Stockholms stad

Informationssäkerhet

- Ledningens genomgång år 2024

Servicenämnden

Ledningens genomgång
Bilaga till Servicenämndens Verksamhetsplan 2024
Dnr: SF 2023/654
Kontaktperson: Maria wedenlid

Ledningens genomgång är ett begrepp inom informationssäkerhet som syftar till att de som ansvarar för informationssäkerheten inom en organisation, minst årligen ska informera sig om hur arbetet går.

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 eller 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 ska ta fram en 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 nämndens verksamhetsuppdrag i budget och följa *Riktlinje för informationssäkerhet* i Stockholms stad.

Dessa aktiviteter ska redovisas både i Ledningens genomgång samt i nämndens verksamhetsplan under mål 3.5. Inventering och informationsklassning är grunden i informationssäkerhetsarbetet. För 2024 är därför området registerförteckning och informationsklassning särskilt prioriterat i Ledningens genomgång.

Alla nämnder och bolagsstyrelser ska prioritera att ta fram en plan för att inventera och klassa information som används i verksamheten alternativt se över och uppdatera genomförda klassningar.

---

[1] Tillämpningsanvisning till stadens riktlinje för informationssäkerhet

[2] anvisningar-for-namndernas-arbete-med-verksamhetsplan-2024.pdf (stockholm.se)

Innehållsförteckning

1. Ledningssystem för informationssäkerhet, LIS 4
1.1 Vad påverkar Servicenämndens informationssäkerhetsarbete? 4
1.1.1 Finansborgarrådets förslag till budget 2024 4
1.1.2 Risk och sårbarhetsanalys 5
1.1.3 Resultatet från egen uppföljning (IKP) 6
1.1.4 Risker som identifierats i GDPR-årsrapport 6
1.1.5 Kompetenslyft ledningsgrupp – C2 Solutions 7
1.1.6 Digitala lyftet – för att öka den digitala mognaden 7
2.1 Förbättringar för verksamhetens LIS 8
2.1.1 Serviceförvaltningens lokala anvisning för informationssäkerhet 8
2.1.2 Kompetenslyft ledningsgrupp - förslag på fortsatt arbete 8
2.1.3 Digitala lyftet – för att öka den digitala mognaden 8
3 Prioritering av åtgärder 9
3.1 Under 2024 ska serviceförvaltningen 9
3.2 Under 2025 ska serviceförvaltningen 10
3.3 Under 2026 ska serviceförvaltningen 10

1. 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 känsliga 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 som är en bilaga till stadens Kvalitetsprogram[3]. Till riktlinjen finns tillämpningsanvisningar som är fastställda av stadsdirektören.

Tillämpningsanvisningarna reglerar ansvar och roller sett till Stockholms stads systematiska informationssäkerhetsarbete. För Servicenämnden räkning har förvaltningschef fastställt en så kallad lokal anvisning som beskriver hur stadens övergripande ledningssystem för informationssäkerhet omhändertas inom serviceförvaltningen.

1.1 Vad påverkar Servicenämndens informationssäkerhetsarbete?

För att upprätthålla ett informationssäkerhetsarbete som är aktuellt över tid ska serviceförvaltningen 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.

1.1.1 Finansborgarrådets förslag till budget 2024

Budgetuppdrag

Servicenämnden har i budget 2024 ett uppdrag att i samarbete med kommunstyrelsen, förskolenämnden, kulturnämnden, socialnämnden, utbildningsnämnden, äldrenämnden och stadsdelsnämnderna påbörja viss drift av centralt beredskapslager för medicinskt skydds- och förbrukningsmateriel, livsmedel samt vissa förbrukningsmateriel i syfte att höja stadens beredskapsförmåga. [4]

---

[3] Stockholms stads kvalitetsprogram (start.stockholm)

[4] kommunstyrelsens-forslag-till-budget-2024.pdf (start.stockholm)

Servicenämnden ska även delta i arbetet inom stadens sektorsorganisation för civil beredskap.
Serviceförvaltningen är utsedd sektorsansvarig för *Livsmedelsförsörjning och dricksvatten*. Som sektorsansvarig ska förvaltningen hålla samman beredskapsutvecklingen och få till stånd samverkan inom sektorn. I takt med utvecklingen av strukturen och sektorsorganisationen kan det bli aktuellt att ta fram och löpande uppdatera sektorsspecifika risk- och sårbarhetsanalyser. Förvaltningen har även ansvaret att hålla ihop sektorns samverkan och samordning med statliga myndigheter och näringsliv.

Intern kontroll
Syftet med intern kontroll är att skapa förutsättningar för en ändamålsenlig och effektiv användning av skattemedel samt för att upprätthålla service med hög kvalitet till kommuninvånarna.

Genom en tillräcklig intern kontroll skapas förutsättningar att förebygga, upptäcka och åtgärda oönskade händelser och därmed minimera risker i verksamheten samt säkra tillgångar och förhindra förluster och oegentligheter som skadar stadens anseende. Arbetet med intern kontroll är en del av stadens kvalitetsarbete.

Utöver nämndens egna identifierade processer ska nämnden, enligt stadens anvisning, ha med den obligatoriska stadsövergripande processen *Systematiskt informationssäkerhetsarbete* i sin väsentlighets- och riskanalys och bedöma om de ska med i internkontrollplanen.

Serviceförvaltningen gör varje år en bedömning av de fem obligatoriska arbetssätten, *behörighetshantering, implementering av lokal anvisning, incidenthantering, informationsklassning* och *informationssäkerhet inom upphandlingsförfarandet*, i väsentlighets- och riskanalysen. Därefter beslutar förvaltningsledningen om vilka av arbetssätten som ska ingå i intern kontrollplanen kommande år.

1.1.2 Risk och sårbarhetsanalys
Stadens arbete med risk- och sårbarhetsanalys (RSA) bedrivs i en tvåårscykel. En ny cykel inleds under 2024.
Serviceförvaltningen har i risk- och sårbarhetsarbetet 2022 identifierat ett antal processer som kan ha risker inom informationssäkerhet och har åtgärdsplaner och kontinuitetsplaner för de delar som förvaltningen har rådighet över. Förvaltningen följer stadens risk- och sårbarhetscykel och instruktioner.

Utöver förvaltningens egna risk- och sårbarhetsarbete kommer förvaltningen att arbeta med dessa frågor inom sektorsorganisationen, både för den sektor som förvaltningen ansvarar för, samt för de tre som serviceförvaltningen deltar i.

1.1.3 Resultatet från egen uppföljning (IKP)

I Servicenämndens tertialrapport 2 2023 rapporterades följande; Inga väsentliga avvikelser har rapporterats eller identifierats under perioden. Arbetet bedöms fortlöpa enligt plan.

I årets internkontrollplan ska kontroll göras av att alla upphandlingar har beaktat informationssäkerhetskrav. De stöddokument som används vid upphandlingar behöver förtydligas med punkter om informationssäkerhet. Ett arbete med att identifiera vilka delar i upphandlings- och avtalsprocessen som måste kompletteras med checklista för informationssäkerhet har genomförts. Nu införs denna checklista till att börja med i upphandlingsprocessen för att sedan införas i avtalsprocessen. Detta har även aktualiserats som en förändring som behöver göras i stadens generella processer för upphandling och avtal.

Ovan nämnda arbete har även resulterat i att förvaltningen ser ett behov av att än mer tydligt koppla samman informationssäkerheten med metodstödet pm3. För att omhänderta tillämpningsanvisningarna för informationssäkerhet krävs kunskap i stadens objektstyrning. Förvaltningen kommer arbeta med att utveckla arbetssätt för att säkerställa att både informationssäkerhet och objektstyrning blir en fastställd del av inköpsprocessen.

I syfte att effektivisera och förbättra tydlighet i förvaltningens förteckning av personuppgiftsbehandling utreds möjligheter av systemstöd. Den nuvarande förteckningen har kompletterats med ytterligare kolumner enligt de rekommendationer som dataskyddsombudet lämnat i sin årsrapport för 2022.

1.1.4 Risker som identifierats i GDPR-årsrapport

Dataskyddsombudet har i årsrapporten för 2022 föreslagit ett antal åtgärder gällande Tekniska och organisatoriska åtgärder, bland annat om hur informationsklassningar, riskanalyser och konsekvensanalyser bör dokumenteras.

Förvaltningen har strukturerat sitt behandlingsregister enligt de krav som staden och integritetsmyndigheten har på ett behandlingsregister. Dataskyddsombudet rekommenderar ändå att

informationen om Tekniska och organisatoriska åtgärder ska finns med i behandlingsregistret i syfte att systematisera och effektivisera arbetet, inte i enlighet med de faktiska kraven. Förvaltningen avser dock att beakta dataskyddsombudets rekommendationer genom att säkerställa att informationen finns och att undersöka om behandlingsregistret bör kompletteras med dessa uppgifter för att skapa en ökad tillgänglighet av informationen.

1.1.5 Kompetenslyft ledningsgrupp – C2 Solutions

Under 2023 genomför Stadsledningskontoret, SLK, en kompetenshöjande satsning inom området informationssäkerhet. En del av detta omfattar aktiviteten *Kompetenslyft Ledningsgrupp*, genom vilken stadens ledningsgrupper erbjöds kompetenshöjande besök.

Den 7 februari genomfördes ett sådant besök hos Serviceförvaltningens ledningsgrupp.

Besöket genomfördes av två externa konsulter på uppdrag av SLK, vilka under cirka två timmar utbildade gruppen inom informationssäkerhetsområdet och diskuterade olika för förvaltningen specifika frågor av intresse.

Hos serviceförvaltningen identifierades:

- Ledningen är engagerad och redo att driva frågorna.
- Förvaltningen har gjort ett stort arbete inom dataskydd, där en grupp med olika kompetenser tillsammans utreder och bereder frågor inom området. Tvärkompetens är något som underlättar arbetet med informationssäkerhet generellt och något som bör lyftas som ett gott exempel inom verksamheten och staden i stort.
- Förvaltningen arbetar löpande med utbildning av medarbetare och har ett aktivt arbete avseende personuppgiftsincidenter.

1.1.6 Digitala lyftet – för att öka den digitala mognaden

Under 2023 genomförde serviceförvaltningen digitala tester av alla medarbetare för att kartlägga kompetensnivåer och eventuella gap inom ett antal digitala områden. Syftet är att öka den digitala mognaden och stärka medarbetarna. Utifrån testresultaten har förvaltningsledningen beslutat om önskade förflyttningar och specificerat utbildningsinsatser för att skapa en stabil grundnivå inom IT. Ett av områdena där förvaltningens medarbetare har ett behov av mer kunskap är *cybersäkerhet och dataskydd*.

2.1 Förbättringar för verksamhetens LIS

2.1.1 Serviceförvaltningens lokala anvisning för informationssäkerhet

Den 13 mars 2023 fastställde förvaltningschef Lokala anvisning för informationssäkerhet.
Anvisningen är presenterad i sin helhet för förvaltningens samtliga chefer på ett chefsforum den 20 mars och finns tillgänglig för alla medarbetare på förvaltningens samarbetsyta.

Enligt anvisningen har Serviceförvaltningen inte ett fastställt årshjul för arbetet med informationssäkerhet, utan planerar arbetet utifrån väsentlighets- och riskanalysen som genomförs i samband med verksamhetsplaneringen och framtagande av intern kontrollplan.

I samband med verksamhetsberättelse och bokslut tar förvaltningen del av dataskyddsombudets årsrapport och hänsyn tas till eventuella rekommendationer till personuppgiftsansvarig som lämnas i rapporten.

2.1.2 *Kompetenslyft ledningsgrupp* - förslag på fortsatt arbete

Efter genomförd *Kompetenslyft ledningsgrupp* föreslog konsulterna från C2 Solutions följande förslag på fortsatt arbete:

- Låt allt arbete utgå från informationshanteringen i verksamhetens ordinarie processer – undvik att skapa isolerade stuprör.
- Ta fram lathundar till chefer och medarbetare (som stödmaterial till den lokala tillämpningsanvisningen) som enkelt beskriver vilka uppgifter som ingår i ansvaret för olika roller och hur det kan integreras i vardagen.
- Ta fram en gemensam incidenthanteringsprocess för så många typer av incidenter som möjligt (informations/IT-säkerhet, dataskydd, arbetsmiljö) som bidrar till snabb identifiering, bedömning, hantering och återställning.
- Säkerställ att informationssäkerhetsfrågorna lyfts fram och ingår i det interna utvecklingsarbete som pågår inom verksamheten, särskilt för nya digitala tjänster som erbjuds.

2.1.3 Digitala lyftet – för att öka den digitala mognaden

Förvaltningsledningen har beslutat att stärka medarbetarna inom området *cybersäkerhet och dataskydd* utifrån resultat i Digitala lyftet. Sen tidigare ska samtliga medarbetare genomföra stadens

obligatoriska e-utbildningar inom dataskydd och informationssäkerhet. Förvaltningen ser ett behov hos medarbetarna att reflektera kring dessa frågor gemensamt i arbetsgrupper. Därför kommer förvaltningen uppmana samtliga chefer att genomföra stadsledningskontorets nya e-utbildningar inom informationssäkerhet med tillhörande stödmaterial på arbetsplatsträffar. Detta är även lyft i förvaltningens kompetensförsörjningsplan.

3 Prioritering av åtgärder

3.1 Under 2024 ska serviceförvaltningen

Förvaltningen ska under 2024 följa upp att den lokala anvisningen efterlevs, främst med fokus på att;

- chefer;
  - årligen ser till att samtliga medarbetare och konsulter genomför stadens obligatoriska e-utbildningar för informationssäkerhet och dataskydd
  - följer upp och utreder de incidenter som verksamheten anmäler i IA.

- objektledare;
  - tillser att informationstillgångar är klassade och att handlingsplaner från klassning tas om hand för systemet.

Förvaltningen har informationssäkerhet som återkommande tema på chefsforum för att upprätthålla kompetens och rutiner. Den lokala anvisningen bör även revideras i avsnitt 4 om befintliga rutiner, eftersom nya rutiner har framkommit sen anvisningen fastställdes.

Under 2024 ska serviceförvaltningen prioritera;

- att inventera och dokumentera vilka informationsklassningar som är genomförda
- att sätta strukturer för informationssäkerheten inom de nya budgetuppdragen gällande centralt omsättningslager och sektorsansvar
- att stärka medarbetarna inom området cybersäkerhet och dataskydd. Förvaltningen kommer genomföra stadsledningskontorets nya e-utbildningar inom informationssäkerhet med tillhörande stödmaterial.
- fortsätta utveckla rutiner för att tydliggöra informationssäkerhet i inköpsprocessen
- utveckla hanteringsanvisningarna
- fastställa en digital strategi för förvaltningen

- säkerställ att informationssäkerhetsfrågorna lyfts fram och ingår i det interna utvecklingsarbete som pågår inom verksamheten, särskilt för nya digitala tjänster som erbjuds.

3.2 Under 2025 ska serviceförvaltningen

Under 2025 ska serviceförvaltningen prioritera;

- att etablera en rutin för regelbundna informationsklassningar
- att ta fram en gemensam incidenthanteringsprocess för så många typer av incidenter som möjligt (informations/IT-säkerhet, dataskydd, arbetsmiljö) som bidrar till snabb identifiering, bedömning, hantering och återställning.
- Utifrån RSA säkerställa kontinuitetsplaner finns.

3.3 Under 2026 ska serviceförvaltningen

Under 2026 ska serviceförvaltningen prioritera:

- Revidering av lokal anvisning.
- Granska hur väl lokal rutin för regelbundna informationsklassningar följs.
- Öva utifrån kontinuitetsplaner.

Fastställd av förvaltningschef Charlotte Goliath 2023-12-05