Stockholms stad

Ledningens genomgång informationssäkerhet 2026

Svenska Bostäder

Beslutad 20 januari 2026

Ledningens genomgång

Dnr: SB 2026/23

Kontaktperson: Abdullahi Ahmed

Sammanfattning

I *Ledningens genomgång* 2026 sammanfattas de viktigaste åtgärderna som bolaget vidtagit för att stärka informationssäkerheten under 2025 och vilka aktiviteter som planeras för 2026. Rapporten är strukturerad för att ge en tydlig bild av hur vi har kommit fram till våra prioriteringar genom att ta hänsyn till flera faktorer som påverkar vårt ledningssystem för informationssäkerhet (LIS), inklusive internkontrollplanen (IKP), omvärldsbevakning och GDPR-årsrapporten.

Under 2025 har vi gjort framsteg i arbetet med informationssäkerhet, dataskydd och IT-säkerhet. Bland de viktigaste insatserna märks ett stärkt arbete med informaitonsklassning, förbättrad hantering av personuppgifter och leverantörsavtal samt utvecklad incidenthantering och omvärldsbevakning. Dessa åtgärder har lagt en stabil grund för att möta både en ökad hotbild och nya regulatoriska krav, såsom ny cybersäkerhetslagstiftningen.

Genom att analysera dessa faktorer har vi kunnat definiera våra prioriterade åtgärder för 2026. Fokus för det kommande året ligger på att förenkla och effektivisera det systematiska informationssäkerhetsarbetet, stärka styrning och sårbarhetshantering samt säkerställa en riskbaserad implementering av kraven i NIS2. Parallellt prioriteras fortsatt utveckling inom leverantörsgranskning, utbildning och kommunikation för att öka både den organisatoriska och den tekniska motståndskraften. Dessa åtgärder beskrivs närmare i kapitel 3.

Sammanfattningsvis ger rapporten en vägledning för hur Svenska Bostäder planerar att vidareutveckla informationssäkerhetsarbetet under det kommande året. Genom ett fortsatt fokus på struktur, kompetens och riskbaserade arbetssätt skapar vi goda förutsättningar för att möta framtida utmaningar och säkerställa att informationssäkerheten även framöver är en integrerad och proaktiv del av verksamheten

Innehållsförteckning

1. Vad är Ledningens genomgång

Informationssäkerhet handlar om att hantera och skydda information på ett strukturerat sätt för att säkerställa dess tillgänglighet, riktighet, konfidentialitet och spårbarhet. Eftersom Svenska Bostäder hanterar stora mängder information är ett systematiskt informationssäkerhetsarbete avgörande för att upprätthålla trygghet, följa lagkrav och säkerställa en effektiv verksamhet.

En viktig del av detta arbete är Ledningens genomgång, en årlig översyn som ger en samlad bild av informationshanteringens status. Den omfattar bland annat uppdaterade externa och interna krav, resultat av riskanalyser samt förbättringsförslag för de mest prioriterade aktiviteterna. Genomgången är därmed ett verktyg för att identifiera förbättringsområden och driva kontinuerlig utveckling.

För att stärka och styra detta arbete genomför Svenska Bostäder Ledningens genomgång som en del av verksamhetsplaneringen. Genom att analysera nuläget och formulera en strategi för det kommande året skapas en tydlig riktning för hur informationssäkerheten kan utvecklas och anpassas efter verksamhetens behov.

1.2 Viktiga förbättringar under 2025

Under året har flera betydande åtgärder genomförts för att stärka informationssäkerhet, dataskydd och IT-säkerhet både för verksamheten och våra kunder. Exempel på genomförda förbättringar inkluderar:

Informationsklassning

- Bolagets samtliga informationstillgångar har klassats i enlighet med hanteringsanvisningar och processtyrning.

Hantering av dataskydd/informationssäkerhet inom leverantörsavtal

- Uppdaterat PUB-avtal med leverantörskontakter och upprättat en ny PUB-mall.
- Säkerställt att det finns underbiträdesavtal
- Stöttat verksamheten med rådgivning och sakgranskning i samband med upphandling eller förändring i leverantörsavtal.

- Genomfört konsekvensbedömning och upprättat en bolagsanpassad riktlinje för personer med skyddad identitet.

IT-säkerhetsarbetet

- Ökat säkerheten i inloggning (SSO) till flera viktiga verksamhetssystem, så som Agda och Planima
- Överfört samtliga lokala verksamhetssystem till nya Systemtjänsteavtalet med ökad fokus på säkerhet
- Upparbetat en rutin för att identifiera och hantera sårbarheter i våra verksamhetssystem för att minska risken att hotaktörer kan nyttja kända sårbarheter för att olovligen komma åt bolagets system och information.

Förbättrad incidenthantering

- Incidenter som anmäls till dataskyddsfunktionen registreras och dokumenteras i stadens incidenthanteringssystem IA, i stället för Excel.

Information och utbildning

- Medarbetare har regelbundet informerats via Svebben om nätfiske och incidenter inom staden, bolaget och hos underleverantörer.
- Utbildat processägare och processamordnare i informationssäkerhet.
- Informerat om dataskydd och informationssäkerhet på SB live, digitala skärmar och Svebben.
- Uppdaterat information på externa webb om registrerades rättigheter enligt GDPR.

Utveckling av arbetssätt för informations- och IT-säkerhet

- Under 2025 införde vi ANTS (automatiska notifieringar för tekniska sårbarheter, vilket ger tidiga varningar om kritiska brister.
- Vi utvecklade även vår omvärldsbevakning genom CERT-SE**:s** veckobrev, som ger en löpande bild av aktuella hot och risker. Vi samverkar nu med CERT Stockholm, stadens nya gemensamma operativa funktion för IT-säkerhet, vilket ger snabbare stöd och bättre samordning vid incidenter. Vi får nu stöd att övervaka publika tjänster.
- Informationssäkerhetsrådet har återetablerats och fungerar nu som en länk till företagsledningens it-styrgrupp.
- Under året har ett närmare samarbete etablerats mellan IT-enheten och Informationsförvaltningsenheten vilket har stärkt den praktiska tillämpningen och vidare utvecklingen av informations- och IT-säkerhetsarbetet.

2. Faktorer som påverkar verksamhetens LIS

Det systematiska informationssäkerhetsarbetet påverkas av externa krav som såsom ISO 27001-certifieringen och GDPR, vilka ligger till grund för stadens riktlinjer. Dessa, tillsammans med bolagsstyrelsens och ledningens krav, styr verksamhetens arbete. Genom ett riskbaserat tillvägagångssätt identifieras och hanteras hot, vilket säkerställer både regelefterlevnad och ständig förbättring.

2.1 Omvärldsbevakning – hot, trender och ny lagstiftning

Ny Cybersäkerhetslag (CSL) och cybersäkerhetsförordning kopplad till NIS2

EU antog 2022 ett direktiv om åtgärder för en hög gemensam cybersäkerhetsnivå inom unionen, det så kallade NIS 2-direktivet. Med anledning av detta utfärdade regeringen den 11 december en ny cybersäkerhetslag och en ny cybersäkerhetsförordning. Båda börjar gälla den 15 januari 2026. Myndigheten för civilt försvar kommer att ta fram närmare föreskrifter kring den nya lagstiftningens implementering. Bolaget bevakar området för att säkerställa regelefterlevnad.

AI-förordningen

AI-förordningen ska säkerställa att AI-system inom EU är säkra, tillförlitliga och används på ett ansvarsfullt sätt, särskilt inom områden där fel kan få stora konsekvenser. Reglerna för högrisk-AI var ursprungligen planerade att börja gälla den 2 augusti 2026, men har efter dialog med både industri och medlemsstater skjutits fram till den 2 december 2027. Samtidigt har arbetet med tekniska standarder försenats, vilket har skapat viss osäkerhet för både utvecklare och användare av AI-system. För bolaget innebär detta att vi under 2026 fortsätter dialogen med berörda leverantörer och säkerställer att upphandlingar av tjänster som innehåller AI-funktioner tar höjd för de kommande kraven.

2.2 Vad händer inom staden – budget, inriktningar, lokala förändringar eller satsningar

Budget 2026

I Stockholms stads budget direktiv till samtliga nämnder och bolag anges att dessa ska:

- utveckla och stärka arbetet med informationssäkerhet samt beakta risker och sårbarheter kopplade till generativ AI och syntetisk media.

I budgeten konstateras att dataläckage inom offentlig sektor visar behovet av stärkt informationssäkerhet.[1]

Ny inriktning för informationssäkerhetsarbetet i staden

Under hösten 2025 har staden genomfört en översyn av ledningssystemet för informationssäkerhet (LIS). Bakgrunden är ökade krav från den nya cybersäkerhetslagstiftningen, stärkt motståndskraft samt det förändrade säkerhetspolitiska läget. Översynen visar att nuvarande arbetssätt behöver utvecklas för att bättre kunna möta dessa förutsättningar. För att möjliggöra en övergång till ett mer riskbaserat cybersäkerhetsarbete planeras följande åtgärder:

- Förenkla och standardisera grundläggande processer inom informationssäkerhet och dataskydd. Med processer menas bland annat arbetet med registerförteckning, klassning, riskanalys och skyddsfaktorer inom IT-säkerhet.
- Frigöra tid för riskhantering och åtgärder ur ett allriskperspektiv.
- Förbättra den stadsövergripande incidenthanteringen.

Efter årsskiftet bjuder staden in till möten där den nya inriktningen för informationssäkerhetsarbetet presenteras, med fokus på nya arbetssätt, bättre systemstöd och en tydligare tidsplan. Samtidigt får bolaget möjlighet att delta i utvecklingen av det uppdaterade ledningssystemet för informationssäkerhet, kallat LIS 2.0**.**

Nytt regelverk för stadens IT-system – projekt LångSIKT

SLK IT har beslutat om ett nytt regelverk för stadens IT-system som påverkar systemarkitektur och nätverkskommunikation för flera av våra verksamhetssystem. Under 2026 pågår projektet LångSIKT som avser att genomföra förändringar av de system som inte uppfyller kraven i det nya regelverket.

CERT Stockholm stöd vid it-säkerhetsincidenter.

[1] Stockholms stads budget 2026

CERT Stockholm [2] är Stockholms stads gemensamma operativa cybersäkerhetsfunktion, med uppdrag att stärka stadens förvaltningar, bolag och stiftelsers förmåga att förebygga, upptäcka och hantera it-säkerhetsincidenter. Det en stödjande funktion som ansvarar för att rådge, koordinera samt samla och sprida kvalitetssäkrad information. Under 2025 har staden etablerat nya centrala tjänster inom cybersäkerhet genom CERT Stockholm. Fokus ligger på förebyggande arbete med sårbarhetsskanning och omvärldsbevakning, samt stärkt incidenthantering och samordning vid IT-incidenter.

2.3 Vad har verksamheten identifierat i RSA-arbetet

2.3.1 Riskanalys kopplad till hantering av skyddad identitet

Under året genomfördes ett fördjupat riskanalysarbete med fokus på hantering av personer med skyddad identitet. Arbetet genomfördes i en särskilt sammansatt grupp bestående av processägare och processamordnare från berörda verksamhetsprocesser.

Syftet var att systematiskt identifiera och bedöma processpecifika **risker** kopplade till informationshantering, behörigheter, systemstöd och arbetssätt i de delar av verksamheten där skyddad identitet förekommer.

Arbetet omfattade:

- Kartläggning av informationsflöden i respektive process,
- Analys av hur personuppgifter hanteras i olika system och moment, samt
- Genomförde riskanalys och tog fram riskmatriser per verksamhetsprocess

Riskanalysen visade på behov av tydligare styrning och mer enhetliga arbetssätt inom hela organisationen. Resultatet av arbetet blev därför framtagandet av en bolagsanpassad riktlinje för hantering av personer med skyddad identitet**,** som nu utgör ett styrdokument i verksamhetens informationssäkerhets- och dataskyddsarbete.

[2] Computer Emergency Response Team

2.3.2 Informationsklassning

Under året genomfördes ett stort informationsklassningsprojekt där samtliga bolagsprocesser analyserades. Arbetet resulterade i uppdaterade klassningsbedömningar.

Efter det omfattande arbetet med informationsklassning blev det tydligt att vi har goda möjligheter att vidareutveckla och stärka våra arbetssätt. Erfarenheterna från genomgången låg till grund för beslutet att under 2026 ta fram en samlad informationskartläggning med informationskatalog samt att förenkla valet av tekniska och administrativa skyddsåtgärder. Syftet är att frigöra mer tid för informationsägare och skapa ännu bättre förutsättningar för den praktiska implementeringen av skyddsåtgärder. Arbetet genomförs i samordning med stadens utveckling av det nya ledningssystemet för informationssäkerhet, LIS 2.0

2.4 Resultatet från egen uppföljning (VoR och IKP)

Under 2025 vidtogs åtgärder för de risker som identifierades i väsentlighets- och riskanalys (VoR 2024), där oönskade händelser inom informations- och IT-säkerhet kunde leda till spridning av känslig information, dataförluster och bristande regelefterlevnad.

För att hantera risker rekryterades en informationssäkerhetsamordnare, ISAM, som har lett arbetet med klassning av informationstillgångar, uppdatering av styrande dokument, utbildningar, risk- och incidenthantering och uppföljning av personuppgiftsbiträdesavtal. ISAM har tydliggjort roller och ansvar i organisationen och bidragit till ett långsiktigt och systematiskt informationssäkerhetsarbete.

Upp till 67 procent av bolagets medarbetare och konsulter har genomgått eller förnyade sina certifikat i e-utbildning *Informationssäkerhet* och e-utbildning *Dataskydd* inom Stockholms stad.

2.5 Risker som identifierats i GDPR-årsrapport

GDPR- årsrapporten för 2025 bedömer dataskyddsombudets (DSO) att bolagets dataskyddsarbete i huvudsak fungerar bra. Vi har en grundläggande struktur för hantering av personuppgifter, med fastställda rutiner, tydliga ansvarsförhållanden och en generell

medvetenhet om dataskyddsförordningens (GDPR) krav. Registerförteckningar och informationssäkerhetsåtgärder är till största delen på plats, och arbete med personuppgifts-incidenter samt hantering av inkommande ärende gällande registerutdrag hanteras löpande.

Samtidigt finns förbättringsområden som behöver hanteras under 2026. Det gäller framför allt förståelsen av alla registrerades rättigheter, dokumentation av riskerna i riskbedömningar samt dokumentation av leverantörskedjor. Genom att stärka det systematiska arbetet och säkerställa kontinuitet i uppföljning och kompetensutveckling kan dataskyddsarbetet förbättras ytterligare och risken för bristande regelefterlevnad minskas. [3]

Rekommendationerna utgör ett stöd för fortsätt utveckling av dataskyddsarbetet och är ett viktigt underlag i planeringen av de prioriterade åtgärderna för 2026 (kapitel 3).

2.6 Information om avvikelser (incidenter och andra händelser)

Under 2025 rapporterades totalt 24 personuppgiftsincidenter. Majoriteten av dessa avser handhavandefel, där information av misstag skickats till fel mottagare via e-post eller andra kanaler.

Under året har bolaget utsatts för ett antal phishingförsök. Även flera av våra underleverantörer har drabbats av intrångsförsök, och i ett fall har en leverantör informerat oss som berörd kund. Phishingattackerna har blivit mer avancerade, riktade och tajmade med hänsyn till exempelvis semesterperioder, organisationens struktur och arbetsbelastning, för att öka risken att medarbetare under stress ska missa varningssignaler. Under hösten noterade vi bland annat flera försök till bluffakturor veckan innan chefer skulle attestera fakturor.

Vår leverantör Miljödata drabbades under året av ett dataintrång som resulterade i en tillgänglighetsincident. Händelsen påverkade åtkomsten till flera system hos Miljödata, men enligt leverantören gick ingen information förlorad och ingen data ändrades. Den berörda informationen rörde personaluppgifter hos anställda, bland annat dokumentation kopplad till avstämningssamtal, frånvaro och rehabilitering. Incidenten har anmälts till Integritetsskyddsmyndigheten (IMY) i enlighet med gällande regelverk.

[3] DSO årsrapport 2025

3. Förbättringar som föreslås för verksamheten

Detta kapitel går igenom de planerade åtgärderna för 2026. De föreslagna åtgärderna bygger på de faktorer som påverkar ledningssystemet för informationssäkerhet (LIS), vilket beskrivs i kapitel 2. Dessa faktorer inkluderar resultat från omvärldsbevakning, riskanalys, internkontrollplan samt revisioner. De prioriterade åtgärderna för 2026 utgör därmed både ett svar på identifierade brister och ett strategiskt steg mot ett mer moget och motståndskraftigt informationssäkerhetsarbete.

3.1 Prioritering av åtgärder 2026

Informationssäkerhetsstyrning

Förenkla och effektivisera det systematiska informationssäkerhetsarbetet.

- Informationskatalogen med samlad förteckning över informationstillgångar, klassningsresultat, system och leverantörsavtal.
- Enkätverktyg införs som stöd för kartläggning, uppföljning och mognadsmätning inom informationssäkerhet.
- Fortsatt stöd till verksamheten i arbetet med informaitonsklassning och riskanalys.
- Skyddsåtgärdspyramiden ny version med uppdaterade tekniska och administrativa skyddsåtgärder.

Styrande dokument

- Uppdatera *Lokal anvisning för informationssäkerhet*
- Årlig översyn av styrande dokument inom informationssäkerhet och dataskydd
- Stödja verksamheten i årlig översyn av lokala rutiner så att de följer både lagkrav och bolagets riktlinjer.

- Bidra och medverka i stadens utveckling av ett nytt ledningssystem för informationssäkerhet LIS 2.0.

Sårbarhetshantering

- Färdigställa och införa en bolagsanpassad process för sårbarhetshantering i samverkan med IT enheten. Processen utgör en central del av arbetet med tekniska skyddsåtgärder

och kontinuerlig riskreducering och omfattar både utveckling av övergripande process samt tillhörande rutiner, med metodstöd från SLK och CERT Stockholm**.**

Cybersäkerhetslagen (NIS2)

- Skapa en gemensam förståelse för NIS2 samt ta fram en handlingsplan för implementering.
- Utveckla ett riskbaserat arbetssätt för prioritering, genomförande och uppföljning av åtgärder inom ramen för handlingsplanen, i linje med kommande föreskrifter och vägledning från MSB.
- Anpassa och stärka incidenthanteringsprocessen för berörda OT-system i enlighet med NIS2:s krav på rapportering, tidsramar och eskalering, inklusive registrering i MSB:s nya incidenthanteringsportal när denna lanseras.
- Stärka efterlevnaden av cybersäkerhetslagen (NIS2) genom riktade utbildningsinsatser, med stöd i MSB:s föreskrifter och vägledning när dessa är på plats.

Leverantörsgranskning

- **Genomföra riskbaserade leverantörsgranskningar** av leverantörer av IT-stödverktyg i syfte att säkerställa efterlevnad av informationssäkerhetskrav (t.ex. ISO 27001, NIS2, GDPR och kravbilden enligt NIS2).

Utbildning och kommunikation

- Utbildningsinsatser med gamification för att stärka lärandet genom utbildningsinsatser med gamification som ökar engagemang och efterlevnad.

- Utbildning i dataskydd och nya systemsstöd version – införandet av ny version av Draftit med riktat stöd till processägare och processamordnare, inklusive utbildning enligt DSO:s rekommendationer, för att säkerställa effektiv tillämpning i det systematiska informationssäkerhetsarbetet.

- Utbildning och kommunikation inom informationssäkerhet inkluderar utveckling av skräddarsydda e-utbildningar anpassade efter målgruppernas behov, med målsättning att säkerställa enhetliga budskap och effektiv kunskapsöverföring.

- Långsiktig utbildning & kommunikationsplan i syfte att stärka och höja säkerhetskulturen inom bolaget.