Ledningens genomgång Informationssäkerhet

Stockholms Hamnar 2026

2025-11-06

Fastställande av Ledningens genomgång

Ledningens genomgång informationssäkerhet fastställs i sin helhet för verksamhetsåret 2026

Föredragande: Frida Carlbring, informationssäkerhetssamordnare

Stockholm 2025-11-21

Magdalena Bosson, VD

Magdalena Bosson

Elektroniskt undertecknad av Magdalena Bosson
Datum: 2025.11.21 14:03:03 +01'00'

Vad är ledningens genomgång

Med ledningens genomgång avses att ledningen ser över verksamhetens systematiska informationssäkerhetsarbete och dess styrning för att säkerställa dess fortsatta inriktning och omfattning. Stockholms Hamnar skall bedriva ett systematiskt och riskbaserat informationssäkerhets- och dataskyddsarbete. Detta innebär att bolaget tar de steg som behövs för att identifiera vilken information som är viktig och sedan införa säkerhetsåtgärder för att skydda den. Arbetsroller kopplat till arbetet med informationssäkerhet- och dataskydd samt aktiviteter har identifierats för att arbetet ska bli en naturlig del av verksamheten.

Informationssäkerhetssamordnaren och dataskyddsombudet samverkar med varandra då både rutiner och åtgärder för områdena går samman.

1 Faktorer som påverkar Stockholms Hamnars ledningssystem för informationssäkerhet

Stockholms stads informationssäkerhetsarbete regleras i en riktlinje som är en bilaga till stadens Kvalitetsprogram. Till riktlinjen finns tillämpningsanvisningar som är fastställda av stadsdirektören, dessa har senast reviderats 2024-11-13. Tillämpningsanvisningarna reglerar ansvar och roller sett till Stockholms stads systematiska informationssäkerhetsarbete.

Stockholms stads nuvarande systematiska arbetssätt som sker inom ramen för ledningssystem för informationssäkerhet, är den grund som gäller även när cybersäkerhetslagen träder i kraft. Stockholms stad kommer då att uppdatera riktlinjer, tillämpningsanvisningar för att de skall bli förenliga med nya lagen.

Stockholms Hamnar har en lokal hanteringsanvisning som beskriver hur stadens övergripande ledningssystem för informationssäkerhet omhändertas inom den egna verksamheten.

1.1 Omvärldsbevakning – hot, trender och ny lagstiftning

I en tid med en allt snabbare teknikutveckling där riskerna är många förekommer incidenter i en allt större omfattning. En stor och uppmärksammad incident som skett under året är när företaget Miljödata utsattes för en attack och miljoner personuppgifter läckte ut. Stockholms Hamnar använder sig inte av denna tjänst men många som arbetar inom verksamheten har varit anställda eller har kopplingar till Stadens förvaltningar.

Framgent ser vi liknande hot som tidigare men nya verktyg riskerar att göra attackerna effektivare och lättare att utföra i större skala. Ett exempel på det är nyttjande av AI i attacker.

Hybridhotet mot samhällskritisk infrastruktur ökar, man har redan sett attacker mot bland annat vattenförsörjning, el och kommunikation.

1.2 Ny lagstiftning

1.2.1 NIS2-direktivet

NIS2-direktivet är en EU-reglering som ska förbättra cybersäkerheten i medlemsstaterna. NIS2-direktivet ersätter det tidigare NIS-direktivet.

Syftet med NIS2-direktivet är att öka motståndskraften mot cybersäkerhetsrisker genom att ställa krav på en hög gemensam cybersäkerhetsnivå för nätverks- och informationssystem inom hela EU. Det handlar om att verksamheter som ansvarar för viktiga samhällsfunktioner ska ha ett systematiskt informationssäkerhetsarbete som leder fram till att lämpliga riskhanteringsåtgärder vidtas. I Sverige kommer NIS2 införas genom en ny lag, cybersäkerhetslagen. Det finns en proposition föreslagen som efter antagande träder i kraft 15 januari 2026.

NIS2 ställer skärpta krav på organisatoriska, tekniska och driftrelaterade säkerhetsåtgärder. Bland annat ställs krav på att verksamheter ska göra riskanalyser och vidta säkerhetsåtgärder för att skydda IT-system och nätverk. Ledningens engagemang i cybersäkerhetsarbetet ska genom det nya direktivet öka.

1.3 Genomförd tillsyn – NIS

Ingen tillsyn från Transportstyrelsen har genomförts under året som gått.

1.4 Resultat från revisioner

Under hösten 2025 har revisionskontoret Stockholm Stad genomfört en revision avseende behörighetshantering i verksamheten. Slutrapport kommer att redovisas innan årsskiftet.

1.5 Status för åtgärder från ledningens tidigare genomgångar

Stockholms Hamnar har under 2025 följt upp de kontrollaktiviteter som redovisades i föregående Ledningens genomgång för informationssäkerhet.

- Uppföljning av registerförteckningar åligger chefer vilket behöver förtydligas med arbetssätt hur detta ska tas om hand.

    - Processen har förtydligats i den lokala anvisningen för informationssäkerhet.
- En tydligare processkartläggning behöver tas fram för att tydliggöra hur personuppgifter och informationsmängder behandlas i verksamheten.
    - Arbete är påbörjat med processkartläggning för att tydliggöra hur personuppgifter och informationsmängder behandlas i verksamheten.
- Fortsatt arbete med nuvarande NIS och förberedelse för kommande NIS2. Detta genomförs med interna resurser men förstärks av extern expertis.
    - GAP-analys genomförd med externt stöd.
    - Initial bruttolista på brister/aktiviteter är upprättad för stöd i vidare prioritering.
- Utbildning av styrelse och ledningsgrupp.
    - Grundläggande information om kommande cybersäkerhetslag föredras styrelse, ledningsgrupp och revisorer 2025-11-12.
- Utbildning för medarbetare inom inköp och upphandling.
    - Kvarstår.
- Följa upp och revidera genomförda informationsklassningar.
    - Initierat, merparten kvarstår.
- Följa upp systemspecifika incidenthanteringsrutiner.
    - Kvarstår.
- Genomföra stickprov av tilldelade behörigheter.
    - Sker i vissa objekt.
    - Processbrist identifierad avseende spårbarhet i tilldelning.
- Stresstest och övning av kontinuitetsplaner kopplat till NIS-direktivet.
    - Kvarstår.

2 Förbättringar som föreslås för Stockholms Hamnars informationssäkerhetsarbete

2.1 Prioritering av åtgärder 2026

- Implementera uppdaterade anvisningen för informationssäkerhet i verksamheten.
- Införande av NIS2-direktivet/cybersäkerhetslagen.
- Funktionen ISAM flyttar organisatoriskt från Säkerhet till IT.
- Funktionen ISAM utökas till en heltidsbefattning.
- Utveckla Ledningens genomgång med tydligare delområden och mätbara mål/effekter.

2.2 Prioritering av åtgärder 2027

- Förbättra, öva och testa systemspecifika kontinuitetsplaner.
- Följa upp att Informationsägare omhändertagit handlingsplaner från klassning.
- Genomföra uppföljning av verksamhetens leverantörer.
- Förvaltningsmodellen PM3 återspeglar övriga staden.

2.3 Prioriteringar av åtgärder 2028

- Fungerande egenkontroller.
- Löpande leverantörsuppföljning.