operativa informationssäkerhetsarbetet och att, med stöd av andra roller såsom Dataskyddsombud (DSO), IT-chef, Verksamhetscontroller, för ändamålet anlitade konsulter etc, säkerställa att verksamheten både vägleds och granskas. Informationssäkerhetssamordnaren (ISAM) arbetar på uppdrag av Företagsledningen (FL) och ansvarar för:

- Att vara kontaktpunkt för stadens centralt informationssäkerhetsansvarige (CISO) samt rapportera allvarliga incidenter till denne.

- Att fungera samordnande kring rådgivning gentemot systemledare, projektledare, upphandlare etc och i det arbetet vid behov koordinera stöd från olika roller såsom Dataskyddsombud (DSO), IT-chef, Verksamhetscontroller, för ändamålet anlitade konsulter etc.
- Att stödja linjeverksamheten i arbetet med riskanalys, informationsklassning, utbildning och kunskapsspridning.
- Att bistå Verksamhetscontrollern vid granskning/revision för de fall det omfattar det lokala informationssäkerhetsarbetet.
- Att bevaka relevanta förändringar i lagstiftning och omvärld vad avser informationssäkerhet.

2.2.2 Förvaltningsgrupp GDPR och Dataskyddsombud (DSO)

På Stockholmsmässan finns en Förvaltningsgrupp GDPR för att omhänderta alla aspekter av ett aktivt dataskyddsarbete.

Förvaltningsgruppen bistår verksamheten med vägledning, översyn och administration av dataskyddsfrågor, såväl strategiska som taktiska och operativa.

Förvaltningsgruppen leds av Dataskyddsombudet (DSO) som är ytterst ansvarig för gruppens löpande arbete och för de beslut som fattas inom gruppen. Styrgrupp utgörs av Företagsledningen (FL). Förvaltningsgruppen ansvarar för:

- Att utbilda, vägleda och instruera verksamheten om åtgärder för efterlevnad av lagar, policyer och rutiner för dataskydd.
- Att vid behov konsultera extern juridisk expertis kring alla frågor som rör dataskydd.
- Att löpande underhålla verksamhetens registerförteckning.
- Att löpande underhålla verksamhetens dataskyddspolicyer.
- Att utforma och instruera om formulering av integritetsmeddelanden i de olika gränssnitt där personuppgifter inhämtas.
- Att administrera och följa upp samtycken.
- Att gallring av personuppgifter sker enligt beslutad rutin.
- Att hantera inrapporterade personuppgiftsincidenter.
- Att vägleda och övervaka upprättandet av nödvändiga personuppgiftsbiträdesavtal.

2.2.3 Systemledare

Systemledare finns utsedda för alla system med särskilt skyddsvärda informationstillgångar. Systemledare IT kompletteras av Systemledare Verksamhet och utgör den samlade Systemledningen för respektive system. Exakt ansvarsfördelning dem emellan kan skilja sig åt mellan olika system.

Systemledningen ansvarar utifrån ett informationssäkerhetsperspektiv för förvaltning, underhåll, utveckling och tillämpning av respektive system genom:

- Att underhålla användarkonton och behörigheter.
- Att underhålla en korrekt basdokumentation för driftskontinuitet.
- Att utföra gallring av personuppgifter där det är tillämpligt enligt beslutad rutin.
- Att bidra i arbetet med informationsklassning genom aktivt deltagande eller genom verifiering av underlag.
- Att arbeta för en informationssäker förvaltning genom samråd med leverantörer och att proaktivt kompatibilitetsgranska, versionshantera, underhålla, uppgradera, uppdatera och konfigurera system.
- Att arbeta för en informationssäker drift genom samråd med leverantörer, interna driftsspecialister eller externa sådana vid outsourcad drift och cloud/SaaS-tjänster.
- Att arbeta för en informationssäker tillämpning genom information och i förekommande fall utbildning till användare eller nyckelanvändare och genom att korrigera och instruera vid avvikande användning som äventyrar informationssäkerheten.

2.3 Granskande

2.3.1 Företagsledning

Företagsledningens granskande roll sker dels genom att årligen inhämta rapporterna ”Årsrapport GDPR” från Dataskyddsombudet (DSO) samt ”Ledningens genomgång” från Informationssäkerhetssamordnaren (ISAM). VD ansvarar för att godkänna och fastställa dessa.

2.3.2 Dataskyddsombud (DSO)

Dataskyddsombudets (DSO) granskande roll syftar till att säkerställa att verksamheten efterlever lagar, policyer och beslutade rutiner avseende dataskydd.

Det sker genom att Dataskyddsombudet (DSO) agerar beslutsmässigt kring frågor som rör GDPR samt säkerställer att agendan för Förvaltningsgrupp GDPR:s arbete omfattar kontinuerligt förbättringsarbete samt rapportering och hantering av avvikelser.

Utöver det ansvarar dataskyddsombudet för rapportering till Företagsledningen (FL) minst årligen i form av ”Årsrapport GDPR”.

2.3.3 Verksamhetscontroller

Verksamhetscontroller ansvarar för uppföljning och rapportering av hur Stockholmsmässan uppfyller krav genom de riktlinjer, policyer och rutiner som staden ålägger Stockholmsmässan samt uppfyllnad av de mål som staden beslutat om för Stockholmsmässans verksamhet.

Informationssäkerhet är ett av flera moment som ingår i arbetet med Väsentlighets- och riskanalys (VOR) samt Internkontrollplan (IKP) och därmed får Verksamhetscontrollern även en granskande roll inom Informationssäkerhet.

Verksamhetscontroller har även rollen som Stockholmsmässans ILS-samordnare.

2.3.4 Externa granskare

Stockholmsmässans verksamhet granskas genom flera externa revisioner, relevanta för arbetet med informationssäkerhet t ex:

- Finansiell revision enligt ISA315 som även omfattar granskning av risker kring informationstillgångar relevanta för den finansiella verksamheten.
- Stockholms stads lekmannarevisioner i den mån de omfattar informationssäkerhet och dataskydd.
- Andra särskilda tillsynskontroller och revisioner som Stockholm stad kan komma att genomföra i bolaget avseende informationssäkerhet och dataskydd.

2.4 Övriga funktioner

Flera funktioner inom Stockholmsmässans verksamhet är involverade i det löpande arbetet med informationssäkerhet.

2.4.1 Infrastrukturtekniker

Infrastrukturtekniker inom IT-avdelningen arbetar aktivt med tekniska skyddsåtgärder för IT- och informationssäkerhet. De arbetar med att vidta, följa upp och kontinuerligt förbättra konkreta säkerhetsåtgärder inom IT-drift och digital arbetsplats och bistår samt vägleder Systemledare och andra stödjande roller med teknisk säkerhetsexpertis.

2.4.2 Arkivansvarig

Arkivansvarig bidrar till det systematiska informationssäkerhetsarbetet genom att bistå ISAM med inventering av informationstillgångar ur ett arkivperspektiv samt med kunskap om hanteringsanvisningar och övrig arkivdokumentation.

2.4.3 Medarbetare

Medarbetare inom Stockholmsmässan förväntas följa lagar, riktlinjer, policyer och instruktioner för en informationssäker verksamhet och genomgå de utbildningar kring informationssäkerhet och dataskydd som tillgängliggörs.

3 Processer, rutiner och dokument

Stockholmsmässans arbete med uppföljning av informationssäkerheten inordnas till stora delar i de övergripande uppföljningsrutinerna Väsentlighets- och riskanalys (VOR) samt Internkontrollplan (IKP).

3.1 Väsentlighets- och riskanalys (VOR)

Informationssäkerhet ingår som en delmängd i den Väsentlighets- och riskanalys (VOR) som görs enligt Stockholms stads övergripande riktlinjer för hela bolagets verksamhet.

3.2 Internkontrollplan (IKP)

Resultatet av Väsentlighets- och riskanalysen (VOR) leder till en definition av s k ”Oönskade händelser” vilka sedan tas in i Internkontrollplanen (IKP) som hanteras enligt Stockholms stads övergripande riktlinjer för hela bolagets verksamhet.

Informationssäkerhet ingår som en delmängd av detta och ett antal kontrollområden inom informationssäkerhet definieras i Internkontrollplanen (IKP). För respektive kontrollområde definieras ett antal olika kontrollpunkter för vilka det genomförs stickprovskontroller.

Eventuella avvikelser i stickprovskontrollerna hanteras omedelbart, schemaläggs eller transporteras för åtgärd i efterföljande års Internkontrollplan (IKP) beroende på karaktär och allvarlighetsgrad.

3.3 Informationsklassificering

Klassning av väsentliga informationstillgångar görs vartannat år, eller oftare för de fall det sker väsentliga förändringar i portföljen, t ex att nya informationstillgångar/system tillkommer eller förändras i väsentlig utsträckning.

I samband med klassning sker en bedömning av tillämpliga lagrum (t ex GDPR) samt en bedömning av konsekvenserna vid en incident utifrån följande säkerhetsaspekter:

- **Konfidentialitet:** Att tillgången till information är begränsad till de användare som behöver den för att utföra sina arbetsuppgifter.

- **Riktighet:** Att information är skyddad från förlust eller förvanskning på grund av obehörig åtkomst, misstag eller tekniska fel.
- **Tillgänglighet:** Att information kan behandlas av behöriga användare, inom rimlig tid och på ett rimligt förväntat sätt.

Konsekvenser bedöms som någon av följande nivåer:

- Ingen eller försumbar skada.
- Måttlig skada.
- Betydande skada.
- Allvarlig skada.

Beroende på val av lagrum samt konsekvens per säkerhetsaspekt faller ett antal informationssäkerhetskrav ut baserat på ISO 27001. En självskattning görs av aktuell kravuppfyllnad vilket genererar en rapport på föreslagna åtgärder. Dessa åtgärder prioriteras och en handlingsplan tas fram.

Åtgärder samt uppföljning och rapportering av att åtgärderna genomförs integreras i arbetet med Internkontrollplanen (IKP).

3.4 Underhåll av dataskydds- och GDPR-frågor

Görs kontinuerligt inom ramen för Förvaltningsgruppen GDPR:s löpande arbete och inkluderar:

- Underhåll av Registerförteckning.
- Underhåll av register med personuppgiftsbiträdesavtal.
- Underhåll av dataskyddspolicyer.
- Underhåll av integritetsmeddelanden i de olika gränssnitt där personuppgifter inhämtas.
- Underhåll av samtycken.
- Underhåll av utbildningsmaterial, rutinbeskrivningar och checklistor.

3.5 Underhåll av policyer och styrande dokument

3.5.1 Vartannat år

Underhåll av följande dokument görs vartannat år eller oftare vid behov:

- Policy för IT- och telefonianvändning och för IT- och informationssäkerhet (styrande dokument)
- Kontinuitetsplan IT (styrande dokument)
- Handlingsplan informationssäkerhetsklassning (redovisande dokument)
- Tekniska och organisatoriska säkerhetsåtgärder (redovisande dokument)

3.5.2 Varje år

Underhåll av följande dokument görs varje år eller oftare vid behov:

- Lokal anvisning (styrande dokument)
- Ledningens genomgång (redovisande dokument)
- GDPR årsrapport (redovisande dokument)

3.5.3 Kontinuerligt

Underhåll av följande dokument görs kontinuerligt vid behov:

- Dataskyddspolicyer (styrande dokument)
- Registerförteckning (redovisande dokument)
- Utbildningsmaterial (styrande dokument)
- Basdokumentation System (redovisande dokument)