Stockholms stad

Nämnd/bolag: Stockholms Hamn AB

Redovisning av grundläggande baskrav för informationssäkerhet

Vid frågor, kontakta Funktionen för stadsövergripande informationssäkerhet, vid avdelningen för it och digitalisering, stadsledningskontoret.
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 informationssäkerhet. 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 informationssäkerhetsområdet enligt lagkrav och riktlinjer. Notera att det finns lagkrav på informationssäkerhetsområdet som innebär att nämnd/styrelse genom dokumentation ska kunna visa sin efterlevnad till de krav som gäller för verksamheten, varför redovisningen fyller en viss funktion även i det avseendet. Baskraven i denna anvisning är inte uttömmande för det informationssäkerhetsarbete som nämnden/bolaget har att genomföra enligt krav i lagar och riktlinjer.

Syftet med informationssäkerhetsarbetet 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 informationssäkerhetsfunktionen är skyldig att utöva för att visa att stadens verksamheter bedrivs i enlighet med de mål och riktlinjer som fullmäktige har beslutat.

Informationsägarens ansvar
Nämnden/bolagsstyrelsen är ytterst informationsägare, tillika personuppgiftsansvarig, i sin verksamhet. Informationsägaren 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 informationssäkerhet.

Förvaltnings- och bolagschef är nämnden/styrelsens operativa informationsägarrepresentant i linjen. Förvaltnings- och bolagschef ansvarar för styrningen och resurssättningen av det lokala informationssäkerhetsarbetet. Förvaltningschef/bolagschef ska årligen tillse att verksamhetsplanen omfattar relevanta informationssäkerhetsaktiviteter samt följa upp utfallet av detta arbete. Avsikten med denna anvisning är att hjälpa förvaltnings- och bolagschefer tillse att vissa grundläggande baskrav planeras och följs upp årligen, enligt krav från lagar och riktlinjer.

Redovisning av grundläggande baskrav

Krav	Status	Kommentar
Förvaltningschef/bolagschef har utsett en lokal informationssäkerhetssamordnare.	Ja	Angelica Wagneryd
Nämnd/bolagsstyrelse har utsett ett lokalt dataskyddsombud.	Ja	Angelica Wagneryd
Förvaltningschef/bolagschef har informerat sig om allvarliga informationssäkerhetsincidenter som drabbat verksamheten under det gångna verksamhetsåret.	Ja	Typer av incidenter som kan kopplas till denna punkt utöver rena informationssäkerhetsincidenter är NIS-direktivet, GDPR/dataskyddet och säkerhetsssskyddet. Samtliga incidenter som inte omfattas av sekretess hanteras i IA som tillhandahålls av AFA via Staden. Inträffade incidenter lyftas upp på lämplig nivå i relevanta forum tex enhetsmöten och avstämningsmöten osv för rimlig informationsspridning. IA är väl förankrat i verksamheten.
Förvaltningschef/bolagschef har informerat sig om andel medarbetare som under det gångna verksamhetsåret genomgått stadens obligatoriska e-utbildning (eller annan likvärdig) om informationssäkerhet och dataskydd.	Ja	Vi använder inte Stadens utbildning i Informationssäkerhet då vi istället har motsvarande information i intern utbildning "Säker i Hamn" om än betydligt mer komprimerad. Orsaken till det vägvalet är att vi får en garanti på att den anställda har genomgått utbildningen då de annars inte får sin behörighetskort/tjänstekort och alltså inte kan arbeta vilket man inte får via Stadens utbildning. Utbildningen är repetativ då de anställda genomgår den varannat år. Ev. kommer det att förändras så att den skall genomföras varje år just med tanke på att innehållet vidgats med bl.a. informationssäkerhet. Samtliga anställda har genomgått utbildningen inom aktuellt intervall och 38 stycken anställda har hittills i år genomfört utbildningen. Dataskyddet är så pass nytt och kräver mer av den anställde när det kommer till mognadsnivå, mindset och beteende. Vi såg inte att vi genom att baka in detta i intern utbildning "Säker i Hamn" skulle få det resultat som Staden kräver avseende den grundläggande kunskapsnivå inom området. Inte heller såg vi det som ekonomiskt rimligt att skapa en parallell utbildning i nuläget då Staden tagit fram en sådan som dessutom är gratis. Alla anställda ska genomgå den utbildningen i samband med att de anställs. Inget beslut har fattats om hur ofta denna utbildning ska genomföras när du väl är anställd men förslaget är även här att den görs årligen. För närvarande är det ett ärende inom staden och hos TIETO då det ej går att avläsa vem som genomfört utbildning när men den har rullats ut till samtliga i
Förvaltningschef/bolagschef har tillsett att verksamhetsplanen för nästkommande år (2021) omfattar sådana åtgärder som är lämpliga utifrån de brister som uppdagats i punkterna 1-4 ovan.		
Förvaltningschef/bolagschef har tillsett att verksamhetsplanen för nästkommande år (2021) omfattar en översyn av nämndens/bolagets registerförteckningar enligt krav i dataskyddsförordningen.	Ja	Ja en översyn är inplanerad främst för att undersöka eventuella underbiträden hos våra personuppgiftsbiträden ytterligare för att säkerställa att personuppgifter inte behandlas utanför EU och på så sätt skulle bryta mot Dataskyddsförordningen. Registerförteckningen finns i systemet Draftit som tillhandahålls via Staden.
Förvaltningschef/bolagschef har tillsett att verksamhetsplanen för nästkommande år (2021) omfattar en översyn av nämndens/bolagets informationsklassningar enligt kraven i riktlinjer för informationssäkerhet.	Ja	Den här aktiviteten är en naturlig del i vårt systematiska informationssäkerhetsarbete. Praktiskt sett så är det respektive informations-, process-, eller systemägare som ansvarar för att informationsklassingen genomförs. Klassningsledare är Informationssäkerhetssamordnaren som stöttar och samordnar. Informationsklassningarna finns i systemet KLASSA som tillhandahålls av SKR via staden.