Antagen av Kommunfullmäktige den 27 juni 2012, § 144, Dnr: KS 1032/12-900

Informationssäkerhetspolicy för Båstads kommun

Inledning

Vi behöver skydda organisationens information på ett sätt som passar vår verksamhet. Detta är nödvändigt för att vi ska uppnå verksamhetsmålen och för att kunder, uppdragsgivare, samarbetspartner, allmänhet och anställda ska känna förtroende för oss. Därför arbetar vi aktivt med informationssäkerhet så att all vår information alltid ska vara konfidentiell, riktig och tillgänglig.

Vi har valt ett gemensamt och strukturerat sätt att arbeta med informationssäkerhet som bygger på den svenska och internationella standarden LIS (ledningssystem för informationssäkerhet). Med stöd av LIS får vi rätt nivå på informationssäkerheten samtidigt som våra anställda får ett stöd i sitt dagliga arbete. Arbetet med informationssäkerhet ska vara långsiktigt och kontinuerligt, omfatta alla delar av vår verksamhet och alla de informationstillgångar som vi äger eller hanterar. Personalen ska få fortlöpande utbildning för att förstå hur informationssäkerhetsarbetet fungerar.

Begreppsförklaringar

Informationstillgångar är allt som innehåller information.

- Informationssäkerhet är säkerhet beträffande informationstillgångar rörande förmågan att upprätthålla önskad konfidentialitet, riktighet och tillgänglighet.
- Konfidentiell information får inte nås av eller avslöjas för någon obehörig. Oftast gäller det innehållet i en informationstillgång men ibland är även tillgångens existens hemlig.
- Riktig information innebär att informationen inte obehörigen får förändras, varken av misstag eller på grund av en funktionsstörning.
- Tillgänglig information innebär att informationen går att utnyttja av behörig användare när det behövs och så mycket som det behövs.
- Ett ledningssystem för informationssäkerhet (LIS) är ett verktyg som hjälper oss att upprätta, införa, driva, övervaka, granska, underhålla och förbättra den önskade nivån på informationssäkerhet i vår organisation.

Viljeinriktning för informationssäkerhetsarbetet

För arbetet med information i Båstads kommun ska gälla att:

- Hantering ska ske på ett sådant sätt att risker för skada på personer, värden, information, och informationssystem minimeras
- Försörjningen ska vara säker, effektiv och bidra till ökat skydd och stöd för medarbetare, samverkande partners och tredje man
- Säkerhetsarbetet ska utgöra en grundpelare för att kommunen även ska kunna utföra sina uppgifter vid extraordinära händelser.

Riktlinjer i informationssäkerhetsarbetet

- Aktuella risker och hot mot informationen, dess hantering och behandling, ska kartläggas inom respektive verksamhet. Denna kartläggning ska ligga till grund för införandet av ett adekvat informationsskydd.
- All information ska klassas efter sin känslighet och därefter få rätt skydd samt finnas tillgänglig när den behövs.
- Det ska finnas tillgång till en gemensam, säker och väl definierad It-infrastruktur.
- Utrustning ska hanteras och förvaras på ett säkert sätt.
- Utbildning i informationssäkerhet ska ges till samtliga anställda.
- Externt engagerad personal och externa tjänsteleverantörer ska ha tagit del av de regler som är relevanta för deras uppdrag innan de får hantera kommunens informationssystem och informationsresurser.

Ansvar

Kommunfullmäktige fastställer informationssäkerhetspolicyn och anslår medel för verksamheten. Kommunstyrelsen är ytterst ansvarig för informationssäkerheten i Båstads kommun. Säkerhetsgruppen har det operativa ansvaret under kommunstyrelsen. Respektive verksamhetsområde kan ta fram riktlinjer och rutiner för sitt område till stöd för denna policy med angivande av ansvarsförhållanden för genomförande och uppföljning. Verksamhetsområdeschefer ansvarar för att informationssäkerhetsarbetet följs upp inom verksamhetsområdet. Samtliga anställda och berörda politiker ska genomgå Myndigheten för samhällsskydd och beredskaps ”Datorstödd informationssäkerhetsutbildning för användare” (DISA) vart tredje år. Samtliga medarbetare ansvarar för att känna till och följa gällande riktlinjer och instruktioner. Den som upptäcker brister i informationssäkerhet måste uppmärksamma sin chef eller säkerhetssamordnaren/It-chef på det. Alla medarbetare måste också rapportera händelser som kan göra att våra informationstillgångar utsätts för risker.

Organisation

Säkerhetsgruppen planerar och följer upp arbetet med informationssäkerhet. Säkerhetsgruppen består av säkerhetssamordnaren, kommunens PUL-ansvarig, kommunikationsansvarig samt IT-chefen med säkerhetssamordnaren som sammankallande. Frågor som berör informationssäkerhet hanteras av IT-chefen.

Revidering och uppföljning

Varje år ska säkerhetsskyddschefen genomföra en intern säkerhetsrevision enligt internkontrollplanen.

Referenser

Terminologi för informationssäkerhet, SIS HB550 utgåva 3, SIS förlag
Strategi för samhällets informationssäkerhet 2010 - 2015, Myndigheten för samhällsskydd och beredskap (MSB)
Personuppgiftslagen (PUL), SFS 1998:204
Svensk standard för ledningssystem för informationssäkerhet SS-ISO/IEC 17799
Basnivå för informationssäkerhet (BITS), MSB
Säkerhetslagen, SFS 1996:627.