Ämne	Skapat av	Revision
Informationssäkerhet	Andreas Holmgren	1.0
Dokument	Skapat datum	Revisionsdatum
Ledningens genomgång 2023	2023-11-13	2023-12-19

Ledningens genomgång 2023

Informationssäkerhet – Stockholmsmässan AB

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

Revisionshistoria			
0.1	2023-11-13	Andreas Holmgren	
0.2	2023-12-01	Andreas Holmgren	Uppdatering efter avstämning med Informationssäkerhetssamordnaren (ISAM), Verksamhetscontroller, CFO och IT-chef.
0.3	2023-12-12	Andreas Holmgren	Uppdatering efter avstämning med Dataskyddsombud (DSO).
1.0	2023-12-19	Andreas Holmgren	Fastställd av VD

Bilagor		
B1	2023-12-19	Ledningssystem – Informationssäkerhet (LIS) – Lokal anvisning v1.0
B2	2022-11-17	Stockholms stads standardmall för Ledningens genomgång

Ämne	Skapat av	Revision
Informationssäkerhet	Andreas Holmgren	1.0
Dokument	Skapat datum	Revisionsdatum
Ledningens genomgång 2023	2023-11-13	2023-12-19

Innehåll

Ämne	Skapat av	Revision
Informationssäkerhet	Andreas Holmgren	1.0
Dokument	Skapat datum	Revisionsdatum
Ledningens genomgång 2023	2023-11-13	2023-12-19

1 Bakgrund

Denna ”Ledningens genomgång” beskriver status på Stockholmsmässans systematiska informationssäkerhetsarbete, påverkansfaktorer, resultat av årets uppföljningar samt genomförda och planerade förbättringar inför kommande år.

1.1 Ägarens krav på ”Ledningens genomgång”

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

”För att kunna styra arbetet ska förvaltningschef/bolagschef minst årligen informera sig om hur arbetet går. Det sker genom att förvaltningschef/bolagschef inhämtar 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.”

Den mall för ”Ledningens genomgång” som ägaren tillhandahållit utgör bilaga för att ge möjlighet att värdera vilka avsteg eller kompletteringar som Stockholmsmässan har gjort vid utformningen av denna ”Ledningens genomgång”.

2 Påverkansfaktorer

2.1 Ny lagstiftning

Det s k **NIS2** är en skärpning av NIS-direktivet och träder i kraft i oktober 2024. Det berör aktörer som bedriver samhällsviktig verksamhet och leverantörer av samhällsviktiga tjänster. En grupp till vilken Stockholmsmässan inte hör och därmed heller inte berörs av.

EU-US Data Privacy Framework är sedan juli 2023 på plats och innebär att det nu är möjligt att överföra personuppgifter mellan EU och USA utan ytterligare skyddsåtgärder (som t.ex. SCC – Standard Contractual Clauses) så länge överföring sker till företag som anslutit sig till det nya ramverket, genom självcertifiering. De överföringar av personuppgifter som i dagsläget sker till USA i Stockholmsmässans verksamhet är underkastade SCC och har tidigare bedömts ej kräva ytterligare skyddsåtgärder utöver det, på grund av avsaknaden av känsliga personuppgifter och den begränsade omfattningen. Därmed får detta inte någon direkt påverkan annat än att det kan medföra administrativa lättnader framgent.

I övrigt finns ingen ny lagstiftning inom informationssäkerhet som Stockholmsmässan behöver agera på under 2024.

2.2 Försäljning av Stockholmsmässans verksamhet

Med anledning av mässverksamhetens förestående försäljning så är planeringshorisonten i denna ”Ledningens genomgång” begränsad till enbart 2024.

3 Uppföljning

3.1 VoR och IKP 2023

Stickprov Internkontrollplan 2023			
Allvarlig störning i IT-miljön	Stickprovskontroller i väsentliga delar i Kontinuitetsplan IT.	Kontroll av reservkraft i datahallar.	Ingen avvikelse.
		Redundanstester av infrastruktur-komponenter.	Mindre allvarlig brist i dokumentation som har åtgärdats.
		Kontroll av backuptagning till målmiljö offsite.	Ingen avvikelse.
		Kontroll av återläsning backuper.	Ingen avvikelse.
Allvarlig informations-säkerhetsincident inträffar	Stickprovskontroller för rutiner för informations-säkerhet.	Uppföljning åtgärdsplan efter informations-säkerhetsklassningar.	Mindre allvarlig brist som tas in i Internkontrollplan 2024.
		Stickprovskontroller i ”Policy för IT och telefonianvändning samt informations- och IT-säkerhet.	Mindre allvarlig brist som har åtgärdats.
Anmälningspliktig personuppgifts-incident (GDPR) inträffar	Stickprovskontroller av rutiner för personuppgifts-hantering	Kontroller utförda för 4 olika mäss-genomföranden.	Ingen avvikelse.

3.2 VoR och IKP 2024

Samma ”oönskade händelser” som för IKP 2023 kommer att gälla även för IKP 2024 såvitt avser Informationssäkerhet.

3.3 Resultatet från revisioner

Inga särskilda revisioner avseende Informationssäkerhet har genomförts under året.

Granskning av risker kring informationstillgångar relevanta för den finansiella verksamheten (inom ramen för den finansiella revisionen enligt ISA315) har genomförts utan anmärkningar.

4 Status 2023 och föreslagna förbättringar 2024

4.1 Tekniska skyddsåtgärder

4.1.1 Vid ingången av året

Stockholmsmässan håller en mycket god teknisk skyddsnivå med bland annat följande tekniska skyddssystem på plats sedan tidigare:

- Redundant driftsmiljö (aktiv-aktiv)
- Omfattande backuptagning (offsite)
- Brandvägg
- Antivirus
- Skyddssystem för e-post (inkl kontroll av länkar och realtidsscanning/spärr av filer)
- Skydd mot DDoS-attacker

4.1.2 Genomförda förbättringar under 2023

- Ny brandväggslösning och förbättringar i routing och filter.
- Förbättrad backuplösning med kryptering som skyddar mot att virus/ransomware kan infektera backup-miljön.
- Integrering av flera särskilt skyddsvärda cloud/SaaS-tjänster med Azure AD och Single-Sign-On-authentication.

4.1.3 Förslag till förbättringar 2024

- Fortsatt integrering av ett antal mindre skyddsvärda cloud/SaaS-tjänster med Azure AD och Single-Sign-On-authentication där det är möjligt.
- Ta i bruk en av våra tillgängliga Cisco-tjänster som ytterligare underlättar förbättringsarbete avseende nätsäkerhet.
- Förbättrad datanätsegmentering för att med stöd av brandväggen reducera risker för spridning av t ex virus eller belastningspåverkande attacker inom och mellan olika delar av Stockholmsmässans datanätverk.

4.2 Organisatoriska skyddsåtgärder

4.2.1 Vid ingången av året

Den organisatoriska skyddsnivån var vid ingången av året acceptabel men med förbättringspotential. Den interna genomlysning som genomfördes under 2022 av GDPR- och dataskyddshanteringen i verksamheten resulterade t ex i en handlingsplan där delar av åtgärderna genomfördes redan under 2022 men där delar av dessa kvarstod vid ingången av 2023.

4.2.2 Genomförda förbättringar under 2023

- Flera åtgärder enligt handlingsplanen efter 2022 års genomlysning av GDPR- och dataskyddshantering var implementerade vid ingången av 2023 och flertalet av kvarvarande åtgärder implementerades sedan under Q1 2023.
- Förvaltningsgrupp GDPR återupprättades och ny DSO (Dataskyddsombud) utsågs.
- Målgruppsanpassade GDPR-utbildningar genomfördes.
- Förbättrad cookiehantering för ökad tydlighet gentemot besökare på våra webbplatser infördes.
- Utbildning av medarbetare i grundläggande informationssäkerhet genomfördes.
- Bättre systematik i informationssäkerhetsarbetet infördes i och med integreringen till stadens krav och riktlinjer.

4.2.3 Förslag till förbättringar 2024

- Skärpta rutiner för konto- och behörighetsadministrationen i de cloud/SaaS-tjänster som inte med rimlig ansträngning går att integrera med Azure AD och Single-Sign-On-authentication.
- Fortsatta utbildningsinsatser för medarbetare i generell informationssäkerhet och säkert användarbeteende i IT-miljön.
- Förbättringar i Förvaltningsgrupp GDPR:s löpande arbete avseende identifiering och korrigering av avvikelser, gallring av personuppgifter samt löpande uppdateringar av registerförteckningen.
- Översyn och uppdatering av ”Policy för IT- och telefonianvändning samt informations- och IT-säkerhet”.
- Översyn och uppdatering av ”Kontinuitetsplan IT”.

- Åtgärder av identifierade brister i basdokumentation för system (från IKP 2023).

5 Beslut

VD har 2023-12-19 fattat följande beslut:

1. Att fastställa detta dokument ”Lokal anvisning” i v1.0
2. Att fastställa rapporten ”Ledningens genomgång” i v1.0
3. Att godkänna i rapporten Ledningens genomgång föreslagna förbättringar 2024.