Ledningens genomgång år 2025

Järva stadsdelsförvaltning

Beslutad [datum]
Reviderad 2025-11-24

Ledningens genomgång

Dnr: JÄRVA 2025/1249

Kontaktperson: Julia Jonsson

Sammanfattning

Ledningens genomgång ska ge information och underlag till stadsdelsdirektören att årligen bedöma om det lokala informationssäkerhetsarbetet och dataskyddsarbetet är tillräckligt och har önskad verkan.

Genomgången kommer att beskriva kort den nya cybersäkerhetslagen kopplad till NIS 2-direktivet som kommer börja gälla i januari 2026. Lagstiftningen syftar till att stärka cybersäkerheten för samhällsvikta tjänster.

Under året har leverantören Miljödata AB blivit utsatt för en ransomware-attack. Angreppet resulterade i att anställdas personuppgifter så som personnummer och hemadress publicerades öppet på darknet. Samtliga månadsanställda samt tidigare anställda under perioden 1 januari 2024 till augusti 2025 omfattas av personuppgiftsincidenten. Även vissa personer med skyddade personuppgifter röjdes.

Genomgången presenterar statistik gällande incidenter som visar på att en stor andel incidenterna handlar om information som omfattas av sekretess och personuppgifter som har röjts. Statistiken visar även på att det är en låg andel medarbetare, chefer och förtroendevalda som har genomfört de obligatoriska e-utbildningarna i informationssäkerhet och dataskydd.

Följande förbättringsförslag rekommenderas till ledningen att vidta:

- Utbildningsunderlag riktade till medarbetare som inte har tillgång till datorer i sitt dagliga arbete.
- Informationssäkerhet inom upphandlingsförfarandet (kvarstår)
- Stärka chefers kunskap inom området informationssäkerhet (kvarstår)
- Involvera ledningsgruppen mer i informationssäkerhetsarbetet (kvarstår)
- Obligatoriska e-utbildningarna ska genomföras i högre grad (kvarstår)

Även en treårsplan redovisas för åren 2026-2028 i ledningens genomgång.

Innehållsförteckning

1. Vad är Ledningens genomgång

Ledningens genomgång är en helhetsbild för den nuvarande situationen för informationssäkerhetsarbetet på Järva stadsdelsförvaltning och syftar till att informera ledningsgruppen om det arbetet som har gjorts, vilka risker som finns och åtgärder som kvarstår från det gångna året. 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 informationssäkerhetsarbetet som beskrivs. 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.

1.2 Faktorer som påverkar verksamhetens LIS

Under det här avsnittet beskrivs områden som påverkar Järva stadsdelsförvaltnings ledningssystem för informationssäkerhet (LIS). Det som beskrivs är bland annat ny lagstiftning, internkontroll, statistik över incidenter och genomförandegraden av de obligatoriska e-utbildningarna för dataskydd och informationssäkerhet, kontinuitetsplanering och en redogörelse över incidenten hos en av stadens leverantörer.

1.2.1 Omvärldsbevakning – hot, trender och ny lagstiftning

1.2.1.1 Cybersäkerhetslagen (NIS 2)

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”[1]

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

[1] https://regeringen.se/rattsliga-dokument/proposition/2025/10/prop.-20252628, hämtad 2025-11-13

och informationssystem för samhällsviktiga tjänster. NIS 1-direktivet omfattar flera sektorer. Den sektorn som träffar Järva 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

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

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

1.2.2.1 Ny chefsstruktur

Från den 1 januari i år så har en ny chefstruktur börjat gälla för Järva stadsdelsförvaltning.

Detta har lett till att det har blivit fler chefer och även att personer som inte har varit chef innan har påbörjat sitt första chefsuppdrag. Detta innebär att det är fler personer som behöver få utbildning om stadens och förvaltningens ledningssystem för systematiskt

informationssäkerhetsarbete och vad som förväntas av dem i deras chefsroll.

1.2.3 Vad har verksamheten identifierat i RSA-arbetet

Stadens RSA-process, som fokuserar på hur samhällsviktig verksamhet påverkas av extraordinära händelser i fredstid och höjd beredskap, genomförs i tvåårscykler. RSA-processen ska säkerställa att samhällsviktig verksamhet alltid kan fortgå genom olika typer av kontinuitetshanteringsåtgärder.

2025 är år två för den pågående cykeln. Under året har avdelningsövergripande kontinuitetsplaner tagits fram för de verksamheter som har bedömts som samhällsviktiga. I kontinuitetsplanerna anges för kritiska system krav på återhämtningstid samt reservrutin och återgångsrutin.

1.2.4 Resultatet från egen uppföljning (VoR och IKP)

1.2.4.1 Riskbeskrivning: Obehöriga får tillgång till information (behörighetshantering)

Föreslagen åtgärd: För system utse roller och fördela ansvar i enlighet med pm3-modellen.

Resultat: Åtgärden genomförs inom pilotprojektet för pm3 och roller har fördelats för system inom objektprodukterna för stöd för administration och stöd för lokal och internservice. Pilotprojektet är genomfört och implementeringsprojekt för pm3 kommer ta vid.

1.2.4.2 Riskbeskrivning: Tillämpningsanvisning efterlevs inte och informationssäkerhetsarbetet sker inte systematiskt (implementering av lokal anvisning)

Föreslagen åtgärd: Implementera förvaltningsövergripande kontroller för uppföljning av lokal tillämpningsanvisning

Resultat: Åtgärden är under genomförande. En rutin för förvaltningsövergripande kontroller för uppföljning av den lokala tillämpningsanvisningen är under framtagande.

1.2.4.3 Riskbeskrivning: Information är inte tillgänglig, försvinner eller kommer obehöriga tillhanda (incidenthantering)

Föreslagen åtgärd: Informationsinsats till samtliga verksamheter via avdelningarnas ledningsgrupper

Resultat: Åtgärden har ännu inte påbörjats på grund av att den är beroende av en aktivitet som har försenats. Åtgärden kommer

sannolikt inte vara klar till utsatt datum men kommer genomföras under året.

1.2.4.4 Riskbeskrivning: Förvaltningens information är inte tillräcklig skyddad (informationsklassning)

Föreslagen åtgärd: Processkartläggning genomförs och lokal rutin för informationsklassning upprättas och implementeras

Resultat: Åtgärden har ännu inte genomförts.

1.2.4.5 Riskbeskrivning: Efterlever inte dataskyddsförordningen (registerhantering av personuppgifter)

Föreslagen åtgärd: Inventering av personuppgiftsregistret

Resultat: Åtgärden är under genomförande. Personuppgiftsregistret är infört i DraftIt och implementering av ett nytt arbetssätt är genomfört där verksamheterna själva kontrollerar sina uppgifter i systemet. Alla verksamheter har genomfört den årliga inventeringen av personuppgiftsregistret.

1.2.4.6 Informationssäkerhet inom upphandlingsförfarandet

Ingen risk har formulerats inom detta område i förvaltningens väsentlighet- och riskanalys (VoR), därför finns det ingen information att redovisa om hur förvaltningen har arbetat med risker inom området.

Risker i upphandlings- och inköpsförfarandet har tidigare tagits upp i ledningens genomgång för 2024, där bland annat förbättringsförslaget som då föreslogs var ”Tydliggör i inköps- och upphandlingsprocesserna att informationssäkerhets- och dataskyddsfrågor alltid måste beaktas när IT-tjänster ska anskaffas eller när känslig information ska delas med leverantören.”

I styrdokumenten och mallar för inköp och upphandling har det under 2025 gjorts uppdateringar där det framgår att informationssäkerheten ska beaktas, men inte tillräcklig information om hur det ska beaktas. Informationen är publicerad på intranätet. Det är oklart hur eller om rutinerna har implementerats. Informationssäkerhetssamordnaren har inte varit involverad i implementeringen.

1.2.5 Resultatet från egen övrig uppföljning

Nedan presenteras statistik för att ge en indikation över hur förvaltningens informationssäkerhetsarbete ser ut.

1.2.5.1 Statistik över de obligatoriska e-utbildningarna

Nedan redovisas antal medarbetare som har genomfört e-utbildningar inom informationssäkerhet och dataskydd. Grundutbildningarna är obligatoriska för alla medarbetare och chefer att genomföra (certifieras). Utbildningarna ska även förnyas årligen annars utgår certifieringen.

Nedan statistik för grundutbildning i dataskydd samt informationssäkerhet för medarbetare inom staden är hämtad från stadens utbildningsplattform. Statistiken hämtades den 2025-11-15.

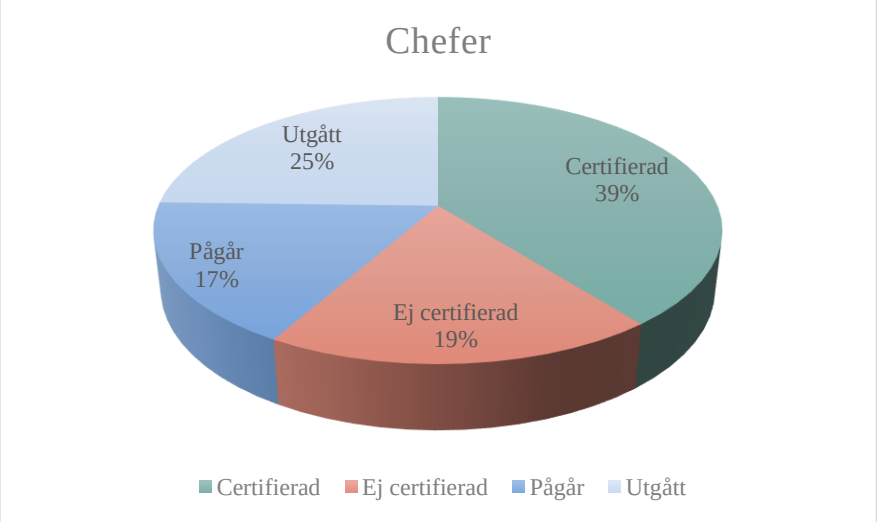
Statistiken för chefer baseras på 122 chefer.

Resultatet för förtroendevalda är baserad på 22 ledamöter. Nämnden består av 26 ledamöter, men 4 av ledamöterna är inte grupperad inom Järva stadsdelsförvaltning i utbildningsplattformen, vilken kan bero på att de till exempel är anställda i andra förvaltningar eller bolag.

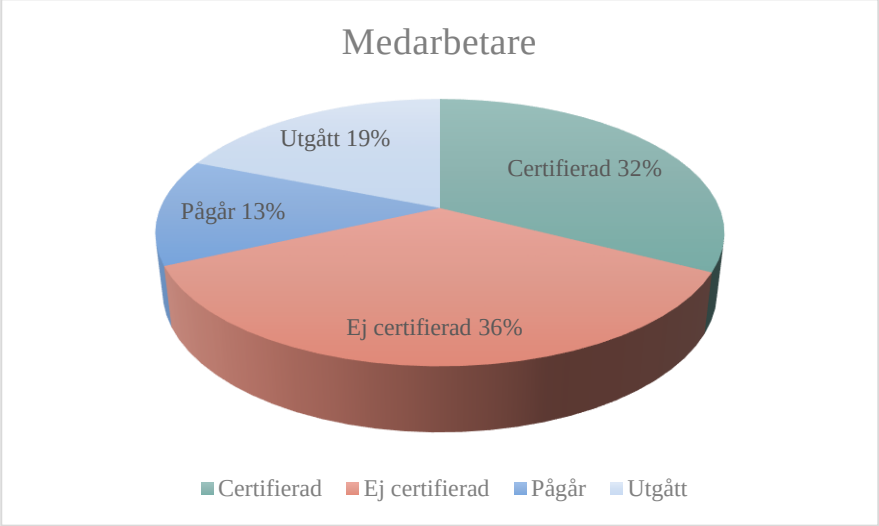
För medarbetare så baseras resultatet på 2 428 medarbetare.

Informationssäkerhet för medarbetare inom staden

39 procent av cheferna är certifierade och har alltså genomfört utbildningen, och 17 procent har påbörjat men inte slutfört utbildningen. Medan 19 procent av cheferna har inte genomfört utbildningen, och 25 procent har inte förnyat sitt certifikat.

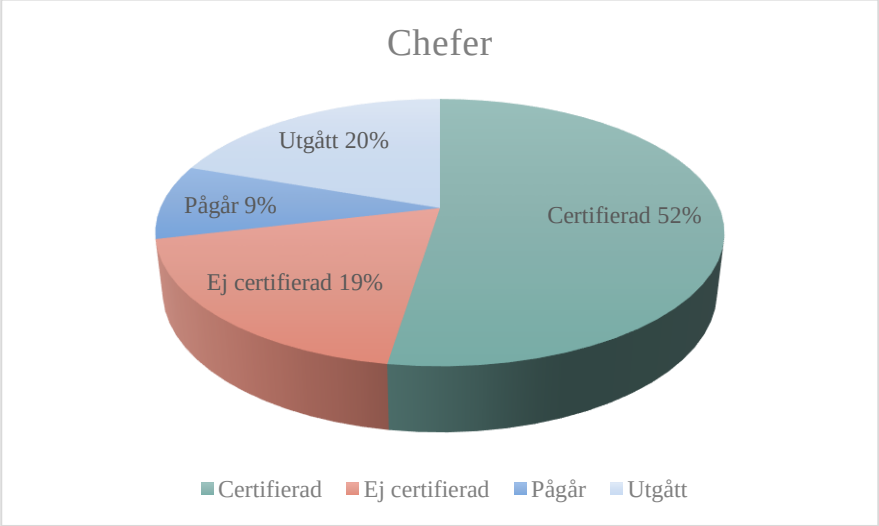


Av medarbetarna så har 32 procent genomfört utbildningarna, och 13 procent har påbörjat dem. 36 procent har inte genomfört utbildningarna och 19 procent av medarbetarna har inte förnyat sitt certifikat.

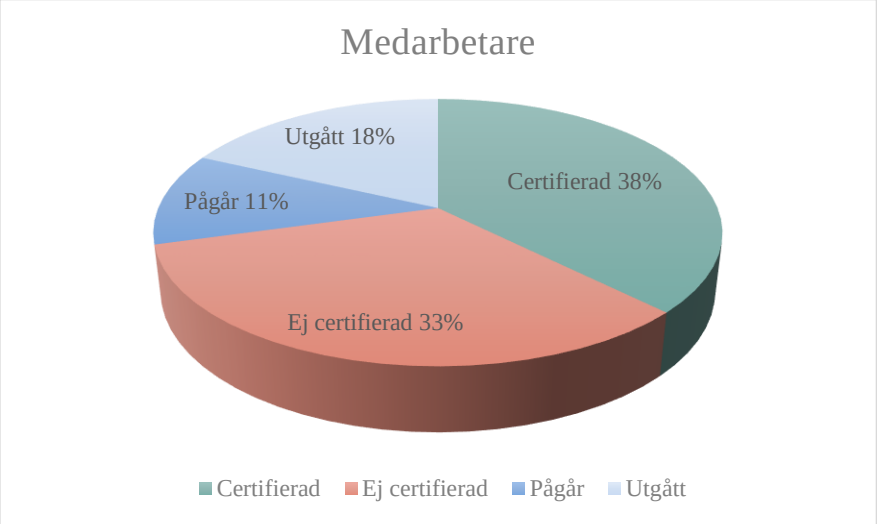


Grundutbildning i dataskydd

Av cheferna har 52 procent genomfört utbildningen och 9 procent har påbörjat utbildningen men inte slutfört. 19 procent har inte genomfört utbildningen och av cheferna har 20 procent inte förnyat sitt certifikat.



Av medarbetarna är 38 procent certifierade och har genomfört utbildningen för dataskydd, och 11 procent har påbörjat utbildningen. 33 procent av dem har inte genomfört utbildningen och 18 procent har inte förnyat sitt certifikat.



1.2.5.2 Incidentrapportering och -hantering

I staden finns flera sätt att rapportera incidenter och avvikelser på till exempel:

- Incidentrapporteringsverktyget IA
- Tietoevry servicedesk 11800 och Fujitsu service desk 33900
- Klagomål
- lex Sarah och lex Maria

Det förekommer informationssäkerhets- och personuppgiftsincidenter inom alla sätten att rapportera incidenter och avvikelser på. Enligt rutinen för incidenthantering av den här typen av incidenter, så ska de rapporteras i incidentverktyget IA. I IA rapporteras även andra incidenter inom arbetsmiljö och verksamheten i stort.

Sammanställning av klagomål

Ett av områdena som följs upp är antal klagomål som inkommer till förvaltningen. Under de år som Järva stadsdelsförvaltning har funnits så har det var få klagomål som har registrerats.

Till Järva stadsdelsförvaltning har det hittills registrerats tre klagomål gällande hantering av personuppgifter i år.

Sammanställning från incidenthanteringsverktyget IA och lex Sarah

Totalt har 46 informationssäkerhet- och personuppgiftsincidenter rapporterats i år, varav 5 av dem har rapporterats via rutinen för lex Sarah.[2]

- Antal incidenter där det har stulits information/personuppgifter (t.ex. dator): 5
- Antal incidenter gällande felregistreringar: 3
- Antal incidenter som rör brist på information/avsaknad av information (tillgänglighet): 8
- Antal incidenter gällande obehörig som har tagit sig in i stadsdelsförvaltningens lokaler: 1
- Antal incidenter där känsliga personuppgifter och sekretess har röjts: 22
- Antal övriga incidenter: 7

Sammanställning av förlustanmälningar till servicedesk

Under 2025 har det rapporterats 26 förlustanmälan om mobila enheter. Det är inte alla mobila enheter som förlustanmäls så det finns ett mörkertal.

1.2.6 Resultatet från revisioner

Revisionskontorets genomför en granskning av hur nämnderna i staden följer upp sina avtal då det i tidigare granskningar av avtalsuppföljning visar genomgående på ett stort utvecklingsbehov i staden.

Avtalsuppföljning en är viktig del inom det systematiska informationssäkerhetsarbetet, där krav om informationssäkerhet och dataskyddsfrågor också behöver följas upp regelbundet med leverantör och personuppgiftsbiträden.

Resultatet från granskningen är inte fastställd ännu, men det är positivt att den här granskningen genomförs, då det saknas tydliga rutiner för registrering av avtal men även för hur avtal följs upp. Informationssäkerhetssamordnaren kommer att följa upp om informationssäkerhetsområdet kommer att tas med i rutinerna och sedan hur implementeringen kommer att gå till för att sprida de nya arbetssätten.

[2] Lex Sarah-rapporter som även har anmälts i IA har räknats med bland incidenterna i IA.

1.2.7 Risker som identifierats i GDPR-årsrapport

Nedan risker är hämtade från dataskyddsombudets (DSO) årsrapport för verksamhetsåret 2024[3]. Arbetet med riskerna redovisas under respektive risk.

1.2.7.1 Osäker e-posthantering med personuppgifter (Kvarstår)

Risken handlar om att den e-posthantering som är idag, alltså att e-postmeddelanden ligger kvar okrypterade i varje medarbetares inkorg, och att det idag saknas rutiner för att säkert kunna dela information digitalt med medborgare.

Under 2025 har förvaltningen arbetat vidare för att minska risken med osäker e-posthantering genom att undersöka om de kvarstående höga riskerna med den upphandlade it-tjänsten för krypterad e-posthantering har åtgärdats. Förvaltningsledningen har fattat beslut om ett stegvis projektinförande för att i det arbetet undersöka vilka arbetssätt som är säkra med tjänsten och vilka administrativa skyddsåtgärder som krävs av verksamheten som ska nyttja tjänsten. Projektets arbete har påbörjats i år och kommer fortsätta under 2026.

1.2.7.2 Brister inom dokumentationen i informationssäkerhets- och GDPR-frågor (Kvarstår)

Staden har en handbok för informationssäkerhetsklassning som en del i ledningssystemet för informationssäkerhet (LIS). Handboken beskriver hur en klassning[4] ska gå till och vilket underlag som kan ingå. Mognaden inom området är generellt lågt i stadsdelsförvaltningen och även i staden, vilket även påverkar de underlag som tas fram eller inte tas fram när it-tjänster köps in eller otydligt personuppgiftsförhållanden i upphandlingar.

Under 2025 har förvaltningen påbörjat arbetet med införandet av förvaltningsmodellen pm3 som är tillför att tydliggöra ansvarsfördelningen för de it-tjänster som förvaltningen använder och den informationen som hanteras i dem. När en it-tjänst köps in ska den även förvaltas av verksamheten som ansvarar för informationen i tjänsten. En del av förvaltningen är att

---

[3] Dataskyddsombudets årsrapport 2024, https://meetingspublic.stockholm.se/welcome-sv/namnder-styrelser/jarva-stadsdelsnamnd/mote-2025-02-20/agenda/bilaga-11-gdpr-arsrapport-2024-jarva-stadsdelsforvaltningpdf?downloadMode=open hämtad 2025-11-11.

[4] Läs mer om vad en informationssäkerhetsklassning är här: https://metodstod-informationssakerhet.msb.se/sv/anvanda/klassning-av-information/ hämtad 2025-11-11.

informationssäkerhetsklassa informationen och säkerställa att it-tjänstens

- inbyggda skydd är tillräckligt (kravställ till leverantör)
- leverantör vidtar adekvata skyddsåtgärder
- och att den egna verksamheten vidtar adekvata skyddsåtgärder.

Stadsdelsförvaltningen håller även på med att se över processen för upphandling och rutiner kopplade till den för att säkerställa att krav om informationssäkerhet omhändertas och att personuppgiftsansvar utreds. Detta är ett arbete som kommer pågå även under 2026. Läs mer under rubriken 1.2.4 Resultatet från egen uppföljning (VoR och IKP).

1.2.7.3 Tredjelandsöverföringar (Kvarstår)

Den 10 juli 2023 fattade EU-kommissionen beslut om adekvat skyddsnivå för USA. Beslutet innebär att överföringar som sker till organisationer som omfattas av ”EU-US Data Privacy Framework” nu kan ske utan att lämpliga skyddsåtgärder behöver vidtas enligt artikel 46[5] i dataskyddsförordningen.

EU-kommissionens beslut bygger på en presidentorder som fattades av den föregående amerikanska presidenten Joe Biden. En presidentorder kan upphöra när som helst tillskillnad från lagändringar som är mer långsiktiga. I och med president Donald Trump tillträde så finns risken att presidentordern gällande EU-US Data Privacy Framework upphör, vilket innebär att det måste finnas en plan för att flytta personuppgifter som lagras i USA till EU/ESS.

Det här är en risk som Järva stadsdelsförvaltning fortsätter att följa. Läs mer i stadsledningskontorets inriktningsbeslut[6].

1.2.7.4 Skyddade personuppgifter inom förskolan (Kvarstår)

Risken rör närvarohanteringen inom förskolan där barn checkas in när de kommer till förskolan, och ut när de blir hämtade.

Administrativa skyddsåtgärder har vidtagits, men tjänsten följer ändå inte de riktlinjer som staden har för hantering av skyddade personuppgifter. Det här är en risk som Järva stadsdelsförvaltning fortsätter att följa.

---

[5] https://www.privacy-regulation.eu/sv/46.htm hämtad 2025-11-11

[6] https://intranat.stockholm.se/globalassets/nyheter/stadsledningskontoret/dokument/pm-reviderat-inriktningsbeslut-tredjelandsoverforingar-beslutad.docx, Hämtad 2025-11-11

1.2.7.5 Central objektförvaltning har inte tillräckligt med resurs och kan inte svara mot lokal (Stadsdelsförvaltningens) objektförvaltning (Ny)

Det uppstår problem i införande av nya tjänster när det råder resursbrist hos central förvaltning. Detta påverkar implementation av nya gemensamma IT-tjänster och det systematiska informationssäkerhetsarbetet som ska ske löpande i den egna lokala organisationen, då det inte finns en central objektsförvaltning som dels samordnar arbetet eller kan ta emot frågor eller krav. Detta leder till att förvaltningar och medarbetare arbetar på olika sätt.

Det här är en risk som Järva stadsdelsförvaltning fortsätter att följa.

1.2.7.6 Ny teknik, t.ex. behandling av personuppgifter och annan information behandlas med AI utan korrekt analys och dokumentation (Ny)

Risken handlade om att området är nytt, och att både leverantörer och medarbetare inte har tillräckligt med kunskap om hur tekniken bakom AI fungerar, och att smarta lösningar och effektivitet går före säkerhet och den personliga integriteten.

Det kan även vara nya funktioner som slås på i befintliga tjänster utan att stadsdelsförvaltningen har kunnat ta ställning till om funktionen är tillräckligt säker.

Det här är en risk som Järva stadsdelsförvaltning fortsätter att följa.

1.2.7.7 Information om avvikelser (incidenter och andra händelser)

Personuppgiftsincident hos leverantören Miljödata AB

Stockholms stad ska införa en ny it-tjänst för hantering av arbetsmiljöincidenter. Ett införandeprojekt drivs av stadsledningskontoret (SLK). Järva stadsdelsförvaltning har inte varit delaktig i att genomföra en informationsklassning[7], och inte heller varit involverad i arbetet med att ta fram informationssäkerhetskrav gentemot leverantör i upphandlingsförfarandet. Det underlag som förvaltningen har fått ta del av är informationsklassningen (klassningsprotokoll) som projektet har genomfört, vilket inte beskriver de krav som har ställts på leverantören. Projektet har intygat att leverantören lever upp till de krav som har ställts. Underlag från informationssäkerhetsklassningen efterfrågades av informationssäkerhetssamordnaren i juni 2025.

[7] Värdera informationen utifrån konfidentialitet, riktighet och tillgänglighet.

Leverantören som har valts är Miljödata AB. Under lördagen den 23 augusti 2025 upptäcktes det att delar av Miljödatas IT-miljö utsattes för ett cyberangrepp. Stockholms stad hade vid den här tidpunkten inte börjat använda it-tjänsten skarpt ännu, utan enbart i en testmiljö.

Dock så hade riktiga personuppgifter lästs in i testmiljön som hämtades från stadens personalsystem. Brukligt är att använda testdata i en testmiljö. Integritetsskyddsmyndigheten (IMY) har även tidigare granskat ett annat företag som använde sig av riktiga personuppgifter i en testmiljö[8]. Att riktig information hade använts fick Järva stadsdelsförvaltnings stadsdelsdirektör information om i samband med att stadsledningskontoret informerade förvaltningen om personuppgiftsincidenten den 26 augusti.

Den 26 augusti fick Järva stadsdelsförvaltning information om att följande personuppgifter fanns registrerade i testmiljön för månadsanställda.

- Namn
- Organisationstillhörighet
- Personnummer

Den 29 augusti rapporterar Järva stadsdelsnämnd personuppgiftsincidenten till IMY.

Den 2 september meddelande Miljödata stadsledningskontoret att Stockholms stads information hade röjts. Antalet kategorier av personuppgifter som hade röjts hade utökats till dessa för månadsanställda:

- Personnummer
- Förnamn och efternamn
- Telefon och mobiltelefon (arbete)
- E-postadress (arbete)
- Utdelningsadress (hem)
- Organisationskopplingar (Webb-ID strukturen i LISA självservice)
- Anställningsidentitet/AD-konto
- Anställningsperiod
- Anställningsform
- Yrkeskod/yrke/befattning

Detta blev Järva stadsdelsförvaltning informerad om den 3 september.

[8] https://www.imy.se/om-oss/arkiv/nyhetsarkiv/fel-av-sj-anvanda-riktiga-personuppgifter-da-it-system-testades/, hämtades 2025-11-11

Den 4 september uppdaterar Järva stadsdelsnämnd sin anmälan till IMY. Samma dag informeras även medarbetare på Järva stadsdelsförvaltning om incidenten via en nyhet på intranätet.

Den 5 september bekräftar Miljödata att informationen har stulits av hotaktören. Förvaltningen fick information om det samma dag.

Den 14 september publicerades det i medier artiklar om att den stulna informationen hade publicerats öppet på Darknet och att den även påstods innehålla skyddade personuppgifter[9].

Den 15 september publicerades en nyhet för alla medarbetare på intranätet som informerade dem om de publicerade personuppgifterna på Darknet och att det pågår en utredning för att klargöra om skyddade personuppgifter har röjts eller inte. Samma dag lämnar Järva stadsdelsnämnd in en komplettering av anmälan till IMY.

Den 17 september meddelar stadsledningskontoret att skyddade personuppgifter hade röjts. Förvaltningen får samtidigt information om att fler personer omfattas än vad som tidigare hade antagits. Incidenten omfattar anställda och tidigare anställda under perioden 1 januari 2024 till augusti 2025. Tidigare hade det rapporterats gälla anställda för perioden april 2025 till augusti 2025. En nyhet om den nya informationen publiceras på intranätet riktat till medarbetare. Information riktad till anställda och tidigare anställda om incidenten publiceras även på stadens webbplats den 17 september.

Den 25 september informeras även anställda och tidigare anställda digitalt via tjänsten Kivra. Under vecka 40 skickades det ut brev med post till de medarbetare som inte hade anmält att ta emot digital post via Kivra.

Medarbetare med skyddad identitet inom Järva stadsdelsförvaltning informerades löpande allt eftersom de uppdagades finnas med i den publicerade informationen.

I Miljödatas slutrapport skriver de att delar av deras it-miljö blivit utsatt för ett antagonistiskt angrepp i form av en så kallad ransomware-attack. Förutom att polisanmäla händelsen så tog de hjälp av en extern cybersäkerhetsfirma för att assisterat i arbetet med att utreda incidenten, hjälpt till att återställa systemfunktionen och även med att öka Miljödatas motståndskraft. Utredningen visade att hotaktören utnyttjade en sårbarhet i en specifik

[9] https://www.tv4.se/artikel/5BNIEjSVrUlaSaXfrZcjtb/personuppgifter-laeckta-oever-en-miljon-svenskar-drabbade, hämtad 2025-11-11

tredjepartsprodukt som varit exponerad mot internet, och eskalerade sina åtkomsträttigheter. Den aktuella produkten är nu borttagen och ersatt.

Även stadsledningskontoret har gjort en polisanmälan för stadens räkning. Järva stadsdelsförvaltning har ännu inte fått någon information om den utredningen till dagens datum (2025-11-13).

Lärdomar från incidenten

En av lärdomarna som går att dra av incidenten är vikten av en god hantering av leverantörskedjan, vilket även inkluderar andra förvaltningar i staden. Varje nämnd är personuppgiftsansvarig och ägare för sin information, och för att Järva stadsdelsförvaltning ska kunna ta det ansvaret så behöver vi förstå hur vår information hanteras av andra förvaltningar och gemensamma leverantörer.

Detta bör avtalas om internt enligt de rutiner som redan finns i staden, och att vi också får insyn hur det är avtalat med gemensamma leverantörer. För att detta ska kunna efterlevas krävs det kunskap om hos de medarbetare som är involverade i liknande projekt, styrgrupper och även i den dagliga förvaltningen av gemensamma it-tjänster och processer.

En annan lärdom är att använda testdata i testmiljöer för att reducera risken för att känslig information röjs. Sannolikheten att det kan hända kanske är den samma, men konsekvensen för verksamheten, individen och samhället reduceras. Det kan även leda till ekonomiska konsekvenser så som böter från tillsynsmyndighet och skadestånd till de registrerade.

1.3 Förbättringar som föreslås för verksamheten

1.3.1 Informationssäkerhet inom upphandlingsförfarandet (kvarstår)

Tydliggör i inköps- och upphandlingsprocesserna att informationssäkerhets- och dataskyddsfrågor alltid måste beaktas när IT-tjänster ska anskaffas eller när känslig information ska delas med leverantören.

En checklista för upphandlingsförfarandet har tagits fram där krav på informationssäkerhet finns med. Checklistan behöver implementeras. I rutinerna för inköp (direktupphandlingar) finns krav om informationssäkerhet, men tydliga instruktioner om hur det arbetet ska genomföras saknas.

1.3.2 Stärka chefers kunskap inom området informationssäkerhet (kvarstår)

Medvetenheten kring informationssäkerhet och dataskydd behöver spridas i organisationen. Chefer behöver visa vägen och arbeta för en god informationssäkerhetskultur inom sina personalgrupper. En förutsättning för att cheferna ska kunna ta det ansvaret är kompetens och verktyg inom området.

1.3.3 Involvera ledningsgruppen mer i informationssäkerhetsarbetet (kvarstår)

Ta fram en struktur för hur informationssäkerhetsarbetet ska följas upp i ledningsgruppen för att ledningen ska kunna följa informationssäkerhetsarbetet, och vid behov besluta om prioriteringar och åtgärder utifrån riskbedömningar.

1.3.4 Obligatoriska e-utbildningarna ska genomföras i högre grad (kvarstår)

De två obligatoriska e-utbildningarna om informationssäkerhet och dataskydd ska genomföras i högre grad av chefer, medarbetare och ledamöter. Detta för att höja den grundläggande kompetensen inom området.

1.3.5 Utbildningsunderlag till medarbetare som inte har tillgång till datorer

Järva stadsdelsförvaltning har flera yrkesgrupper där personalen inte har tillgång till datorer och därför inte heller kan genomföra de obligatoriska e-utbildningarna i samma utsträckning som andra yrkesgrupper. Det finns dessutom behov av utbildningsunderlag som presenteras på ett enklare sätt då flera medarbetare inte har svenska som första språk. Utbildningarna bör anpassas efter personalgruppernas behov och verksamhetsområde.

1.4 Treårsplan för åren 2026-2028

1.4.1 2026

- Ta fram utbildningsunderlag till verksamheter där medarbetare inte har tillgång till datorer.
- Fortsatt implementering av pm3-modellen.
- Ta fram metod/arbetssätt för att följa upp informationssäkerhetsklassningar systematiskt.
- Påbörja implementering av NIS 2-direktivet och utgå från arbetet som har genomförts i RSA-arbetet.
- Ta fram information för hur tjänster som bygger på artificiell intelligens (AI).
- Informationssäkerhetsklassa informationstillgångar.

- Inventering av personuppgiftsbehandlingar.
- Revidera lokala tillämpningsanvisningarna.
- Genomföra övning för ledningsgrupp till exempel antagonistisk cyberattack.
- Inventering av kontinuitetsplaner för att mäta hur motståndskraftig stadsdelsförvaltningen är när information inte är tillgänglig, eller går förlorad.

1.4.2 2027

- Fortsatt implementering av pm3-modellen.
- Fortsatt implementering av NIS 2-direktivet.
- Genomföra övning inom verksamheter, till exempel nätverksbortfall eller dataförlust.
- Informationssäkerhetsklassa informationstillgångar.
- Inventering av personuppgiftsbehandlingar.
- Revidera lokala tillämpningsanvisningarna.

1.4.3 2028

- Informationssäkerhetsklassa informationstillgångar.
- Inventering av personuppgiftsbehandlingar.
- Revidera lokala tillämpningsanvisningarna.
- Genomföra övning inom verksamheter, till exempel nätverksbortfall eller dataförlust.
- Slutföra implementering av pm3-modellen.
- Genomföra övning för ledningsgrupp till exempel antagonistisk cyberattack.

Beslutad xxx