Lekebergs kommun

Datum:
2025-10-30

Fastställd av:
Kommunfullmäktige

Ansvarig för revidering:
Kommunstyrelsen

Ansvarig tjänsteperson:
Säkerhetschef

Granskad:

Diarienummer:
KS 25-620

Policy för informationssäkerhet

Lekebergs kommun

Policy
Program
Plan
Riktlinje
Regler

Innehållsförteckning

Inledning

Policyn beskriver de övergripande principer som ska gälla för informationssäkerhetsarbetet i Lekebergs kommun. Informationssäkerhetspolicyn gäller för hantering av all information, i alla dess former i kommunen inklusive bolag och för de som arbetar på uppdrag av kommunen. Det sistnämnda ska regleras genom avtal.

Lekebergs kommuns informationssäkerhetsarbete utgår ifrån ISO/IEC 27000 och organisationens verksamhetskrav samt gällande författningar. Informationssäkerhetsarbetet består av styrande dokument som utgörs av denna policy med tillhörande riktlinjer och eventuella rutiner samt tillämpningsanvisningar.

Arbetet med informationssäkerhet ska vara långsiktigt, systematiskt och kontinuerligt.

Denna policy gäller för hela Lekebergs kommun med dess majoritetsägda bolag; alla anställda, förtroendevalda och andra som har behörighet att använda kommunens information.

Begreppsförklaring

Informationstillgångar: Allt som innehåller information samt allt och alla som bär på information. T ex mobiltelefoner, verksamhetssystem och medarbetare.

Informationssäkerhet: Är den säkerhet som omfattar våra informationstillgångar och förmågan att upprätthålla önskad konfidentialitet, riktighet och tillgänglighet.

Konfidentiell: Information som inte får nås eller avslöjas för någon obehörig. Oftast gäller det innehållet in en informationstillgång men ibland är även tillgångens existens hemlig.

Riktighet: Innebär att informationen inte får ändras av obehöriga, inte av misstag och inte på grund av en funktionsstörning.

Tillgänglighet: Innebär att informationen går att nyttjas av behörig användare när det behövs och så mycket det behövs.

Spårbarhet: Aktiviteter ska kunna härledas i efterhand. Vem som har utfört aktiviteten, vad som har skett samt var aktiviteten har utförts. I möjlig mån ska det även kunna spåras hur aktivitetens utfördes.

Verksamhetssystem: I vissa fall även kallat informationssystem, är de system som insamlar, lagrar, bearbetar eller distribuerar och presenterar information.

Syfte och mål

Syftet med informationssäkerhetspolicyn är att beskriva hur kommunen ska uppnå en god informationssäkerhet.

Kommunens informationssäkerhetsarbete ska skydda informationen inom verksamheten mot yttre och inre hot. Skyddet ska vara anpassat till skyddsvärdet, risk och lagkrav och därigenom möjliggöra för kommunens verksamheter att

uppnå sina mål. Följande mål är styrande för informationssäkerheten i kommunen:

Säker och riskbaserad informationshantering: Informationstillgångar klassificeras och riskbedöms samt hanteras utifrån dess skyddsbehov, så att den är riktig och tillgänglig när den behövs och skyddas mot obehörig åtkomst. Det för att värna verksamhetens förmåga att utföra sitt uppdrag och skydda individer mot skada men lika viktigt är att värna integriteten för medborgarna. Medborgarna ska känna trygghet i hur kommunen omhändertar deras intressen avseende integritet och säkerhet i behandlingen av dennes uppgifter.

God informationssäkerhetskultur: Behovet av skydd av information bedöms och är en central del i arbetet på alla nivåer i verksamheten utifrån de risker och hot som finns mot informationen och medarbetare är medvetna om sitt ansvar som användare.

Effektiv incidenthantering: Kommunen har förmåga att hindra, hantera och lära av allvarliga informationssäkerhetsincidenter.

Robust informationshantering: Verksamheterna, IT och IT-infrastrukturen är riskbedömda och har planerat för vilka åtgärder som ska vidtas vid avbrott, störningar och kriser.

Handlingsplan: Informationssäkerhetsaspekter ska beaktas i handlingsplaner och verksamhetsplaner.

Verksamhetsanknytning: informationssäkerhetsarbetet ska så långt de går inkluderas i befintliga processer och rutiner.

Ansvar och organisation

Kommunfullmäktige fastställer den informationssäkerhetspolicy som ska gälla för Lekebergs kommun.

Kommunstyrelsen ansvarar för att kommunens informationssäkerhetspolicy och riktlinjer för informationssäkerhet utarbetas och hålls aktuella. Lekebergs säkerhetschef leder, samordnar och följer upp kommunens informationssäkerhetsarbete.

Kommunstyrelsen ansvarar också för samordningen av informationssäkerhetsarbetet i kommunen.

Varje nämnd och bolagsstyrelse är utifrån denna policy ansvarig för informationssäkerheten inom sitt verksamhetsområde. Nämnd eller bolagsstyrelse ska anta verksamhetsspecifika styrdokument för informationssäkerhet där detta bedöms som nödvändigt.

Alla medarbetare har ett ansvar för att säkerheten fungerar genom att följa uppställda säkerhetsregler. Det samma gäller även när tillfällig personal eller extern aktör/ uppdragstagare anlitas. Den som upptäcker brister i informationssäkerheten ska snarast uppmärksamma sin närmaste chef. Alla

medarbetare ska kunna rapportera händelser som kan göra att informationstillgångar utsätts för risker.

Arbetssätt och skyddsåtgärder

Kommunens verksamheter ska arbeta systematiskt med informationssäkerhet och följa ISO 27001 standarden.

Kommunens verksamheter ska arbeta med att identifiera informationstillgångar och dess flöden. Informationstillgångarna ska klassificeras.

Alla informationstillgångar ska ha en ägare. Informationsägaren ansvarar för klassificeringen och ställer de säkerhetskrav som behövs för att nå önskad säkerhet.

Verksamheterna ska omvärldsbevaka och genomföra riskanalyser vid införandet av nya verksamhetssystem och vid förändringar. Vid behov ska verksamheterna vidta nödvändiga åtgärder för att se till att informationstillgångarna har rätt skydd, vidare ska verksamheterna följa upp och dokumentera incidenter och vidtagna åtgärder kring dessa.

Kommunen ska ställa krav på informationssäkerhet vid upphandling, utveckling, användning och avveckling av verksamhetssystem. De krav som ställts ska även följas upp. Relevanta säkerhetskrav ska gälla vid såväl intern som extern drift av verksamhetssystem. Viss säkerhetsklassad information kan kräva säkerhetsskyddad upphandling (SUA).

Verksamheterna ska arbeta med kontinuitetsplanering och ha beredskap för avbrott, påfrestande situationer. Detta gäller även när externa aktörer för informationshantering anlitas. Samhällsviktiga verksamheter ska kunna upprätthållas på acceptabel nivå vid olika typer av störningar och krissituationer. Det är viktigt att alla har ett högt säkerhetsmedvetande och kritiskt ifrågasätter händelser som kan påverka informationssäkerheten.

Ansvariga enligt detta dokument ska följa upp att beslutade åtgärder är genomförda, att uppsatta mål är uppfyllda, att regler och riktlinjer följs samt att styrdokument vid behov revideras.

Uppföljning och revidering

Informationssäkerhetspolicyn ska revideras vid varje ny mandatperiod eller vid behov. I samband med revideringen ska tillhörande riktlinjer och tillämpningsanvisningar revideras på motsvarande sätt.