Haninge kommun

2015-04-20

Kommunstyrelseförvaltningen

Bo Jensen
Säkerhetsstrateg

Policy - Informationssäkerhet

Denna policy innehåller Haninge kommuns viljeinriktning och övergripande mål för informationssäkerhetsarbetet. Samtliga nämnder och deras verksamheter omfattas av denna informationssäkerhetspolicy. Policyn konkretiseras i tillhörande riktlinjer.
Policy för informationssäkerhet utgår från Haninge kommuns Program för säkerhet och riskhanteringsarbete (KF 27/2011) och kompletterar övriga styrdokument inom dokumenthantering, IT-säkerhet och kommunikation.

Bakgrund

Behovet av informationssäkerhet ökar i takt med att kommuninvånarna förväntar sig effektiv kommunikation, dels via självbetjäning med hjälp av olika e-tjänster och dels i sin direktkontakt med kommunen. I allt större utsträckning sker också i förvaltningarna användning och utveckling av systemstöd för att leverera tjänster på ett effektivt sätt. Invånarna ska kunna förvänta sig att kommunen hanterar information som rör dem, exempelvis personuppgifter och information om de olika tjänster de använder, på ett säkert sätt. I samband med kriser krävs också effektiv och säker kommunikation med berörda verksamheter och invånare.
Konsekvensen av bristande informationssäkerhet kan medföra störningar i samhällsviktiga verksamheter, att information går förlorad, förvanskas eller rent av stjäls. Det kan även medföra ekonomiska förluster och att förtroendet för eller varumärket Haninge kommun påverkas negativt.

Dokumenttyp	Dokumentnamn	Fastställd/Datum	Gäller från datum
Policy	Informationssäkerhet	xxxx-xx-xx	xxxx-xx-xx
Beslutat av	Ansvarig avdelning och dokumentförvaltare (namn)	Reviderad	
KS	Kommunstyrelseförvaltningen/kansliet		
Dokumentinformation		Diarienr	Version
Nyupprättad.		KS xx/xxxx	1.0

Informationssäkerhet

Informationssäkerhet omfattar hela kommunens verksamhet och all information utan undantag. Oavsett den hanteras i cyberrymden, i datorer, i ett telefonsamtal eller på ett papper. Då stora delar av informationen hanteras med hjälp av IT-system handlar informationssäkerhet även om teknik.

Med informationssäkerhet säkerställs följande:

- *Riktighet* – Att information inte kan förändras av obehöriga, av misstag eller på grund av störningar i funktion/system. Informationen ska vara tillförlitlig, korrekt och fullständig
- *Sekretess* – Att information i dokument, system och handlingar etc. med lagkrav om sekretess eller motsvarande inte görs tillgängliga eller avslöjas för obehörig
- *Spårbarhet* – Att i efterhand kunna härleda specifika aktiviteter eller händelser till ett identifierat objekt ex. handling, användare, dator, skrivare eller system/program
- *Tillgänglighet* – Att information är tillgänglig i skälig och förväntad utsträckning och inom rimlig tid

Övergripande målsättning

En god informationssäkerhet syftar till att säkra en effektiv informationsförsörjning och att undgå fel som påverkar möjligheterna att bedriva en ändamålsenlig verksamhet.
Arbetet med informationssäkerhet ska vara systematiskt och långsiktigt.
Genom att säkerställa en god nivå av systematiskt informationssäkerhetsarbete möjliggörs att lagkrav följs, kritisk verksamhet upprätthålls, informationsläckage förhindras, kontroll av kostnader uppnås, förtroendet för kommunens tjänster och varumärke skyddas.

Strategiska målområden

- Informationsförsörjningen ska vara säker, effektiv och bidra till stöd åt verksamheterna
- Informationssäkerhetsarbetet sker enhetligt och systematiskt
- Kommunövergripande rutiner, regler och anvisningar ska upprättas
- Samtliga informationstillgångar ska vara identifierade och förtecknade. Av förteckning ska framgå vem som är informations/system ägare och förvaltare
- Genom klassificering värdera och prioritera informationstillgångar utifrån verksamhetens krav på riktighet, sekretess, spårbarhet och tillgänglighet
- Personal ska ha kunskap om gällande informationssäkerhetsregler som rör det egna tjänstestället och de informationssystem/rutiner som där används
- Händelser i informationssystemen som kan leda till negativa konsekvenser för kommunens åtaganden ska identifieras, åtgärdas och förebyggas
- I syfte att ha förmåga att bedriva verksamheten på acceptabel nivå både under normala förhållanden och vid kriser eller störningar ska kontinuitetsplanering genomföras för varje informationstillgång baserad på omfattning av informationens samlade krav
- Informationssäkerhetsarbetet ska minst följa standarderna ISO/IEC 27001 och ISO/IEC 27002. Myndigheten för samhällsskydd och beredskaps metoder och vägledningar tillämpas

Ansvar och roller

Kommunstyrelsen
Kommunstyrelsen har det övergripande ansvaret för att informationssäkerhetsarbetet kan utföras systematiskt och att utförandet sker enhetligt i samtliga nämnder. Det innebär att kommunstyrelsen leder, samordnar och utvecklar kommungemensamma arbetssätt utifrån de strategiska målområdena.
Kommundirektör
På kommunstyrelseförvaltningen utser kommundirektören enhet/funktion för det samordnade uppdraget och i övrigt stödjer förvaltningen utifrån kommunstyrelsens ansvar.
Kommunstyrelseförvaltningen
Kommunstyrelseförvaltningen verkställer kommunstyrelsens uppdrag genom framtagande av regler och anvisningar. Upprättar rutiner för säkerhetsanalys av system i drift och vid nyanskaffning samt uppföljning av efterlevnad av regler och anvisningar. Stödjer systemägare och systemförvaltare i deras utförande av uppgift.

Nämnd
Som informationsägare har nämnd ett ekonomiskt, funktionellt och säkerhetsmässigt ansvar för sina informationssystem. Respektive nämnd ansvarar för att informationssäkerhetsarbetet sker på ett ändamålsenligt sätt enligt kommunstyrelsens anvisningar.
Förvaltningschef
Inom respektive verksamhetsområde ansvarar förvaltningschef för att systemägare utses för respektive informationssystem och i övrigt stödjer det egna informationssäkerhetsarbetet utifrån nämndens ansvar.
Systemägare
Systemägare har övergripande ansvar för respektive system och dess användning.
Systemförvaltare
Systemförvaltare har det funktionella ansvaret för ett system. Systemförvaltare är systemägarens utförare som ser till att systemets funktionalitet upprätthålls och planerade aktiviteter upprätthålls samt att utbildning av användare genomförs.

Medarbetare
Medarbetare är skyldiga att följa upprättade regler och anvisningar i sin arbetsutövning. Brister i informationssäkerheten ska omedelbart rapporteras till närmast överordnad chef.

Uppföljning

Policyn och ingående strategiska målområden är giltig tills vidare. Uppföljning och ev. revidering ska göras minst vart fjärde år. Uppföljning/revidering syftar till att:

- Utvärdera genomfört arbete enligt de strategiska målområdena
- Utvärdera efterlevnad av myndighetskrav och standarder
- Utvärdera hur regler och anvisningar följs och är ett stöd för verksamheterna
- Utvärdera behov av fortsatt samordning och utveckling