Informations- och cybersäkerhetspolicy		
Framtagen av IT-chef	Godkänd av Styrelse	Granskad av (vid behov) ISAM, Säkerhetschef
Datum 2025-12-10	Revisionsdatum 2026-12-16	Sida Sida 1 av 3

1 Syfte

Syftet med denna informations- och cybersäkerhetspolicy är att fastställa en gemensam grund för Stockholms Hamnars systematiska informationssäkerhetsarbete och att säkerställa att all information och alla IT-resurser skyddas mot obehörig åtkomst, förlust, manipulation, avbrott och cyberangrepp.

En god efterlevnad av Stockholms stads krav och gällande lagstiftning skapar en robust och motståndskraftig digital miljö, som skyddar bolagets samhällsviktiga tjänster samt upprätthåller förtroende hos kunder, medborgare, leverantörer och myndigheter.

2 Omfattning

Policyn gäller för all information (digital, pappersburen, muntlig), alla IT-system, nätverk, digitala resurser och alla användare (medarbetare, konsulter och leverantörer) som behandlar eller får tillgång till bolagets information.

3 Mål

Arbetet ska säkerställa:

- Tillgänglighet, riktighet, konfidentialitet och spårbarhet.
- Förhindra cyberangrepp, dataintrång och informationsläckor.
- En robust och motståndskraftig digital miljö som stödjer samhällsviktiga tjänster.
- Efterlevnad av lagar, riktlinjer och avtal.
- Skapa förtroende hos kunder, medborgare och myndigheter.

4 Styrning och ramverk

Arbetet styrs av Stockholms stads riktlinjer och tillämpningsanvisningar för informationssäkerhet och bolagets lokala tillämpningsanvisningar. Dessa baseras på etablerade ramverk som ISO 27000, NIS2-direktivet, MSB:s föreskrifter (om risk- och sårbarhetsanalyser, incidentrapportering och tekniska åtgärder), GDPR samt ITIL och PM3. Detaljerade beskrivningar av informationssäkerhetsarbetet finns i bolagets lokala tillämpningsanvisningar.

5 Roller och ansvar

Ledningen (VD och styrelse) har det övergripande ansvaret för att informationssäkerhetsarbetet bedrivs enligt denna policy.

- IT-chef: ansvar för ledningssystem, tekniska skyddsåtgärder och rapportering.
- Informationssäkerhetssamordnare: samordnar och följer upp informationssäkerhetsarbetet.

- Chefer: säkerställer efterlevnad och utbildning inom sina verksamheter.
- Medarbetare och konsulter: ska följa policyn och rapportera incidenter.
- Säkerhetschefen, tillika säkerhetsskyddschef, ansvarar fysisk säkerhet samt den informationssäkerhet som regleras av säkerhetsskyddslagen.

6 Utbildning och medvetenhet

Alla chefer- och medarbetare ska genomföra obligatorisk utbildning i informations- och cybersäkerhet minst en gång per år. Särskild utbildning ska ges till roller med utökat ansvar. Konsulter som anlitas ska ta del av bolagets policys, riktlinjer och rutiner för informations- och cybersäkerhet.

7 Riskhantering

Bolaget ska bedriva ett riskbaserat informationssäkerhetsarbete. Bolagsövergripande riskanalys för informations- och cybersäkerhet ska genomföras minst årligen och vid större förändringar. Risker ska dokumenteras, värderas och åtgärdsplaner fastställas. Styrelsen ska årligen delges bolagsövergripande riskanalys och tillhörande åtgärdsplan.

8 Incidenthantering

Rutiner för hantering av incidenter ska finnas.
Alla medarbetare är ansvariga för att uppmärksamma och registerna incidenter.
Betydande incidenter ska dokumenteras, analyseras och rapporteras till utsedd myndighet inom 24 timmar.

9 Kontinuitet och återställning

En kontinuitetsplan ska finnas och uppdateras årligen.
Backup ska tas regelbundet, testas och förvaras på ett säkert sätt.
Återställningsövningar ska genomföras minst en gång per år.

10 Leverantörshantering

Leverantörsavtal ska omfatta administrativa och säkerhetstekniska krav.
Kritiska leverantörer ska årligen riskbedömas.

11 Tillgångs- och behörighetsstyrning

Behörigheter ska ges enligt principerna om behov och minsta möjliga behörighet.
Behörigheter ska omprövas regelbundet och tas bort vid avslut av anställning eller uppdrag.

12 Tekniska skyddsåtgärder

Bolaget ska upprätthålla en hög teknisk säkerhetsnivå genom att använda etablerade skyddsåtgärder för nätverk, system och klienter, säkerställa regelbundna uppdateringar,

övervakning och detektion av säkerhetshändelser samt skydd mot skadlig kod. Känslig information ska skyddas med lämpliga säkerhetsmekanismer såsom kryptering och multifaktorautentisering, och säkerhetskopiering ska ske enligt fastställda krav för att möjliggöra snabb återställning.

13 Kontroller och uppföljning

Revisioner och kontroller ska genomföras minst årligen. Resultat av revisioner och kontroller ska dokumenteras och leda till förbättringsåtgärder.
Ledningens genomgång för informationssäkerhet för bolagets koncernledning genomförs två gånger per år. Styrelsen följer upp bolagets arbete med informationssäkerhet i samband verksamhetsplanering och budget.

14 Giltighet och revidering

Denna policy gäller från och med 2025-12-10 och är fastställd av styrelsen. Policyn ska revideras minst en gång per år eller vid större förändringar i verksamhet, teknik eller lagstiftning.