

Redovisning av grundläggande baskrav för informations säkerhet

Vid frågor kontakta Funktionen för stadsövergripande informations säkerhet, vid avdelningen för it och digitalisering, stadsledningskontoret.
Redovisningen ska fyllas i och biläggas nämndens/bolagets verksamhetsberättelse för 2022.
E:post: funktion.slk.informationssakerhetcentralt@stockholm.se

Kommentar

Anvisningar

Detta dokument ger anvisningar om hur nämnder och bolag ska redovisa sin följsamhet till ett urval av kraven från stadens riktlinjer för informations säkerhet. Urvalet är gjort för att representera några av de mest grundläggande baskraven som en nämnd/bolag har att genomföra för att kunna visa att nämnden/bolaget leder och styr risker inom informations säkerhetsområdet enligt lagkrav och riktlinjer. Notera att det finns lagkrav på informations säkerhetsområdet som innebär att nämnd/styrelse genom dokumentation ska kunna visa sin efterlevnad till de krav som gäller för verksamheten, varför redovisningen fyller en funktion även i det avseendet. Baskraven i denna anvisning är inte uttömmande för det informations säkerhetsarbete som nämnden/bolaget har att genomföra enligt krav i lagar och riktlinjer.

Anvisningen är avsedd att besvaras med stöd av den *lokala informations säkerhetssamordnaren* som är sakkunnig och utgör förvaltningschefens/bolagschefens primära stöd.

Syftet med informations säkerhetsarbetet är att skapa förutsättningar att ändamålsenligt och effektivt nå stadens mål om trygg, effektiv och modern storstad för stadens invånare, företagare och besökare. Stockholm har som ambition att bli världsledande inom digitaliseringsområdet vilket ytterligare adresserar vikten av dessa frågor.

Den uppföljning som anvisas i detta dokument är även en del av den interna kontrollen som stadens verksamheter inklusive den centrala informations säkerhetsfunktionen är skyldig att utöva för att visa att stadens verksamheter bedrivs i enlighet med de mål och riktlinjer som fullmäktige har beslutat.

Informations ägarens ansvar

Nämnden/bolagsstyrelsen är ytterst informations ägare, tillika personuppgiftsansvarig, i sin verksamhet. Informations ägaren ansvarar för att den information som verksamheten hanterar är riktig och tillförlitlig samt ansvarar för hur informationen hanteras och sprids. Det är därför ett budgetuppdrag för nämnder och bolag att arbeta systematiskt och ändamålsenligt med informations säkerhet.

Förvaltnings- och bolagschef är nämnden/styrelsens operativa informations ägarrepresentant i linjen. Förvaltnings- och bolagschef ansvarar för styrningen och resurs sättningen av det lokala informations säkerhetsarbetet. Förvaltningschef/bolagschef ska årligen tillse att verksamhetsplanen omfattar relevanta informations säkerhetsaktiviteter samt följa upp utfallet av detta arbete. Avsikten med denna anvisning är att hjälpa förvaltnings- och bolagschefer tillse att vissa grundläggande baskrav planeras in i nästföljande verksamhetsplan och följs upp årligen.

Redovisning av grundläggande baskrav

	Krav	Status	Kommentar
1	Förvaltningschef/bolagschef har inrättat en <i>ändamålsenlig organisation</i> ¹ med tillräckliga resurser för att hantera verksamhetens aktiviteter ² för informations säkerhet inklusive dataskydd samt övriga områden ³ .	Ja	Valnämnden har en informations säkerhetssamordnare och ett dataskyddsombud.
2	Förvaltningschef/Bolagschef har fastställt en <i>lokal anvisning</i> ⁴ som beskriver hur stadens övergripande ledningssystem för informations säkerhet omhändertas i den egna verksamheten.	Ja	Valnämnden följer stadsledningskontorets anvisningar.
3	Förvaltningschef/bolagschef har tillsett att dataskyddsombudet har en <i>självständig och oberoende ställning</i> ⁵ och rapporterar till nämnd/styrelse ⁶ .	Ja	Valnämnden har anlitat ett externt dataskyddsombud som finns på JPInfonet.

4	Förvaltningschef/bolagschef har tillsett a) att verksamhetens informationsmängder ⁷ har kartlagts samt b) att de viktigaste informationsmängderna även har klassat och riskbedömts.	a) Ja b) Ja	a) Registerförteckningen är uppdaterad. b) Informationssäkerhetsklassning är gjord.
5	Förvaltningschef/bolagschef har tillsett att verksamheten, utifrån riskprioritering ⁸ , har följt upp implementeringen av skyddsåtgärder för de viktigaste informationsmängderna. Skyddsåtgärderna berör både den egna verksamheten samt leverantörer/biträden.	Ja	Leverantören har fått visa vilka skyddsåtgärderna har vidtagit.
6	Förvaltningschef/bolagschef har säkerställt att registerförteckningen ger en rättvisande bild av verksamhetens personuppgiftsbehandlingar och hålls uppdaterad.	Ja	
7	Förvaltningschef/bolagschef har informerat sig om att verksamhetens informationssäkerhetsrisker hanteras i en handlingsplan ⁹ , samt beslutat om vilka av dessa som tas om hand i verksamhetsplanen för nästkommande år.	Ja	

Fotnoter:

1) Olika verksamheter behöver utforma och införa stöd på olika sätt för att få bästa effekt, det är det som avses med begreppet *ändamålsenlig organisation*.

2) *Exempel på möjliga aktiviteter som ska utföras för att informationssäkerhetsarbetet inkl. dataskydd följer nedan. Aktiviteterna utgör en sorts verktygslåda:*

Informationsklassning, riskanalys, riskbehandling, behörighetsstyrning, uppföljning av behörigheter, kravställning i avtal, säkerhetshantering i förvaltningsarbete, upphandlingar, och projekt, uppföljning av skyddsåtgärder för egen- resp. leverantörs verksamhetsprojekt för etablering av dataskydd, registerförteckningar, konsekvensbedömningar, upprättande av personuppgiftsavtal med instruktioner, översyn och statusrapportering, inventering och hantering av 3:e-landsöverförande, juridisk omvärldsbevakning av. GDPR och dataskyddspraxis

3) Övriga områden som ställer säkerhetskrav varierar beroende på den verksamhet som bedrivs och kan t.ex. avse NIS-direktivet, patientdatalagen, tillgänglighetsdirektivet, m.m.

4) Den så kallad lokala anvisningen är ett dokument som beskriver den inrättade organisationen som ska hantera verksamhetens aktiviteter för informationssäkerhet (det är alltså ett dokument som beskriver kravpunkten 1 - *Ändamålsenlig organisation*). Den lokala anvisningen ska minst beskriva ansvarsfördelningen inom förvaltningens/bolagets egna informationssäkerhetsorganisation (roller och mandat), vilken effekt informationssäkerhetsarbetet ska leda till lokalt, specifik lagstiftning som gäller för verksamhetens informationshantering samt hur arbetet följs upp lokalt. Det är ett krav att förvaltningschef/bolagschef kan visa hur det lokala informationssäkerhetsarbetet styrs, vilket den lokala anvisningen delvis redogör för.

5) Dataskyddsombudet (DSO) ska kunna arbeta självständigt och oberoende, utan att bli påverkad av andra inom organisationen. Det är därför viktigt att dataskyddsombudet inte har andra arbetsuppgifter som kan krocka med rollen som dataskyddsombud. (källa IMY, <https://www.imy.se/verksamhet/dataskydd/det-har-galler-enligt-gdpr/dataskyddsombud/>)

Om dataskyddsombudet företräder arbetsgivaren i en *chefsroll* eller har andra utföraruppdrag i linjen såsom *arkivarie* eller deltar operativt i säkerhetsarbetet i rollen som *lokal informationssäkerhetssamordnare* så utgör det ett hinder för ombudets självständighet och oberoende. Den personuppgiftsansvarige (PuA) råder över ändamål och medel vilket dataskyddsombudet måste vara frikopplad från.

6) Dataskyddsombudet ska rapportera direkt till den personuppgiftsansvariges eller personuppgiftsbitrådets högsta förvaltningsnivå. (källa: GDPR Artikel 38.3)

7) Det är verksamhetens information som ska skyddas, därför behöver verksamhetens information först kartläggas. Med informationsmängd avses en logisk sammanhängande gruppering av information exempelvis inom en process. Olika verksamheter hanterar olika information beroende på verksamhetens uppdrag och de aktiviteter som följer av uppdraget, t.ex. för en stadsdelsnämnd, en fackförvaltning eller ett av stadens bolag.

8) Efter en genomförd klassning får verksamheten ut en lista över de skyddsåtgärder som verksamheten behöver arbeta med för att skydda informationen. Riskprioritering syftar till att skilja på höga och låga risker i förvaltningarnas/bolagens verksamheter, så att resurser kan styras till skyddsåtgärder som är mest kritiska för verksamheten. Riskprioritering utgör således ett stöd för vilka skyddsåtgärder som verksamheten väljer att tillämpa och i vilken ordning.

Prioriterade risker kan exempelvis röra sårbarhet för ransomware, personuppgiftsbehandlingar med höga risker, 3:e-landsöverföringar av personuppgifter, NIS-tillgänglighetsrisker, brister i behörighetsstyrning, brister i verksamhetens rutiner, brister i verksamhetens/leverantörens uppföljning av skyddsåtgärder, ej genomförda konsekvensbedömningar för dataskydd, brister i verksamhetens mejlhantering av känslig information eller personuppgifter, framtagande av rutiner för att hantera brister, brister av skydd för känsliga personuppgifter, avsaknad eller fel i lagliga grunder för personuppgifter eller känsliga personuppgifter, avsaknad av eller brister i rutin för registerutdrag av personuppgifter, m.m.

9) För att visa på att ett ändamålsenligt och effektivt informationssäkerhetsarbete bedrivs i verksamheten över tid behöver förvaltningschef/bolagschef informera sig om att risker löpande identifieras, prioriteras och att prioriterade risker åtgärdas. Informationssäkerhetssamordnaren har den verksamhetsövergripande stödfunktionen att sammanställa sådan information från verksamheten, att informera förvaltningschef/bolagschef om prioriterade informationssäkerhetsrisker för verksamheten samt följa upp det fortsatta arbetet. Med handlingsplan avses sådan dokumentation som verksamheten använder för motsvarande planering och uppföljning av risker. En handlingsplan kan visa vilka frågor som beslutats för åtgärd, vem som ansvarar för genomförandet, beräknade datum när åtgärder är genomförda samt hur uppföljning/utvärdering av åtgärder planeras och av vem. Handlingsplanen bör omfatta risker från för verksamheten relevanta kravområden såsom riktlinjer för informationssäkerhet, dataskydd, NIS-direktivet, patientdatalagen, tillgänglighetsdirektivet m.fl.