ALINGSÅS KOMMUN

Informationssäkerhetspolicy i Alingsås kommun

Antagen av kommunfullmäktige den 11 december 2019, § 237

Inledning

Alingsås kommun har en säkerhetspolicy och riktlinjer och organisation för säkerhets- och beredskapsarbete i Alingsås kommun. Policyn och riktlinjerna beskriver målsättningar för det beredskaps- och säkerhetsarbete som ska bedrivas inom Alingsås kommun. Informationssäkerhet utgör en del av detta arbete. Denna policy innehåller Alingsås kommuns viljeinriktning och övergripande principer gällande informationssäkerhetsarbetet i kommunen.

Omfattning

Alla verksamheter inom Alingsås kommun omfattas av denna policy inklusive de kommunala bolagen och räddningstjänstförbundet.
Det är inte tillåtet att besluta om lokala regler som avviker från denna policy.

Denna policy kompletteras med *Riktlinjer för Informationssäkerhet i Alingsås kommun* och *Handlingsplan för informationssäkerhet i Alingsås kommun.*

Om informationssäkerhet

Information finns och hanteras i alla kommunens verksamheter. Att information som kommunen hanterar i relationer med kommuninvånare, företag och organisationer såväl som inom vår egen organisation är korrekt, utgör en grund för tillit och förtroende. Det är viktigt att information i alla externa och interna

kontakter är tillgänglig när det behövs och att information skyddas vid behov för att vi ska kunna fullgöra vårt uppdrag i samhället.

Informationssäkerhet handlar om att skapa och upprätthålla lämpligt skydd av information. Detta innefattar information i alla dess former; text, ljud, bild, film osv. och oavsett hur information lagras, bearbetas och kommuniceras. Det kan vara med stöd av IT, dokument eller direkt av oss människor i form av tal. Informationssäkerhet begränsas inte till säkerhet i IT-system utan omfattar information i alla dess former och oberoende hur information lagras, bearbetas och kommuniceras.

Arbetet med informationssäkerhet går ut på att skydda och bevara den information Alingsås kommun har att ta ansvar för utifrån fyra aspekter:

- Tillgänglighet - Tillgänglig för dem som behöver och har rätt att ta del av den.
- Riktighet - Tillförlitlig och inte förvanskad.
- Konfidentialitet - Skyddad från obehörig åtkomst.
- Spårbarhet - Att i efterhand kunna härleda specifika aktiviteter eller händelser till ett identifierat objekt ex. handling, användare, dator, skrivare eller system/program.

Mål med informationssäkerhetsarbetet

Informationssäkerhetens syfte är att medverka till att uppfylla kommunens mål och strategier samt efterleva lagar, förordningar, föreskrifter och avtal.
Alingsås kommun ska uppnå och upprätthålla informationssäkerhet som:

- innebär en robust, säker och tillförlitlig informationshantering.
- i möjligaste mån motsvarar medborgares och externa verksamheters behov och förväntningar.
- möjliggör och underlättar digitalisering och att den sker med tillräcklig säkerhet.

- möjliggör att samtliga kritiska informationstillgångar informationsklassas.

Principer och arbetssätt

För att uppnå uppsatta mål med informationssäkerheten ska arbetet gentemot kommunens verksamheter vara normerande, stödjande och kontrollerande. Arbetet med informationssäkerhet i kommunen ska:

- vara systematiskt och bygga på den vedertagna standardserien ISO/IEC 27000 med strävan att ett ledningssystem för informationssäkerhet integreras i kommunens styrning.
- vara förebyggande och ha en förmåga att hantera informationssäkerhetsincidenter, störningar, och eventuella kriser.
- vara väl kommunicerat i verksamheten där medarbetare genom utbildning och information får en säkerhetsmedvetenhet med syfte att ha en korrekt informationshantering.
- löpande ses över och utvecklas då omvärld och hot är under ständig förändring.
- följa och samverka med omgivande samhället: Myndigheter, företag och nätverk. Särskilt normgivande aktörer inom informationssäkerhet såsom Sveriges kommuner och landsting (SKL) och Myndigheten för samhällsskydd och beredskap (MSB).

Informationsklassning

Alingsås kommun ska använda sig av en enhetlig modell för informationsklassning. Informationsklassning innebär att verksamheter klassar sina informationstillgångar utifrån interna och externa krav på konfidentialitet, riktighet och tillgänglighet. Genom att klassa information kan verksamheter 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 ordinarie verksamhetsansvar. 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 informationssäkerhetsansvar för ett antal roller. Ansvar och tillhörande ansvarsområden för respektive roller beskrivs utförligare i riktlinjer för informationssäkerhet.

Kommunfullmäktige - fastställer den informationssäkerhetspolicy som ska gälla för kommunen.

Kommunstyrelsen - ansvarar för att kommunens informationssäkerhetspolicy följs och för samordning av informationssäkerhetsarbetet i kommunen. Kommunstyrelsen ansvarar för att riktlinjer för informationssäkerhet utarbetas och hålls aktuella. Kommunstyrelsen ska årligen fastställa en övergripande handlingsplan för informationssäkerhetsarbetet.

Nämnder - är ytterst ansvarig för informationssäkerhet inom sitt verksamhetsområde.

Kommundirektör - har kommunstyrelsens uppdrag att sörja för att informationssäkerhetsarbetet bedrivs så effektivt som möjligt och ansvarar för att övergripande tillämpningsanvisningar utarbetas och hålls aktuella i enlighet med policy och riktlinjer.

Säkerhetschef - har det övergripande ansvaret att leda, utveckla och samordna Alingsås kommun säkerhetsarbete.

Informationssäkerhetssamordnare - har det övergripande ansvaret att leda, utveckla och samordna informationssäkerhetsarbetet.

Informationssäkerhetssamordnare ska arbeta i samråd med säkerhetschefen och övriga ledamöter i kommunens informationssäkerhetsråd.

IT-säkerhetssamordnare - har det övergripande ansvaret att säkerställa säkerheten i Alingsås kommuns IT-miljö och är stödjande vid kravställning på externa aktörer. Ingår i kommunens informationssäkerhetsråd.

Systemägare - är ansvarig för information i system, vanligtvis förvaltningschef. Ansvarar för beslut om vidareutveckling och avveckling av system.

Systemförvaltare – har det funktionella och dagliga ansvaret för system. Systemförvaltare fungerar i hög grad som systemägarens utförare och ser till systemets funktionalitet samt planerade/beslutade aktiviteter genomförs och upprätthålls.

Informationsägare – äger information inom sitt verksamhetsområde och ansvara för informationens kvalitet samt att hanteringen uppfyller krav på informationssäkerhet.

Medarbetare - alla medarbetare inom verksamheten har ett ansvar för verksamhetens informationssäkerhet. Varje anställd ska i eget arbete följa riktlinjer för informationssäkerhet samt eventuella verksamhetsspecifika regler.

Kommunjurist - har det övergripande ansvaret att leda, utveckla och samordna arbetet med hantering av personuppgifter. Ingår i kommunens informationssäkerhetsråd.

Dataskyddsombud – ansvarar för att informera och ge råd till den personuppgiftsansvariga organisationen kring vilka skyldigheter som gäller enligt dataskyddsförordningen. Ombudet ska också bevaka att reglerna följs och fungera som kontaktperson för Datainspektionen.

Informationssäkerhetsråd - i detta forum sker kommunens samordning och uppföljning av informationssäkerhetsarbetet och informationssäkerhetssamordnaren är sammankallande. Representanter för

kommunens olika verksamheter samt säkerhetschefen ska ingå och rådet ska sammanträda regelbundet.

Uppföljning

Efterlevnaden av informationssäkerhetspolicy och underliggande styrdokument ska regelbundet följas upp. Informationssäkerhetssamordnare ska löpande rapportera läge och status gällande informationssäkerhet till säkerhetschef. Säkerhetschef sammanställer årligen en rapport till kommunstyrelsen.
Om särskilda skäl finns, som exempelvis allvarliga incidenter, brister eller behov, ska det motivera ytterligare rapporteringar. Vid behov granskas informationssäkerhetsarbetet av oberoende part.