2022-03-21
Fastställd: Kommunfullmäktige 2022-05-05, § 49

Gäller för: Samtliga nämnder
Dokumentansvarig:
Informationssäkerhetssamordnare

Dnr : **KS2022/63-5**

Policy för informationssäkerhet och dataskydd

Innehållsförteckning

1. Inledning

Denna policy innehåller Bollebygd kommuns viljeinriktning och övergripande principer gällande informationssäkerhetsarbetet och personuppgiftshanteringen i kommunen. Alla verksamheter inom Bollebygd kommun omfattas av denna policy.

Denna policy konkretiseras i styrdokumentet. Riktlinjer för informationssäkerhet och dataskydd. Förvaltningarna har till ansvar att arbeta fram egna rutiner för hur informationssäkerhets- och dataskyddsarbetet ska se ut.

1.1 Syfte

Syftet med denna policy är att säkerställa att rätt och riktig information ska nå rätt mottagare i rätt tid och vara skyddad för obehörig åtkomst och förstörelse.

2. Bakgrund

Det finns information som hanteras i alla kommunens verksamheter. Den information som kommunen hanterar, är i relation till kommuninvånare, företag och organisationer såväl som inom den egna organisationen ska vara korrekt, och utgör en grund för tillit och förtroende. Det är viktigt att information i alla externa och interna relationer och kontakter är tillgänglig när det behövs och att information skyddas vid behov för att kommunen ska kunna fullgöra sitt uppdrag i samhället.

Informationssäkerhet handlar om att skapa och bevara rutiner och skydd av information utifrån fyra aspekter:

- Konfidentialitet: att information inte tillgängliggörs eller avslöjas till obehörig.
- Riktighet: att information är korrekt, aktuell och fullständig.
- Tillgänglighet: åtkomlighet för behörig person vid rätt tillfälle.
- Spårbarhet: härledning av utförda aktiviteter till en identifierad användare.

Information kan vara text, ljud, bild, film, tal med mera som hanteras med stöd av IT, papper eller direkt av människor. Hantering av information kan vara insamling, registrering, organisering, strukturering, lagring, bearbetning eller ändring, framtagning, läsning, användning, utlämning genom överföring, spridning eller tillhandahållande på annat sätt, justering eller sammanförande, begränsning, radering eller förstöring. Informationssäkerhet handlar således om administrativ säkerhet såväl som IT-säkerhet. Ägaren av en viss typ av informationstillgång kallas informationsägare.

Att arbeta med informationssäkerhet höjer värdet på våra tjänster och den service vi erbjuder. Ett korrekt och säkert arbetssätt ökar förtroendet och tilliten till organisationen. Ett tryggat och säkert arbetssätt och en hög medvetenhet ger högre kvalité och bättre förutsättningar för att lösa arbetsuppgifter på bästa sätt.

2.1 Om personuppgiftshantering

I många avseenden förekommer även personuppgifter i information som hanteras. Personuppgifter står under särskilt skydd och råder under särskilda bestämmelser enligt Dataskyddsförordningen, GDPR samt nationell kompletterande lag; Dataskyddslag. För personuppgifter gäller således särskilda regler för hantering. Inom ramen för informationssäkerhet är det viktigt att identifiera personuppgifter som särskilt skyddsvärda samt ändamålsenligt hanterade.

2.2 Principer

Policyn ska vara styrande, stödjande och kontrollerande. Innehållet ska hjälpa till i arbetet med att identifiera hot, sårbarhet, risker och integrera risk- och sårbarhetsanalyser för våra behandlingar. Vidare möjliggöra processer för att genomföra åtgärder som minskar hot, sårbarheter och risker till acceptabel nivå.

Arbete med informationssäkerhet och personuppgifter i Bollebygds kommun ska:

- Vara systematisk och grundas på gällande standardserier och att skapa ett ledningssystem för informationssäkerhet och dataskydd (LISD).
- Löpande ses över och utvecklas då omvärld och hot ständigt förändras.
- Vara förebyggande och ha en förmåga att hantera säkerhets- och personuppgiftsincidenter, störningar, och eventuella kriser.
- Vara kommunicerad till verksamheten, medarbetarna och förtroendevalda ska vara medvetna, utbildade, få information för att nå och upprätthålla högt säkerhetsmedvetande, riktig hantering av personuppgifter och leva upp till denna policy samt underliggande styrdokument för informationssäkerhet.
- Innebära säker och tillförlitlig informations- och personuppgiftshantering.
- Efterleva krav i lagar, förordningar, föreskrifter och avtal.
- Höja kvalitet, effektivitet, och stärka den personliga integriteten.
- Följa och samverka med omgivande samhället: Myndigheter, företag och nätverk. Särskilt normgivande aktörer inom informationssäkerhet såsom Sveriges kommuner och regioner (SKR), Myndigheten för samhällsskydd och beredskap (MSB) och Swedish Institute for Standards (SIS).

Med det möter kommunen förväntan och ställer krav på kommunens interna processer, IT-system och informationshantering. Organisationen ska säkerställa en säker personuppgiftshantering, ett kommande e-arkiv och tillhandahållandet av öppen data. Kommunen ska medverka i det digitala samhället och den digitala utvecklingen.

2.3 Arbetssätt

Bollebygd kommuns informationssäkerhetsarbete ska vara långsiktigt och ständigt pågående. Till grund för arbetet är den svenska och internationella standardserierna ISO 27000. Ledningssystem för informationssäkerhet och dataskydd, (LISD). Med stöd av LISD får kommunen rätt nivå på informationssäkerheten samtidigt som dess anställda får ett stöd i sitt dagliga arbete.

Arbetet ska omfatta alla delar av kommunens verksamhet och gälla de informationstillgångar som kommunen äger och/eller hanterar.

2.4 Uppföljning

Efterlevnaden av informationssäkerhetspolicy, riktlinjer för informationssäkerhet och riktlinjer för personuppgiftshantering ska regelbundet följas upp. Informationssäkerhetssamordnare ska rapportera läge och status gällande informationssäkerhet till kommunstyrelsen, rapporteringen ska ske en gång per år. Om särskilda skäl finns, som exempelvis allvarliga incidenter, brister eller behov, ska det motivera ytterligare rapporteringar.

3. Roller och ansvar

Kommunfullmäktige är ytterst ansvarig för informationssäkerhets- och dataskyddsarbetet och uttrycker sin viljeinriktning i denna policy. Kommunstyrelsen ansvarar för att samordna och följa upp kommunens informationssäkerhets- och dataskyddsarbete. Kommunstyrelsen har det övergripande ansvaret för att utarbeta, förvalta och följa upp riktlinjer för informationssäkerhet och dataskydd.

Nämnder med förvaltning ansvarar för informationsägarskapet inom ramen för sina verksamheter. Informationsägaren har det yttersta ansvaret för sin information och avgör vilken information som får hanteras, hur den ska hanteras och av vem den får hanteras. Dataskyddsförordningens stadgar pekar ut att ansvaret är knutet till den som är personuppgiftsansvarig. Det innebär att det är kommunens nämnder som själva har det yttersta ansvaret för att personuppgiftsbehandlingar i varje enskilt fall utförs i enlighet med förordningens regler och principer.

Policyn för informationssäkerhet och dataskydd gäller för alla informationstillgångar och personuppgiftsbehandlingar i alla verksamheter inom kommunen. Policyn gäller för samtliga aktörer som kan komma att hantera kommunens information och personuppgifter.

De som hanterar information och personuppgifter ska ha kunskap om det regelverk som gäller för hur informationen och personuppgifterna får hanteras och har själva ett ansvar för att informationssäkerheten och dataskyddet upprätthålls. Vid upptäckt av incident eller brister ska incidentrapportering ske enligt rutin.