Stockholms stad

Ledningens genomgång Bromma stadsdelsnämnd 2025

Beslutad 2025-XX-XX

start.stockholm

Ledningens genomgång Bromma stadsdelsnämnd 2025
December 2025
Dnr: BRO 2025/600
Kontaktperson: Maria Palme

Sammanfattning

Dokumentet Ledningens genomgång innehåller analyser och förslag på aktiviteter för att förbättra dataskyddsarbetet. Genomgången ska ge information och underlag till stadsdelsdirektören att årligen bedöma om det lokala informationssäkerhetsarbetet och dataskyddsarbetet är tillräckligt och har önskad verkan. I den här rapporten är det endast det övergripande informationssäkerhets-arbetet som beskrivs.

Bromma stadsdelsförvaltning och staden arbetar utifrån standard ISO 27001. Här finns det beskrivningar på hur arbetet ska genomföras utöver de angivna riktlinjerna. Bromma ingår också i ett kluster som samarbetar i GDPR och informationssäkerhetsfrågor med stadsdelsförvaltningarna i Järva och Hässelby-Vällingby, också kallat Trillingen. Syftet är att i ett ökat hotklimat och krav från verksamhet och samhälle i frågorna, samarbeta och finna synergier.

Informationssäkerhet fastställs genom klassning och är en del av dataskydd utifrån fokus på IT-tjänstens utformning och skyddsvärde.

Skyddsnivåerna kopplas till den information som förvaras eller behandlas där rutiner för användare, systemens innehåll och utformning, samt var systemen finns placerade fysiskt.

Förbättringsförslagen i detta dokument rör dokumentation, budget och organisering för år 2026, 2027, 2028.

Efterlevnad av dataskyddsförordningen följs upp i Dataskyddsombudets årsrapport för dataskydd (GDPR-årsrapport) som biläggs nämndens verksamhetsberättelse för 2025. Ledningens genomgång kommer att redogöra kort vad GDPR-årsrapporten för 2024 kom fram till.

Förklaringar av förkortningar eller processer förklaras i särskild bilaga med länkar.

Innehåll

1. Ledningssystem för informationssäkerhet - LIS

Ledningssystem för informationssäkerhet (LIS) är ett stöd för hur informationssäkerhetsarbetet styrs i verksamheter vilket består av Stockholms stads övergripande tillämpningsanvisningar för informationssäkerhet samt de rutiner, guider och anvisningar som finns antagna. Bromma stadsdelsförvaltning har den 18:e december 2024 antagit lokala tillämpningsanvisningar. I de lokala tillämpningsanvisningarna finns till exempel:

- användning av internet och e-post
- åtgärder till skydd mot skadlig kod
- fysisk säkerhet
- incidenthantering
- mobilt arbete
- inventarier och licenser
- behörighetsadministration
- loggning.

En stor del av arbetet med att driva ett ledningssystem, handlar om att informera medarbetare om de regler som ingår i ledningssystemet.

Ledningens genomgång är en del i ett systematiskt informationssäkerhetsarbete. Ledningen ska hålla sig informerad om informationssäkerheten i sin verksamhet. Stadsdelsnämnden är informations- och personuppgiftsansvarig medan förvaltningschefen är operativt ansvarig och ska se till att resurser finns, samt att medarbetare har den utbildning och information som krävs för uppdraget.

Övergripande informationssäkerhetsansvarig finns på stadsledningskontoret. Lokalt i nämnden finns en informationssäkerhetssamordnare (ISAM). Informationssäkerhetens ansvar ska följa linjeorganisationens. Nämnden arbetar utifrån stadens riktlinjer och tillämpningsanvisningar och ska anta den lokala anvisningen.

Enligt Stockholms stads tillämpningsanvisning för informationssäkerhet ska förvaltningschef/bolagschef inhämta en rapport, 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 att årligen bedöma om det lokala informationssäkerhetsarbetet och dataskyddsarbetet är tillräckligt och har önskad verkan. Förvaltningschefen ska ta upp aktiviteter som rör informationssäkerhet och dataskydd i verksamhetsplaneringen, och i det interna arbetet uppnå tillräcklig intern kontroll.[1]

Inventering och informationsklassning är grunden i informationssäkerhetsarbetet. För 2026 ska verksamheterna fortsätta arbetet med inventering av nya system, processer, kontinuerligt uppdatera registerförteckning och revidera informationsklassningar. Det genomförda arbetet med verksamhetsnära rutiner behöver implementeras och vid behov revideras.

Stor vikt bör fortsatt läggas på rutiner för incidenthantering, övning av incidenthantering och uppföljning i det systematiska arbetet med lärdomar och förebyggande verksamhet, så kallade lessons learned.

Alla nämnder och bolagsstyrelser ska visa på förbättringar i arbetet som leder till ökat skydd för informationstillgångar

2. Omvärldsbevakning – hot, trender och ny lagstiftning

2.1 Utvecklingen av AI

Under 2024 antogs flera olika nya lagar som ska reglera och definiera vad man får och inte får göra med AI hjälpmedel.

Den nya så kallade AI-förordningen antogs av EU-parlamentet antog lagen i mars 2024, och ministerrådet i maj 2024. De flesta

[1] Tillämpningsanvisning till stadens riktlinje för informationssäkerhet

delarna kommer att börja gälla fullt ut 24 månader efter ikraftträdandet, men vissa delar kommer att tillämpas tidigare.

Utvecklingen av tekniken sker i snabb takt och eventuella hot är i dagsläget delvis okända. En utmaning är att säkerställa kvaliteten och ägarskapet/ upphovsrätten till utkomsten från AI:t samt hur felaktigt framtagen information ska rättas.

Nedan är utdrag som beskriver användandet av generativ AI, krav ställd på transparens och om verksamheter använder AI i exempelvis myndighetsutövning, kommer krav på hur beslut härleds och vilken information som ges till medborgare att AI används vara i fokus.

Generativ AI, som ChatGPT, klassas inte som hög risk, men måste uppfylla kraven på transparens och copyrightlagstiftning inom EU. Det krävs att tillverkare/ägare måste:

- Märka att innehållet har genererats av AI.
- Utforma systemet för att förhindra att produkten genererar olagligt innehåll.
- Offentliggöra sammanfattningar av upphovsrättsskyddade data som används för utbildning.

Kraftfull, generell AI som kan innebära systemrisker, exempelvis den mer avancerade modellen GPT-4, måste gå igenom omfattande undersökningar. Alla misstänkta resultat måste rapporteras till EU-kommissionen.

För all AI behandling krävs konsekvensbedömning enligt GDPR, riskbedömning enligt AI-förordningen och informationsklassning innan AI:t kan användas av verksamheten. Detta för att kontrollera att användningen följer lagstiftningen och eventuella risker kan omhändertas korrekt.

2.1.1 Påverkan Bromma stadsdelsförvaltning

AI-tekniken är ny och det finns en generell kompetensbrist i samhället om den. I Stockholm stad saknas det en central AI-riktlinje. Avsaknaden av styrande dokument påverkar förvaltningen genom att ramverk och inriktning för vad AI ska användas till saknas. Det gör att det finns en osäkerhet i vad exempelvis Svea GPT kan användas till.

Utvecklingen av tekniken sker i snabb takt och eventuella hot är i dagsläget okända.

Under 2025 har flertalet befintliga IT-tjänster fått AI:n implementerade, ibland utan vetskap i verksamheten.

AI är numera väldigt lättillgängligt, fler tjänster och produkter får AI inbyggt från start utan att användaren kanske är införstådd med att den arbetar i bakgrunden. I rollen som ISAM är det ett konstant arbete med att bevaka om och hur dessa tjänster finns med vid till exempel uppgraderingar av tjänster. ZoomX och ersättaren Nordic for Zoom är tydliga exempel på detta. Vid uppgraderingar och införande finns AI-funktioner med utan att dessa har informationssäkerhetsklassats innan driftsättning.

Förvaltningen ska uppmuntra och stödja verksamheterna i att använda AI på ett klokt och korrekt sätt. Medarbetare i förvaltningen kommer ofta till IT-strateg/ ISAM och DSO och vill använda AI i tjänsten. Ibland rör det sig om tjänster som förvaltningen redan vet är osäkra till exempel på grund av tredjelandöverföringar. Förvaltningen försöker då hitta andra tjänster som kan motsvara verksamhetens behov.

Utmaningen är att kunskap, förståelse och lagstiftning går långsammare än tekniken inträde i marknaden för produkter och tjänster. Detta kommer kräva både utbildningsinsatser, riktlinjer och alla medarbetares ansvar att förstå den teknik som möjliggörs och hur man hanterar den.

2.2 NIS2 –Cybersäkerhetslagen

Införandet av cybersäkerhetslagen (NIS 2) har skjutits upp flera gånger, så föregående års information om den nya lagstiftningen kvarstår. Den 15 januari 2026 föreslås lagen att träda ikraft enligt regeringens proposition *”Ett starkt skydd för nätverks- och informationssystem – en ny cybersäkerhetslag”*

NIS 1-direktivet (the directive on security of network and information systems) som antogs 2016, syftade till att öka EU:s medlemsländers informationssäkerhetsförmågor gällande nätverk och informationssystem för samhällsviktiga tjänster. NIS 1-direktivet omfattar flera sektorer. Den sektorn som träffar Bromma stadsdelsförvaltning är hälso- och sjukvård. Detta direktiv gäller just nu, men kommer ersättas av NIS 2.

NIS 2-direktivet är en uppdatering av NIS 1-direktivet och omfattar fler sektorer och krav kring cybersäkerhet. EU:s medlemsländers beroende till digitala tjänster och nätverk är stort vilket betyder att de cyberhot som finns måste adresseras och förebyggas, vilket kravställs i NIS 2-direktivet.

De sektorer som kommer omfattas av cybersäkerhetslagen är:

- Energi
- Transporter
- Bankverksamhet
- Finansmarknadsinfrastruktur
- Hälso- och sjukvårdssektorn
- Dricksvatten
- Avloppsvatten
- Digital infrastruktur
- Förvaltning av IKT-tjänster (mellan företag)
- Offentlig förvaltning
- Rymden
- Post- och budtjänster
- Avfallshantering
- Tillverkning, produktion och distribution av kemikalier
- Produktion, bearbetning och distribution av livsmedel
- Tillverkning
- Digitala leverantörer
- Forskning

2.2.1 Påverkan på Bromma stadsdelsförvaltning

Bromma stadsdelsförvaltning kommer träffas av två av sektorerna, *hälso- och sjukvård* och *offentlig förvaltning.*

2.3 Nya regler för kameraövervakning

Från den 1 april 2025 gäller nya regler för kamerabevakning. I och med de nya reglerna behöver inte längre ansökan om tillstånd för kamerabevakning göras hos IMY. Dock ska en intresseavvägning mellan bevakningsintresset och den enskildes intresse av att inte bli bevakad göras. Intresseavvägningen ska dokumenteras och den som bevakar ska även ha en förteckning med vissa uppgifter om den

kamerabevakning som bedrivs eller som har upphört de senaste fem åren.

2.3.1 Påverkan på Bromma stadsdelsförvaltning

I budgeten för 2026 uppmuntras stadens verksamheter till att använda möjligheten för kameraövervakning för att öka tryggheten för våra invånare. Viktigt är att förvaltningen gör arbetet med både intresseavvägning och informationssäkerhetsarbetet samt dokumenterar detta. IMY är tillsynsmyndighet för kamerabevakning och precis som med alla andra nya digitala objekt måste förvaltningen göra ett informationssäkerhetsarbete innan kamerabevakning, på varje enskild plats, sätts upp och aktiveras.

2.4 Datorer och mobiler och IOT (Internet Of Things)

Fler enheter kommer att bli uppkopplade och fler enheter än tidigare kommer att ha fast eller trådlös uppkoppling. Detta är i de allra flesta fallen önskvärt, men ställer allt större krav på att stadsdelen vet hur enheterna fungerar, och att vi förstår hur information flödar mellan olika system och tjänster. Ett exempel inom verksamheterna i Bromma är att vissa robotdammsugare har kameror för bättre rumsorientering.

2.4.1 Påverkan på Bromma stadsdelsförvaltning

De senaste årens trend med IOT börjar övergå till att bli etablerade på marknaden och ses inte längre som något nytt eller nydanande. Dock finns utmaningarna kvar då man inom en snar framtid kommer förvänta sig att alla enheter är mer eller mindre uppkopplade. Det gör att när man rör sig som medborgare eller anställda i olika miljöer kommer dessa enheter prata med varandra mer än någonsin i historien.

I de flesta fallen kommer detta vara önskvärt, exempelvis vill man att sin smartklocka ska synka med sin kalender, men då detta sker trådlöst finns risker med att man inte märker om data delas på ett felaktigt eller riskabelt sätt med andra enheter. Tidigare i historien behövdes oftast en mänsklig handling som nycklar, samtal eller annan mänsklig interaktion för att dela data, idag görs det osynligt och oftast ljudlöst utan någon uppenbar förvarning.

Detta kommer ställa stora krav på att enheter konfigureras och för myndigheter måste dessa styras med centrala och övervakade/proaktiva inställningar för tjänster och enheter.

2.5 Hotaktörer - cybersäkerhet

Det går att läsa följande i MSB:s rapport från 2020 ”De cyberhot som riktas mot Sverige är mångfacetterade och kan kopplas till flera olika typer av aktörer. I huvudsak kan de delas upp i statliga aktörer och kriminella grupperingar. I viss omfattning förekommer även ideologiskt motiverade aktörer, såsom hacktivister eller grupperingar med terrorkopplingar. Statliga aktörer som genomför cyberangrepp mot Sverige har oftast som syfte att inhämta information som kan gynna det egna landets utrikes- och säkerhetspolitiska intressen, eller att stärka det egna landets ekonomi och industriella utveckling genom industrispionage.

Kriminella grupperingar som genomför cyberangrepp vill i de flesta fall tjäna pengar genom till exempel ransomware-attacker där utsatta företag krävs på lösensummor, medan ideologiskt motiverade aktörer tenderar att agera enligt sina egna formulerade agendor.”

2.5.1 Påverkan på Bromma stadsdelsförvaltning

Omvärldsläget verkar fortfarande försämras med fler oroshärdar, fler konflikter både i Sverige och i omvärlden. Via olika nyhetsmedier rapporteras om både direkta krigshandlingar men också om påverkanskampanjer och desinformationskampanjer.

För Bromma så är de troligaste scenarion de som rör desinformation och dataintrång/dataförluster. Ett sätt att motverka detta är att ha god ordning på den information stadsdelen förvaltar, se till att den är korrekt och arkivbeständig samt att vi hanterar allmänna handlingar korrekt och utlämning sker skyndsamt. Ett exempel från 2025, är den så kallade Miljödataincidenten där både tidigare och nuvarande anställdas personuppgifter genom en attack mot leverantören sedan publicerades på Darknet.

Det är viktigt att Bromma stadsdelsförvaltning hanterar information korrekt och vi har transparens och förvaltar medborgares förtroende att hantera informationen.

En av åtgärderna är att värdera information så rätt skyddsåtgärder vidtas och att stödsystem upprättas för att hantera de ökande informationsmängderna.

3 Vad händer inom staden – lokala förändringar eller satsningar

I budgeten för 2026 ser Bromma stadsdelsförvaltning att informationssäkerheten har fått mer resurser. Det är glädjande att stadens centrala styrning tydligt pekar på att informationssäkerhet är en allt viktigare område och behöver få mer plats.

Under 2025 har staden blivit bättre på att genomföra normerande och samarbeta i dessa klassningar. Det finns mer systematik och metod men är personbundet att det utförs enligt arbetssättet från centrala förvaltningar. Socialförvaltningens arbetssätt att dela upp förvaltningarna i tre kluster (där trillingen är ett) och att respektive kluster får utse deltagare, har blivit ett allt mer tongivande arbetssätt i staden. Glädjande är att det delvis är trillingens sätt att samarbeta som legat till grund för arbetsmodellen.

Bromma stadsdelsförvaltning och Trillingen, har fortsätt utmaningar där de från central verksamhet inte finns kunskap om att normerande klassningar behöver göras innan upphandling eller driftsättning. Här är det viktigt att förvaltningens avdelningschefer och andra nyckelpersoner vidarebefordrar information om nya objekt eller utveckling av befintliga objekt till förvaltningens ISAM. Att få fram kvalitativa normerande klassningar sparar tid när det kommer till det lokala arbetet.

Antalet it-tjänster fortsätter öka i Stockholms stad och så även i Bromma stadsdelsförvaltning. It-tjänsterna blir ofta mer integrerade och flöden i och mellan system kräver informationsskydd under hela livscykeln. System är oftare molntjänster och levereras oftare som en tjänst av en extern leverantör.

Det är viktigt att så långt som möjligt minimerar möjligheter till manuella fel, det vill säga. den mänskliga faktorn. Det är också viktigt att ställa höga krav på upphandlingar och upphandlingskrav både gällande it-design och it-arkitektkrav, fysisk teknik och även

medarbetares kunskap och fortbildning. Stor vikt bör läggas på de avtal som gäller hantering av personuppgifterna, som tecknas mellan Bromma stadsdelsförvaltning och leverantörerna för att säkerställa leverantörens och underleverantörernas hantering i alla led.

Utmaningar och förseningar med olika leveranser till verksamheter gör att alternativa rutiner eller arbetssätt används, men även i dessa fall måste regelverken och rutiner uppfyllas. Ett exempel på detta är när verksamheterna inte får tillgång till arbetsverktyg eller it-tjänster som leder till att verksamheten skapar egna manuella rutiner, vilka kan brista i säkerhet.

En tydligare skiljelinje mellan lokala system och molnbaserade system blir tydligare. Lagar som GDPR, AI-förordningen och NIS2 påverkar olika leverantörer som erbjuder alternativ till molntjänster. Dessa har inte alltid de bästa verksamhets- och säkerhetslösningarna.

3.1 Påverkan på Bromma stadsdelsförvaltning

Kontinuerligt fler system och mer avancerade integrerade system kräver mer tid för informationssäkerhet. Det gäller dels den rutinmässiga hanteringen av formalia som klassningsprotokoll och uppföljning, men också kompetenskrav på de som utför arbetet. Det behövs både mer tid då det blir fler system. Det behövs tid att lära sig och utreda all teknik, lagar och riktlinjer som ändras.

Som en spegling av budgeten och omvärldsutvecklingen har Bromma stadsdelsförvaltning påbörjat rekrytering av en ISAM/ arkivarie under 2026. Tidigare har tjänsten delats på it-ansvarig/ISAM. En bättre lösning då ISAM ska kunna granska it.

Det kräver att det är flera som delar på arbetsbördan och säkerställer ett det finns viss redundans och överkapacitet på de discipliner som krävs för att göra klassningar grundligt och korrekt. Området har växt så mycket på senare år att det är svårt för enstaka medarbetare eller på ett fåtal ha den kompetens om alla specialområden som myndighetsutövningen kräver. Tiden då vi kan luta oss mot personberoenden är förbi och informationssäkerhet är en del av alla arbetsuppgifter dygnet och året om.

Med en spridd kunskap i verksamheten och en syn på informationssäkerhet som en del av ordinarie arbetsuppgifter blir det inte heller betungande eller en pålaga, det blir lätt att göra rätt.

4 Topp 5 risker inom informationssäkerhet

Risk	Beskrivning	Bedömning	Förslag åtgärder
Allmänna handlingar riskerar inte att kunna lämnas ut.	Säkra meddelanden används felaktigt/ slentrian.	HÖG	Utbilda och stickprov
	Nordic 4 Zoom dokumentdelning	HÖG	Stänga av funktion
AI används på eget bevåg, skapar eget konto.	Inga tekniska spärrar finns att starta konton. Tjänstemannautövning med AI.	HÖG	Inbyggd standard för integritetsinställningar
Tjänstetelefoner används privat	Bristande respekt och förståelse för hur man ska använda sin utrustning.	HÖG	Tekniska spärrar för at ladda ner appar.
Tjänstetelefoner används av obehöriga (närstående ex barn, sambo)	Brist i ansvarskänsla i och med att man låter obehöriga använda utrustningen och kommer åt information. (Lagbrott)	HÖG	Utbildning och uppföljning.

Personer med sekretessmarkering skyddas inte tillräckligt.	Staden saknar gemensam hantering för hur man arbetar med skyddad id. Både för medborgare och personal.	HÖG	Efter att staden tagit fram riktlinje och process, bryta ner i lokala rutiner.

5 Uppföljning av tidigare beslut

5.1 Uppdaterad lokal tillämpningsanvisning för informationssäkerhet

Beslut om informationssäkerhetsarbete har tagits av förvaltningen genom att de lokala tillämpningsanvisningarna uppdaterats och därefter fastställdes av direktör 2024-12-18. I den beskrivs förvaltningsspecifik organisation, årshjul och rutiner för verksamheten som rör informationssäkerhetsarbetet.

5.2 Uppföljning av roller i de lokala tillämpningsanvisningarna

Tabellförklaring

Grönt	Gult	Rött
Inga anmärkningar eller brister behöver åtgärdas omgående	Brister och anmärkningar behöver åtgärdas med handlingsplan.	Omgående åtgärder behöver tas fram och implementeras.

Funktion i organisation	Roll enligt anvisning	Status 2024	Status 2025
Ledning	Utse nödvändiga roller inom organisationen	-Kvarstår att genomföra samtliga klassningar och	-Kvarstår

	samt anta de lokala tillämpningsanvisningarna. Tillse att resurser finns och medarbetare har den utbildning och information som krävs för uppdraget.	genomföra årliga uppdateringar för de befintliga som ännu ej är genomförda. -Kvarstår att förankra i samtliga verksamhetsområden den.	-Kvarstår
Chefer	Utreda incidenter, säkerställa registervård, göra inköp i enlighet med gällande lagar och styrdokument, klassa viktiga tillgångar, ta fram lokala rutiner för den egna verksamheten utifrån behov	-Kunskaps-luckorna kvarstår -Brister finns i registervården, behöver förbättras.	-Kvarstår -Kvarstår
		-Lokala rutiner och förankring i verksamheten släpar efter.	-Lokala verksamhetsrutiner framtagna. Implementeras 2026.
Processägare	Äger processer inom verksamhetsområde inom klassificerings-struktur. Fattar beslut när osäkerhet uppstår vid hantering av information.	-Olika verksamheter har olika benämningar och alla har inte uttalade processägare -Hanterings-anvisningens processer är inte implementerat vilket gör att det blir svårt att se vem som äger informationsflöden.	-Kvarstår -Kvarstår
Objektägare	Ansvarar för informationstillgången (objekt) och utser objektledare.	Är utsedda	Kontrollerade och uppdaterade
Objektledare	Ansvarar för informationssäkerhet i objekt genom att se till att dokumentation finns på plats och	Är utsedda	Kontrollerade och uppdaterade

	att rutiner finns och följs.		
ISAM	Att vara kontaktpunkt, rådgöra, samverka och stödja, omvärldsbevaka och följa upp.	Bedömt av Stadsdelsdirektören- Ingen förändring	Ingen förändring
DSO	Vägleda, informera, självständigt bevaka de registrerades intressen.	Bedömt av Stadsdelsdirektören- Ingen förändring	Ingen förändring
ILS-samordnare	Stödjande inom sina respektive områden.	Ny ILS-samordnare	Informationssäkerhet implementerat i ILS.
Arkivansvarig och arkivarie	Stödjande inom sina respektive områden.	Ingen förändring	Ingen förändring
Stadsdelsarkivarie	Stödjande inom sina respektive områden.	Ingen förändring	Ingen förändring
Dataskydds- och informationssäkerhetsambasadörer	Fungera som mellanhand för informations-spridning och -inhämtning i verksamheten. Sammanhållande och stöttande.	Ska utses nya till nätverket.	Nätverket med ambassadörer startar och arbetar enligt årshjul.

5.3 Uppföljning av årshjul

Aktivitet	Resultat 2023	Resultat 2024	Resultat 2025
Tertial 1			
Ambassadörsnätverk	Under tertial 1 2023 har nätverket med så kallade ambassadörer ersatts av objektägare	Har nu ersatts av PM3 rollerna	Nätverket beslutas att starta och detta sker i T1.

	och objektledare enligt PM3-modellen		
Årsrapport Ledningens genomgång	Årsrapport inlämnad till Bromma stadsdelsnämnd 2022	Årsrapport inlämnad till Bromma stadsdelsnämnd 2024	Årsrapport inlämnad till Bromma stadsdelsnämnd 2025
Klassning av förvaltningens mest skyddsvärda information	Arbetet påbörjat enligt PM3-modellen	Objektledare är utbildade	Pågående efter prioritet och följer normerande klassningar i staden.
Årlig klassning, som en del av det systematiska informationssäkerhetsarbetet, av förvaltningens mest skyddsvärda information	Startar 2024	Delvis genomförda, behöver skötas systematiskt över flera år.	Delvis genomförda, behöver skötas systematiskt över flera år.
Uppdatering av årshjul gällande informationssäkerhet	Årshjulet uppdaterat	Årshjulet är uppdaterat	Årshjulet är uppdaterat
Dataskyddsombudet anordnar utbildningstillfälle för stadsdelsnämnden	Genomfört vid dragning av Dataskyddsombudets årsrapport	Nämnden är utbildad och utbildas årligen.	Nämnden är utbildad och utbildas årligen.
Dataskyddsombudets årsrapport lämnas till nämnden	Genomfört januari 2023 för år 2022	Genomfört januari 2024 för år 2023	Genomfört januari 2025 för år 2024
Objektledarna ska genomföra kontroller av behörigheter	Arbetet påbörjat 2023 och pågår under 2024	Enligt Internkontroll-planen	Enligt Internkontroll-planen
Uppdatera rutin för NIS-incidenter	Genomfört genom Medicinskt ansvarig sjuksköterska (MAS) Behöver ses över efter NIS2	Uppdaterad av MAS	Uppdaterad av MAS

	utredningen är klar i februari 2024		
Tertial 2			
Uppdatera registerförteckning personuppgiftsbehandlingar	Uppdatering genomförd	Uppdatering delvis genomförd, släpar efter med kunskapslucko r för objektägare.	Delvis genomfört av ambassadörerna. Inväntar ny plattform för DraftIT 2026.
Ta fram/ uppdatera verksamhetens rutiner för informationssäkerhet /GDPR	Rutin framtagen för utlämnande av allmän handling, gallring av arkivhandlingar, behörighetsrutiner, rutin för e-post och posthantering, och rutin för rent skrivbord, ren skärm, förvaring av dokument samt rutin för utskrifter, rutin för diarieföring och hantering av allmänna handlingar	Hanteringsanvisningar och kontroller släpar efter, bristande tid för kontroller, fokus är på att ta fram klassningsunderlagen.	Arbete kommer att vara klart årsskiftet 2025/26 och implementeras 2026.
Kontrollera och uppdatera informationstillgångarna i ISAM:s förteckning	Pågår löpande	Pågår löpande	Pågår löpande
Granska PUB-avtal/leverantör (DSO och Arkivarie)	Redovisas i Dataskyddsombudets årsrapport	Redovisas i Dataskyddsombudets årsrapport	Redovisas i Dataskyddsombudets årsrapport
Tertial 3			
Granska och uppdatera styrande	Genomfört	Genomfört löpande	Genomfört löpande

dokument gällande: -Incidenthantering -hantering av personuppgifter -lokala tillämpningsanvisningen -information på Intranätet -upphandling			
Kontrollera och uppdatera informationsklassningarna	Genomfört löpande	Genomfört löpande	Genomfört löpande
Följa upp informationssäkerhetsincidenter som skett under året	Görs kontinuerligt under året	Görs kontinuerligt under året	Genomfört löpande i Trillingsam-arbetet.
Se över dataskydds- och informations-säkerhetsorganisationen	Genomförs av förvaltningsledningen	Genomförs av förvaltningsledningen	Genomförs av förvaltningsledningen
Uppföljning genomförda utbildningar för medarbetare och chefer. (ISAM tar ut rapport)	Genomfört	Genomförs i verksamheten, kontrollerat manuellt och muntligt, men IT-tjänstens har brister i rapportverktygen för genomfördstatus.	Genomförs i verksamheten, kontrollerat manuellt och muntligt, men IT-tjänstens har brister i rapportverktygen för genomfördstatus.
Verksamhets-berättelse	Genomfört	Genomfört	Genomfört

ISAM Rapport Ledningens genomgång			
GDPR Årsrapport framtagning (DSO)	Pågår	Pågår	Pågår

5.4 Uppföljning av mål i verksamhetsplanen (VP) 2025

VP Mål	**Resultat**
Förvaltningens nyckelpersoner ska utbildas i de lokala tillämpningsanvisningarna för informationssäkerhet	Genomförs löpande under året vid nyanställning av nyckelpersoner
Samtliga IT-tjänster som förvaltningen använder ska vara klassade	Majoriteten av IT-tjänsterna i förvaltningen är klassade
Samtliga verksamheter ska skriva lokala rutiner utifrån Brommas lokala tillämpningsanvisningar för informationssäkerhet	Uppföljning sker i samband med verksamhetsberättelsen 2025

5.5 Uppföljning av tidigare förslag från ISAM

Rekommendation	**Resultat**
Implementera PM3 i hel verksamheten	Delvis genomfört.
Uppdatera tillämpningsanvisning gällande rutiner för NIS2 och de senaste lagkraven inom till exempel AI och policys från staden.	Delvis genomfört. Ej antagen när rapporten skrivs.
Säkerställa att kontinuitetshantering säkerställs och övas.	En föreläsning av extern expert genomfördes för Trillingen 2025. Kontinuitetsplaner fortsätter kontinuerligt att uppdateras löpande.
De IT-tjänster som är inventerade ska ha genomförd klassning alternativt	Delvis genomfört.

genomför årlig klassning och riskanalys.	
Vid nyrekrytering av medarbetare till vissa nyckelroller och chefspositioner, utarbeta förslag på hur man kan premiera eller säkerställa att frågor som rör datakunskap tas omhand Förbereda kompetenshöjande och kompletterande utbildningar för nyrekryterade.	Genomfört
Förslag på fler uppföljningstillfällen som följer VP-arbetet i övriga förvaltningen. -Informationssäkerhetsarbetet stäms av i formella processer årligen. Arbetet med detta behöver delas upp och bättre hanteras löpande under ett verksamhetsår. Att göra bra analyser samtidigt som arbetet med verksamhetsberättelsen pågår i slutet av året, är en utmaning. Den bör följa stadens övriga tertialarbete.	Genomfört med muntlig rapport i FvL tre gånger.
Stärka och förbättra rutinerna gällande informationssäkerhet vid upphandlingar och inköp. -Redan vid inköp och i referensgrupper för upphandlingar bör dataskydd beaktas. Kan i värsta fall ur ekonomisk synvinkel leda till att man inte kan använda nya IT-tjänster. De blir betydligt dyrare efter extra skyddsåtgärder, eller så införs system utifrån riskfaktorer som inte är tillräckligt säkra.	Inte genomfört. Kvarstår

5.6 Resultatet från revisioner

Under 2025 har inga externa eller centrala informationssäkerhets revisioner genomförts i Bromma stadsdelsförvaltning. Interna revisioner sker löpande enligt internkontrollplanen.

5.7 Risker som identifierats i Dataskyddsombudets årsrapport 2024

Bedömning	Risk
HÖG	Osäker e-posthantering med personuppgifter (Kvarstår från 2023)
HÖG	Brister inom dokumentationen i informationssäkerhets- och GDPR-frågor (Kvarstår från 2023)
HÖG	Tredjelandsöverföringar (Kvarstår från 2023)
MEDEL	Skyddade personuppgifter inom förskolan (Kvarstår från 2023)
MEDEL	Central objektförvaltning har inte tillräckligt med resurs och kan inte svara mot lokal (Stadsdelsförvaltningens) objektförvaltning (Ny)
HÖG	Ny teknik, t.ex. behandling av personuppgifter och annan information behandlas med AI utan korrekt analys och dokumentation (Ny)

5.7.1 DSO ger råd och rekommendationer till Stadsdelsnämnden

1. Dataskyddsombudets rekommendation för att minimera risken att personuppgifter e-postas utan tillräckligt skydd, är att de risker som kommit fram under projektet att införa tjänsten ”Säkra meddelanden” åtgärdas.

2. Genom att ta fram, implementera och kommunicera tillämpningsanvisningarna för informationssäkerhet och dataskydd kommer ansvaret bli tydligare för vem som ska ta fram dokumentationen som i dag saknas.

3. Nämnden rekommenderas att ta höjd för risken och bestämma aptiten för vad man är villig att riskera när man ingår nya avtal med leverantörer där överföringar till tredjeland sker. Rådet är också att ha en tydlig exitplan och genomlysa marknaden i förstahand inom Sverige och

EU/EES. Rutiner för att genomföra TIA, Transfer Impact Assessment, behöver också tas fram.

4. Vid införandet av nya tjänsterna inom förskolan behöver perspektivet skyddade personuppgifter omhändertas särskilt.

5. Att ge råd om hur den centrala organisationen ska få mer resurs att utföra sitt arbete är svårt. Men, vi kan belysa utifrån Stadsförvaltningens perspektiv att det blir svårt att arbeta effektivt när den brister och det tenderar att byggas flaskhalsar.

6. Som DSO rekommenderar jag att ni fortsätter vara nyfikna på ny teknik och våga satsa på den. Men, rekommendationen är att göra det med stor medvetenhet och arbeta efter den metod som finns framtagen för informationsklassning, riskanalys och konsekvensbedömning. Genvägar blir kostsamma både utifrån sanktioner (både GDPR och AI-förordningen kan ge sanktioner var för sig) men också individens rättigheter får aldrig förminskas eller glömmas bort.

6 Förbättringar för verksamhetens LIS

Förslagen till förbättringar avser perioden 2026-2028 utifrån dagens omvärldsläge och styrkor/svagheter i nämndens arbete. Då ledningens genomgång sker årsvis som en del av det systematiska arbetet, kommer anpassningar och nya krav att hanteras och föreslås. Detta som en naturlig del av arbetet kommande år.

Denna rapport utvärderar innevarande och föregående års aktiviteter. Eventuella förbättringsförslag eller bristeranalyseras och förslag läggs fram vid nästa rapport som kommer 2026.

6.1 Förbättringsaktiviteter under 2026

- Befästa och förbättra arbetet med PM3 i förvaltningen.

- Stärka och förbättra rutinerna gällande informationssäkerhet vid upphandlingar och inköp.

  - Redan vid inköp och i referensgrupper för upphandlingar bör dataskydd beaktas. Kan i värsta fall ur ekonomisk synvinkel leda till att man inte kan använda nya IT-tjänster. De blir betydligt dyrare efter extra skyddsåtgärder, eller så införs system utifrån riskfaktorer som inte är tillräckligt säkra.

- Utarbeta förslag och rutiner på hur man bör säkerställa kunskapsöverföring vid omorganisationer eller vid personalförändringar.

  - Att jobba på ett bra sätt med informationssäkerhet tar tid att lära sig. Man måste tillägna sig kunskaper som man oftast inte har fått via skolans utbildningar eller via den kärnverksamhet där man är verksam. Man behöver öva dessa i praktiskt arbete och sätta sig in i rutiner och processer. Det är idag en utmaning när medarbetare slutar/börjar. Det tar lång tid att lära upp, men den största förlusten är verksamhetskännedomen, medarbetare som slutar har unik kunskap om sin verksamhet som riskerar att gå förlorad.

- Intern förankring av beslut och rekommendationer att säkerställa information i linjeorganisationen.

  - Det finns idag olika kunskap hos chefer, både inom och mellan våra förvaltningsområden. Vanligaste förklaringen till att man inte har hört om det kan vara att man inte förstått, men slutresultatet är ofta det samma. Det är brister i rutiner och processer.

- Förslag på kontroll och genomförandet av obligatoriska utbildningar. Kurser bör genomföras enskilt, kunskapstestet slår inte väl ut när det

genomförs i grupp. Statistik och uppföljning, vilka som gått obligatoriska kurser är svart att följa upp.

- En bättre uppföljning av vilka kurser, deras innehåll och hur de genomförs skulle förbättra förankringen hos den enskilda medarbetaren. Uppföljning försvåras om kurser som är tänkta att vara individuell genomförs i grupp. De som saknar viss kunskap får inte den chans de behöver för att tillägna sig den.

6.2 Förbättringsaktiviteter under 2027

- Informationssäkerhetsklassa informationstillgångar.
- Inventering av personuppgiftsbehandlingar.
- Revidera lokala tillämpningsanvisningarna.
- Genomföra övning inom verksamheter, till exempel nätverksbortfall eller dataförlust.
- Förbättra PM3-modellen.
- Genomföra övning för ledningsgrupp till exempel antagonistisk cyberattack.
- Utveckla rutiner där säkerhetssamordnare och ISAM kartlägger risker kopplat till dataskydd, där informationssäkerhet är en delmängd. En helhetssyn tas fram för informationssäkerhetsarbete med berörda samordnare som gör gemensam risk- och sårbarhetsanalyser.
- Tydligare mandat och en budgetstyrning kopplad mot dataskydd bör tas fram. Medel måste reserveras utöver det som rör inköp och upphandling. Det arbete som måste läggas ner på kontroller och skapande av formalia, är i många

6.3 Förbättringsaktiviteter under 2028

- Informationssäkerhetsklassa informationstillgångar.
- Inventering av personuppgiftsbehandlingar.
- Revidera lokala tillämpningsanvisningarna.
- Genomföra övning inom verksamheter.

- Genomföra övning för ledningsgrupp.
- Förbättra PM3-modellen.

7 Länkarkiv

Ledningssystem för informationssäkerhet (LIS) (msb.se)

Dataskydd för verksamheter | IMY

NIS 2 | SKR

IoT – så funkar det - IoT Sverige

Sverige ska bli ledande inom artificiell intelligens | Digg

Hotaktörer (msb.se)

KLASSA, informationsklassning | SKR