SURAHAMMARS KOMMUN

SURAHAMMARS KommunalTeknik AB VATTEN—MILJÖ

Surahammarshus AB
Trygghet i boendet
www.surahus.se

POLICY FÖR INFORMATIONSSÄKERHET

Gäller för samtliga nämnder och styrelser

Revideras vid inaktualitet

Antagen av kommunfullmäktige: 2022-12-05, KF § 98
Ansvarig handläggare: Elin Bergerin, Digitaliseringsutvecklare

SURAHAMMARS KOMMUN

Innehåll

SURAHAMMARS KOMMUN

Syfte

Informationssäkerhetspolicyn är ett övergripande dokument som redovisar Surahammars kommuns övergripande mål och inriktning med informationssäkerhet samt hur ansvaret i dessa frågor är fördelat.

Om informationssäkerhet

Information finns i alla kommunens verksamheter och handlar om allt det vi gör, exempelvis om vår personal, våra tjänster, vår ekonomi och det omgivande samhället med medborgare, företag, föreningar osv. Information är därför i sig en av kommunens viktigaste tillgångar. För att skapa tillit och förtroende och för att nå en hög kvalitet i vårt arbete måste information hanteras på rätt sätt. Informationssäkerhet handlar om att skapa och upprätthålla lämpliga rutiner och skydd av information utifrån tre aspekter:

- **Konfidentialitet:** att informationen är tillgänglig endast för de personer som har behörighet att ta del av den
- **Riktighet:** att innehållet i informationen ska var korrekt och inte kunna förändras av obehöriga
- **Tillgänglighet:** att information är nåbar när den behövs

Informationssäkerhet begränsas inte till säkerhet i IT-system utan omfattar information i alla dess former och oavsett hur information lagras, bearbetas och kommuniceras. Information kan t ex vara i form av text, ljud, bilder och film, och kan hanteras med stöd av IT, papper eller direkt av oss människor i form av tal.

Mål med informationssäkerhet

Informationssäkerhet har inget egenvärde, utan ska bidra till att Surahammars kommun når sina övergripande visioner, strategier och mål samt efterlever lagar, förordningar, föreskrifter och avtal. Surahammars kommun ska uppnå och upprätthålla en informationssäkerhet som:

- Innebär en robust, säker och tillförlitlig informationshantering,
- Möjliggör och underlättar digital transformation och att den sker med tillräcklig säkerhet,
- Bidrar till att uppsatta mål nås gällande exempelvis kvalitet, effektivitet och personlig integritet,
- I möjligaste mån motsvarar medborgares och externa verksamheters behov och förväntningar

Principer och arbetssätt

För att uppnå uppsatta mål med informationssäkerheten ska arbete gentemot kommunens verksamheter vara normerande, stödjande och kontrollerande.

Arbetet med informationssäkerhet inom Surahammars kommun ska:

- Bygga på en helhetssyn som utgår ifrån information, men som också innefattar processer, människor och teknik,
- Vara systematiskt och bygga på den etablerade standardserien ISO 27000,
- Löpande ses över och förbättras eftersom omvärld och hot är under ständig förändring,
- Vara förebyggande, men också ha en god förmåga att hantera incidenter, allvarliga störningar och kriser som ändå kan inträffa,
- Vara väl kommunicerat till verksamheten; all personal bör fortlöpande få information och utbildning för att uppnå och upprätthålla ett högt säkerhetsmedvetande, med syfte att ha en korrekt informationshantering,
- Ske i aktiv samverkan med det omgivande samhället såsom myndigheter, företag och nätverk, särskilt som är normgivande inom informationssäkerhet som t ex SKR (Sveriges kommuner och regioner), MSB (Myndigheten för samhällsskydd och beredskap) och SIS (Swedish Standards Institutet).

Verksamhetsdriven informationssäkerhet genom informationsklassning

Surahammars kommun ska tillämpa en enhetlig modell för informationsklassning som anger olika nivåer av skyddskrav och ska baseras på interna och externa krav på informationens konfidentialitet, riktighet och tillgänglighet.

Genom att klassa information kan verksamheterna identifiera känslig och kritisk information och säkerställa att denna får tillräckligt skydd, men ibland också för att undvika att information får onödigt överskydd.

Ansvar och organisation

Ansvaret för informationssäkerhet följer det ordinarie verksamhetsansvaret. Detta gäller från kommunledning till enskild medarbetare, och innebär att den som är ansvarig för en viss verksamhet också är ansvarig för informationssäkerheten inom verksamhetsområdet. Kommunens informationssäkerhetssamordnare och övriga som arbetar specifikt med informationssäkerhet, IT-säkerhet eller andra relaterade frågor, fungerar som stöd till kommunens verksamheter att fullfölja informationssäkerhetsansvaret.

Nedan beskrivs informationssäkerhetsansvaret för ett antal roller.

Kommunfullmäktige uttrycker sin viljeriktning rörande kommunens arbete med denna policy.

Kommunstyrelsen ansvarar för att samordna och följa upp kommunens informationssäkerhetsarbete. Kommunstyrelsen har det övergripande ansvaret för att utarbeta, förvalta och följ upp policy för informationssäkerhet.

Nämnderna/styrelserna Varje enskild nämnd ansvarar för den information och de informationssystem som finns inom det egna verksamhetsområdet och är ytterst ansvarig för informationssäkerheten inom sitt verksamhetsområde.

Medarbetare, förtroendevalda, elever och uppdragstagare ansvarar för att följa de styrdokument och eventuellt verksamhetsspecifika regler gällande informationssäkerhet som finns samt agera säkerhetsmedvetet.

Kommunchef har det övergripande ansvaret för informationssäkerheten och att det finns en tydlig ansvarsfördelning för att upprätthålla säkerheten.

Informationsägare är den som bestämmer ändamål och medel för behandlingen och hanteringen av informationen. Ansvaret för respektive informationstillgång följer verksamhetsansvaret. Informationsägaren avgör vilken information som får hanteras, hur den hanteras och av vem.

Systemägare /Objektägare har ansvaret för information i system, vanligtvis förvaltningschef. Ansvarar för beslut om vidareutveckling och avveckling av system.

Förvaltningsledare/Systemförvaltare har det funktionella (dagliga) helhetsansvaret för ett system/objekt. Förvaltaren fungerar i hög grad som system/- objektägarens utförare och ser till att systemets/objektets funktionalitet samt planerade och beslutade aktiviteter genomförs och upprätthålls.

Säkerhetsskyddschef ansvarar för informationssäkerheten i verksamheten som har betydelse för Sveriges säkerhet och lyder under säkerhetsskyddslagen.

Krisberedskapssamordnare genomför säkerhetsanalyser på uppdrag av säkerhetsskyddschefen.

Dataskyddsombudet övervakar att dataskyddsförordningen efterföljs inom organisationen genom att utföra kontroller och informationsinsatser.

Informationssäkerhetssamordnare har det övergripande ansvaret att leda, utveckla och samordna arbetet med informationssäkerhet i kommunen. Stödfunktion för ledning och verksamheter.

IT-chef har det operativa ansvaret för att uppfylla de krav som verksamheten ställer på den tekniska IT-infrastrukturen. IT-chefen eller motsvarande har ett särskilt ansvar för den tekniska IT-säkerheten.

SURAHAMMARS KOMMUN

Uppföljning och rapportering

Efterlevnaden av informationssäkerhetspolicy och styrdokument gällande informationssäkerhet ska följas upp regelbundet.

Informationssäkerhetssamordnare ska årligen rapportera läge och status gällande informationssäkerhet till kommunchef och kommunstyrelse. Särskilda skäl, som exempelvis allvarliga incidenter, brister eller behov, kan motivera ytterligare rapporteringar.