STYRDOKUMENT
POLICY
2021-10-20
DNR: 2021-000166

Antagen av Kommunfullmäktige 25 januari 2022 § 9
Gäller från och med den 1 februari 2022 och tillsvidare

Policy för informationssäkerhet och personuppgiftshantering

Laholms kommunfullmäktige
Postadress: 312 80 Laholm. Besöksadress: Humlegången 6
Växel: 0430-150 00. www.laholm.se

Inledning

Denna policy innehåller Laholms kommuns viljeriktning och grundläggande synsätt på en övergripande nivå gällande arbetet för informationssäkerhet i organisationen.

Policy för informationssäkerhet och personuppgiftshantering gäller för alla verksamheter i kommunen, inklusive kommunala bolag. Det är inte tillåtet att besluta om lokala regler som inte följer denna policy.

Kommunstyrelsen är ansvarig för att hålla dokumentet aktuellt.

Informationssäkerhet

Laholms kommuns förvaltningar hanterar dagligen information och är beroende av att informationen är tillförlitlig. Informationssäkerhet handlar om att skapa och upprätthålla rutiner och skydd av informationstillgångar så att informationen:

- är tillgänglig när den behövs.
- är korrekt och inte manipulerad eller förstörd.
- endast är tillgänglig för behöriga personer att ta del av.

Ett systematiskt arbete med informationssäkerhet höjer värdet på tjänster och service. Det är grundläggande att informationen som kommunen handskas med är riktig för att kommuninvånare, näringsliv och andra organisationer skall känna förtroende och tillit.

Med rätt nivå av informationssäkerhet uppnås hög kvalitet och god effektivitet i det dagliga arbetet. Det är därför viktigt att kommunens informationstillgångar identifieras och klassificeras utifrån konfidentiell karaktär, riktighet, spårbarhet och tillgänglighet.

Informationstillgångar

Med informationstillgångar avses all information oavsett vilken form eller miljö den förekommer i. Information kan vara text, bilder, ljud, film och samtal som kommuniceras muntligen, i digital form eller som finns lagrad på kommunens olika digitala ytor. Information kan även vara fysiskt utskrivna dokument och anteckningar på papper.

Information kan hanteras genom insamling, organisering, strukturering, registrering, lagring, ändring eller bearbetning, framtagning, läsning, användning, justering eller presentation, begränsning, radering eller förstöring. Den kan även lämnas ut genom överföring och spridning eller leverans på annat sätt.

Policyn för informationssäkerhet och personuppgiftsbehandling gäller för all hantering av informationstillgångar i Laholms kommun oberoende av om den hanteras analogt eller digitalt med system eller programvara, automatiskt eller manuellt och oberoende av dess form eller vilken miljö den förekommer i.

Personuppgiftshantering

Personuppgifter förekommer ofta i information som hanteras. Personuppgifter har ett särskilt skydd och råder under särskilda bestämmelser enligt EUs Dataskyddsförordning samt nationell lag med kompletterande bestämmelser, Dataskyddslagen samt andra registerförfattningar.

För personuppgifter gäller därför särskilda regler för hantering. Inom ramen för informationssäkerhet är det viktigt att identifiera personuppgifter som särskilt skyddsvärda samt ändamålsenligt hanterade.

Principer

Policyn ska stödja arbetet med att identifiera hot, sårbarhet, risker och upprättande av risk- och sårbarhetsanalyser för kommunens behandlingar av information. Dessutom ska policyn möjliggöra processer för att genomföra åtgärder som minskar hot, sårbarhet och risker till acceptabel nivå.

Arbetet med informationssäkerhet och personuppgifter i Laholms kommun ska:

- vara systematiskt och bygga på den svenska och internationella standarden ISO 27000 (ledningssystem för informationssäkerhet, LIS) med mål att skapa ledningssystem för informationssäkerhet.
- löpande ses över och utvecklas då omvärld och hot är under ständig förändring.
- vara förebyggande och utveckla förmågan att hantera säkerhetsincidenter och personuppgiftsincidenter, störningar, och eventuella kriser. I det arbetet ingår att klassa information.
- vara kommunicerat till verksamheten. Personal ska vara medvetna, utbildade och få nödvändig information för att nå och upprätthålla hög säkerhetsmedvetenhet, hantera personuppgifter korrekt och leva upp till denna policy för informationssäkerhet och personuppgiftshantering.
- följa och samverka med omgivande myndigheter, nätverk, särskilt normgivande aktörer inom informationssäkerhet såsom Sveriges kommuner och Regioner (SKR), Myndigheten för samhällsskydd och beredskap (MSB) och Swedish institute of standardization (SIS).

Roller och ansvar

Ansvaret för informationssäkerhet och personuppgiftshantering följer verksamhetsansvaret. Detta innebär att den som är ansvarig för en viss verksamhet även ansvarar för informationssäkerheten och personuppgifter inom verksamhetsområdet.

Kommunstyrelsen

Kommunstyrelsen har det övergripande ansvaret för informationssäkerhetsarbetet. I detta ligger ett ansvar för att upprätta en organisation kring informationssäkerhet som fungerar som stöd till kommunens förvaltningar för att uppfylla informationssäkerhetsansvaret och ett korrekt hanterande av personuppgifter. Kommunstyrelsen har även ansvaret för att nämndsövergripande reglementen, instruktioner och anvisningar upprättas.

Nämnder

Nämnderna har det yttersta ansvaret för informationssäkerheten inom respektive verksamhetsområde och är även ytterst ansvarig vid incidenter i nämnden. Nämnderna ansvarar för att anta riktlinjer för informationssäkerhet.

Förvaltningschefen

Inom en nämnds verksamhetsområde ansvarar förvaltningschef eller motsvarande för att konkreta regler och anvisningar är utformade så att en anpassad säkerhet för informationen kan upprätthållas. I detta ansvar ligger att vederbörande ska tillse att kunskapen om dessa sprids i organisationen.

Uppföljning

Kommunfullmäktige ska, minst en gång per mandatperiod pröva om styrdokumentet är aktuellt. Om styrdokumentet inte är aktuellt ska det upphävas, revideras eller sammanföras med annat styrdokument vid behov.