Stockholm, 26 mars 2025
DNR: SISAB 2025/148

Ledningens genomgång informationssäkerhet 2024

Sammanfattning

Ledningens genomgång innebär en genomlysning av befintligt ledningssystem för informationssäkerhet och förbättringsförslag med åtgärder. Bolagschef ska, enligt stadens tillämpningsanvisning för informationssäkerhet, minst årligen informera sig om bolagets informationssäkerhetsarbete. Det sker genom att bolagschef inhämtar rapport, så kallad ”Ledningens genomgång” från informationssäkerhetssamordnaren.

Bakgrund

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 och 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]

I anvisningar för nämndernas arbete med verksamhetsplan 2024[2] uppmanas samtliga nämnder och bolagsstyrelser att ta fram en tillämpningsanvisning till stadens riktlinje för informationssäkerhet.

Ledningens genomgång med 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.

---

[1] Stockholms stads kvalitetsprogram (start.stockholm)

[2] I riktlinje för informationssäkerhet i Stockholms stad beslutad av kommunfullmäktige 2022-02-21, Dnr: 2021/866 står att ”Stadens inriktning är att informationssäkerhetsarbetet inom nämnder och styrelser ska utgå från den internationella standarden SS-ISO/IEC 27001/2. Informationssäkerhetsarbetet ska alltid utföras med hänsyn tagen till stadens övergripande mål samt till nämnders och styrelsers egna verksamhetsuppdrag.”

SISAB, Skolfastigheter i Stockholm AB

Postadress:
Box 5010
121 05 Johanneshov

Besöksadress:
Palmfeltsvägen 5, våning 5
121 62 Johanneshov

Tel: 08-508 460 00
e-post: diarie@sisab.se
webbadress: www.sisab.se

Org.nr: 556034-8970
Styrelsens säte: Stockholm
En del av Stockholms stad

Alla nämnder och bolagsstyrelser ska prioritera att inventera och klassa informationstillgångar som används i verksamheten alternativt se över och uppdatera genomförda informationsklassningar enligt tillämpningsanvisningarna till stadens riktlinje för informationssäkerhet.

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 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 riktlinje för informationssäkerhet och tillhörande tillämpningsanvisning som är bilagor till stadens kvalitetsprogram. Tillämpningsanvisningen revideras årligen och fastställs av stadsdirektören. Tillämpningsanvisningen reglerar ansvar och roller sett till Stockholms stads systematiska informationssäkerhetsarbete.

SISAB har utarbetat en lokal tillämpningsanvisning LTA för informationssäkerhet som specificerar hur stadens övergripande ledningssystem och insatser appliceras inom SISAB. För att upprätthålla ett informationssäkerhetsarbete som är aktuellt över tid ska SISAB 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.

Omvärldsbevakning- Förändringar i externa och interna frågor som är relevanta för ledningssystemet för informationssäkerhet

Krav på informationssäkerhet baseras dels på interna verksamhetskrav, dels på rättsliga och avtalsmässiga krav samt utifrån krav från intressenter. Informationssäkerhetsarbetet är därför inte isolerat, utan SISAB:s informationssäkerhet integreras i alla verksamhetsprocesser och samordnas med ledningsarbetet.

Vid internt utvecklingsarbete, särskilt vid framtagande av nya digitala tjänster, ska säkerställas att informationssäkerhets- och dataskyddsfrågorna alltid lyfts fram och ingår i arbetet.

Lagstiftning och avtalsmässiga krav

SISAB ser ständigt över de lagar och krav som är relevanta för verksamheten.

Övrig påverkan

I Kommunfullmäktiges beslut till budget 2025 [3] anges att beredskapsförmågan ska fortsätta öka, exempelvis genom att analysera och hantera risker- och sårbarheter samt genom krisledningsplanering, kontinuitetshantering, systematiskt

[3] stockholms-stads-budget-2025.pdf

informationssäkerhetsarbete, krigsorganisation samt årliga, obligatoriska krisledningsövningar.

Risk och sårbarhetsanalys (RSA)

Stadens arbete med risk- och sårbarhetsanalys (RSA) bedrivs i en tvåårscykel. En ny cykel inleddes under 2024. Under 2025 kommer arbetet fokusera på kontinuitetshantering. Gällande informationssäkerhet lyfts risken ”brist eller bortfall av infrastruktur/system” vilket kan innebära att tillgång till system försvåras eller omöjliggörs, att daglig drift påverkas samt risk för informationssäkerhetsincident.

Resultat av egen uppföljning (IKP)

Enligt Internkontrollplanen (IKP) V17 för 2025 kan vi se att arbetet för att tydliggöra hur SISAB arbetar med informationssäkerhet samt hur information ska klassificeras (utöver GDRP)- pågår. Detta arbete behöver intensifieras för att skapa ett fullständigt ramverk för informationssäkerhet. En bristande struktur kan leda till risken att SISAB:s medarbetare saknar insyn i var information finns, leder till ökad sårbarhet för integritetsintrång och säkerhetsincidenter samt kan leda till bristande efterlevnad av regulatoriska krav (exempelvis bevarande och offentlighetsprincipen) samt varumärkesrisker. Brist på informationssäkerhet kan leda till felaktigt fattade beslut samt att beslut tas på fel grunder.

Resultat från revisioner

Under år 2023 har inga rekommendationer från revisionen lämnats om informationssäkerhet.

Information om informationssäkerhetens prestanda

Ett bra informationssäkerhetsarbete är en förutsättning för effektiv och korrekt informationshantering.

Lokala tillämpningsanvisningar avseende roller och ansvar, övergripande informationssäkerhet samt instruktioner för olika områden har tagits fram och några är reviderade.

- Instruktion utifrån anvisning för distansarbete
- Instruktion för informationssäkerhet och GDPR-incidenter
- Instruktion för informationsklassning A-Ö
- Instruktion för videomötestjänster
- Utbildning cybersäkerhet på SISAB

De lokala tillämpningsanvisningarna kompletterar stadens centrala riktlinjer och tillämpningsanvisningar för informationssäkerhet och beskriver hur SISAB tillämpar de övergripande reglerna av informationssäkerhetsarbetet, roller och ansvar i den egna verksamheten.

Informationshanteringen inom SISAB ska bedrivas på ett sätt som tillgodoser interna behov och externa krav på informationssäkerhet. Rutiner/Instruktioner och interna

processer för att SISAB skall kunna bedriva ett systematiskt och fungerande informationssäkerhetsarbete håller på att etableras.

Avvikelser och korrigerande åtgärder

Arbete med att identifiera avvikelser och korrigerande åtgärder pågår. SISAB har inom vissa områden, så som Antura och T-LAN, arbetat systematiskt med organisationens informationstillgångar, intressenters krav och identifierade risker. Kartläggningen ger stöd i vilka säkerhetsåtgärder som organisationen behöver, hur väl åtgärderna fungerar idag och vilka åtgärder som bör prioriteras för att minska organisationens risker och få en bättre anpassad informationssäkerhet i organisationen.

Incidentrapportering/statistik

Under 2024 har 14 stycken informationssäkerhetsincidenter rapporterats i IA-systemet. Av dessa incidenter kan två betraktas som verksamhetsrelaterade incidenter. Händelser som inrapporterats som spam och bluffmejl eller dylikt har inte identifierats som verksamhetsrelaterade så länge det är inrapporterat som informativ information och inte har lett till någon verksamhetspåverkande incident. Däremot har incident rörande IT-säkerhet- PDF med trojan, inbrott på kontor och filmer på sociala medier lett till att verksamheten riskerats att påverkas.

Resultat från övervakning och mätning

Informationssäkerhetssamordnare (ISAM) arbetar tillsammans med identifierade informationsägare med verktyg för efterlevnad som fungerar som hjälp för organisationen att stämma av organisationens efterlevnad av standarden SS/EN ISO 27001.

Identifiering av processer och oönskade händelser

Av bolagets cirka 80 system och tjänster har 18 st av bolagets system och tjänster klassats, 17 har en tydlig handlingsplan varav riskanalys gjorts för 10 st.

Vid varje klassningstillfälle har arkivfunktionen deltagit för att implementera hanteringsanvisningarna som under hösten 2024 har reviderats, där revidering framförallt har berört HR, servicecenter och informationssäkerhet och GDPR.

Bolagets register över behandling, registerförteckning, är ej helt processbaserad och genomförd utifrån hanteringsanvisningarna.

Värdering och hantering av oönskade händelser

Många av verksamhetens informationstillgångar saknar informationsklassning. Dock har bolagets viktigaste system prioriterats och system, som enligt stadens nya tjänsteavtal ska flyttas, har klassats. Arbetet fortsätter under 2025 med att informationssäkerhetsklassa tillgångarna enligt årshjulet[4].

[4] Lokala tillämpningsanvisningen Dnr SISAB 2025/42

Åtgärder i handlingsplan från genomförda riskanalyser ska också tas om hand. Vissa risker är beroende av andra händelser och därför är rekommendationen för organisationen att koppla samman säkerhet med trygghet (fysiskt och organisatoriskt) för att på sikt åstadkomma bättre motståndskraft mot oönskade incidenter. Med avsikten av oönskad händelse menas risken för att informationen hanteras felaktigt. Det behöver belysas ur flera perspektiv. Informationstillgångar definieras inte enbart av system. Informationstillgångar är organisationens information och de resurser som behandlar informationen, exempelvis genom att ta emot, lagra, bearbeta, visa eller kommunicera den. Informationstillgångar är de tillgångar som informationssäkerheten ska skydda.

Hur påverkas verksamheten om informationen förvanskas, försvinner eller hamnar i orätta händer? Korrekt informationshantering behöver säkerställas inom verksamheten.

Obligatoriska utbildningar inom Informationssäkerhet för medarbetare i staden

2024-11-26 hade 139 medarbetare, inklusive extern inhyrd personal (konsulter), genomfört stadens obligatoriska utbildningar inom dataskydd och informationssäkerhet. Utav dessa 139 var 25 chefer på SISAB. Information har gått ut till samtliga berörda chefer som har återkopplat om att de skall påminna sina medarbetare om att genomföra utbildningen.

Årshjul

Anger informationssäkerhetssamordnarens årliga plan för informationssäkerhetsarbetet.

Årshjulet utgår från stadens tillämpningsanvisningar för informationssäkerhet, SISAB:s informationssäkerhetsmål och övrigt som framkommer under verksamhetsåret inklusive dataskydd.

Regelbundna aktiviteter som genomförs årligen.

Några rekommendationer i DSO-årsrapport:

- Roll och ansvar för dataskydd i verksamhetsprocesserna, utifrån hanteringsanvisningarna, behöver sättas för att kunna systematiskt hantera t.ex. en begäran om tillgång till personuppgifter, ett registerutdrag.
- Arbetet med att uppdatera och förteckna personuppgiftsbehandlingar processbaserat i ett behandlingsregister behöver fortsätta under 2025 för att bland annat säkerställa laglig grund för hantering av personuppgifter.
- Fortsätta att ta fram styrdokument, strategier och uppdatera instruktioner såsom exempelvis angående de registrerades rättigheter, så som rätten till radering.
- Fortsätta att implementera tekniska och organisatoriska åtgärder i enligt med dataskyddspraxis, som exempelvis kryptering och pseudonymisering.
- Årlig översyn av integritetspolicy och instruktion-rutin för att säkerställa att integritetspolicyn intern- och extern tydligt informerar enligt gällande praxis.
- Införliva den nya mallen för konsekvensbedömning avseende dataskydd i verksamheten, likaså stadens mall för tredjelandsöverföringsbedömning.

Planerade och genomförda aktiviteter samt planering inför kommande år

ISAM övriga händelsestyrda uppgifter:

- incidenthantering

- informationsklassningar
- följa upp anställningsförändringar - behörighetsrevision
- följa upp framtagna instruktioner
- kravhantering inför inköp/anskaffning system/tjänst och molntjänster
- remisshantering
- utbilda specifika målgrupper
- säkerställa systemlista med objektägare/processägare
  genomföra säkerhetsmånad i oktober

SISAB har arbete kvar avseende informationssäkerhetsklassificeringar samt även fortsatt utveckling av medarbetares kompetens där stadens obligatoriska utbildning är fortsatt prioriterat under 2025 och kommande år. SISAB har under 2024 även tagit fram en egen cybersäkerhetsutbildning. De informationsklassningar som tidigare genomförts har flera klassats om under 2024, då bland annat flytt av servrar till stadens nya tjänsteavtal krävde aktuella klassningar.

Att tillsammans med driftleverantör säkerställa tekniska säkerhetskrav är ett arbete som kvarstår inför NIS2 och cybersäkerhetslagen där hela kedjan ska stå robust och ha motståndskraft att stå emot olika former av angrepp. Detta är även viktigt ur ett dataskyddsperspektiv då praxis på området utvecklas hela tiden och påverkar tekniska och organisatoriska säkerhetskrav. Rutiner för ett systematiskt informationssäkerhetsarbete har reviderats och årshjul har också anpassats för att det löpande informationssäkerhetsarbetet, informationssäkerhetsmål och verktyg för ett strukturerat informationssäkerhetsarbete ska kunna bedrivas systematiskt efter SISAB:s behov.

Informationssäkerhetsmål

Stadens tillämpningsanvisningar för informationssäkerhet består av övergripande mål. Målen har anpassats till SISAB:s lokala behov. Kortsiktiga informationssäkerhetsmål är mål som direkt eller indirekt uttrycker hur SISAB som organisation på cirka 1-2 år ska arbeta för att uppnå verksamhetens långsiktiga strategiska mål. De kortsiktiga målen är konkreta och har en tydlig koppling till de analyser som organisationen har gjort.

Effektmål anger vilken effekt SISAB eftersträvar på lång sikt genom organisationens informationssäkerhetsarbete. Målen handlar om hur SISAB ska stödja och förbättra organisationens informationssäkerhetsarbete. Resultatmål anger vilka resultat SISAB eftersträvar på lång sikt genom organisationens informationssäkerhetsarbete. Dessa mål handlar mer övergripande om hur SISAB som organisation långsiktigt ska arbeta med informationssäkerhet.

Resultat från riskbedömning och status för riskbehandlingsplan

Riskbedömning är processen för att bestämma hur allvarlig en risk är. Allvarlighetsgraden bestäms utifrån en sammanvägning av både sannolikhet för risken och dess konsekvenser. Handlingsplan är en ”att-göra-lista” som tar upp åtgärder som inte kan genomföras omedelbart.

SISAB:s riskbedömning genereras genom arbetet med informationsklassning. En handlingsplan erhålls efter klassningsarbetet. Handlingsplanen ligger till grund för

riskanalysen där ställning skall tas över om standardåtgärderna är tillräckliga. Riskerna förs in i en åtgärdsplan (verktyg-utforma-åtgärdsplan).

Dataskyddsförordningen och Integritetsskyddsmyndigheten ställer upp kriterier för när en konsekvensbedömning avseende dataskydd ska genomföras, likaså vad som är dataskyddsrisker som har påverkan på individ.

Kvarstår på bolaget är att säkerställa att systemöversikten/systemlista med användningsområde får en systemägare/objektägare för samtliga tjänster och att verksamheterna också representeras med objektägare samt objektledare.

Möjligheter till ständig förbättring 2025-2026

Under 2025 och 2026 föreslås följande prioriterade åtgärder som aktiviteter:

- att informationssäkerhet och dataskydd är en stående punkt på SISAB:s informationsförvaltningsforum
- att modeller som tas fram inom exempelvis informationsförvaltarforum måste utgå från lagstiftning som dataskyddsförordning och informationssäkerhet NIS
- att bolagets klassificeringstruktur och hanteringsanvisningar efterlevs processtyrt
- att informationssäkerhet ingår i alla inköp/upphandlingar samt följs upp vid leverantörsmöten

Planerade och prioriterat arbete och aktiviteter under kommande perioder

SISAB behöver sammanfattningsvis:

1. Arbeta med att klassningars handlingsplaner fullföljs
2. Tilldela informationsägare till respektive system - roller och ansvar i systemlistan med verksamhetsspecialister(objektägare och objektledare)
3. Fortsätta implementering av lokal anvisning
4. Implementera incidenthantering, informationsklassning och informationssäkerhet inom upphandlingsförfarande
5. Följa upp utbildningsinsatser för chefer och medarbetare/konsulter
6. Kontinuitetsplanera för motverka risker som är identifierade och prioriterade enligt RSA