Policy för informations-säkerhet och dataskydd

Alingsås kommun

Typ av styrdokument: Policy
Beslutande instans: Kommunfullmäktige
Datum för beslut: ÅÅÅ-MM-DD
Diarienummer: 2024.230 KS

Gäller för: Kommunkoncernövergripande
Giltighetstid: Tillsvidare
Revideras senast: Vid behov
Dokumentansvarig:
Informationssäkerhetsansvarig

Innehåll

1. 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 och dataskydd utgör en del av detta arbete. Denna policy innehåller Alingsås kommuns viljeinriktning och övergripande principer gällande arbetet med informationssäkerhet och dataskydd i kommunen.

2. Omfattning

Alla verksamheter inom Alingsås kommun omfattas av denna policy. Efter antagande av respektive bolag och förbund gäller denna policy även för 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 och dataskydd i Alingsås kommun.

3. Om informationssäkerhet

Information finns och hanteras i alla kommunens verksamheter. Det är viktigt att information i alla externa och interna relationer och kontakter är tillgänglig när det behövs, att information går att lita på 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 tre 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.

Cybersäkerhet avser skyddet av datorer, servrar, nätverk, programvara och data från skador, angrepp eller obehörig åtkomst. Det handlar om att skydda information och system från olika typer av hot, inklusive cyberattacker, dataintrång, virus och andra skadliga aktiviteter. Cybersäkerhet omfattar normalt sett flera aspekter:

- Skydd av information
- Nätverkssäkerhet
- Applikationssäkerhet
- Endpoint-säkerhet
- Incidenthantering
- Utbildning och medvetenhet
- Regelverk och efterlevnad
-

Cybersäkerhet är avgörande för att skydda både information i en alltmer digitaliserad värld, där cyberhot blir allt mer sofistikerade och vanliga.

4. Om dataskydd

Dataskydd handlar om att skydda individers personuppgifter och därmed deras integritet. Dataskyddsarbetet i Alingsås kommun baseras på reglerna i EU:s dataskyddsförordning (GDPR). Alla verksamheter måste följa dataskyddsreglerna vid behandling av personuppgifter. Det innebär bland annat att följa de grundläggande principerna, se till att behandlingen av personuppgifter som görs har en rättslig grund samt informera de registrerade om hur deras personuppgifter hanteras av verksamheten.

5. Målsättningen med informationssäkerhets- och dataskyddsarbetet

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

- innebär en robust, transparent, 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.
- skydda personuppgifter.

6. Principer och arbetssätt

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

7. Ansvar och organisation

Ansvaret för informationssäkerhet och dataskydd 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 informationssäkerhet och dataskydd inom verksamhetsområdet. Kommunens informationssäkerhetsansvarige och övriga som arbetar specifikt med informationssäkerhet, IT-säkerhet eller andra relaterade frågor, fungerar som stöd till kommunens verksamheter att fullfölja informationssäkerhets- och dataskyddsansvaret.

Nedan beskrivs informationssäkerhets- och dataskyddsansvar för ett antal roller.

Kommunfullmäktige - fastställer den policy för informationssäkerhet och dataskydd som ska gälla för kommunen.

Kommunstyrelsen - ansvarar för att kommunens policy för informationssäkerhet och dataskydd följs och för samordning av arbetet i kommunen samt att riktlinjer för informationssäkerhet utarbetas och hålls aktuella. Kommunstyrelsen ska årligen fastställa en övergripande handlingsplan för informationssäkerhets- och dataskyddsarbetet.

Nämnder - är ytterst ansvarig för informationssäkerhet och dataskydd inom sitt verksamhetsområde.

Kommundirektör - har kommunstyrelsens uppdrag att säkerställa för att arbetet 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.

Informationssäkerhetsansvarig (CISO) - har det övergripande ansvaret att leda, utveckla och samordna informationssäkerhetsarbetet.

Informationssäkerhetsansvarig ansvarar för följande:

- att kommunens styrande dokument inom området är aktuella
- att utveckla och förvalta metoder, vägledningar och annat stödmaterial inom informationssäkerhetsområdet
- kompetensförsörjning och att öka informationssäkerhetsmedvetandet inom kommunen, t.ex. genom rådgivning och utbildning
- att stödja verksamheterna i frågor som rör informationssäkerhet
- kontroll och uppföljning av informationssäkerheten i kommunen
- omvärldsbevakning inom informationssäkerhetsområdet
- administrerar SKR:s KLASSA-verktyg
- Rapporterar läge och status gällande informationssäkerhet till kommunstyrelsen en gång per år. Oftare om särskilda skäl finns som exempelvis allvarliga incidenter, brister eller behov
- Sammankallar och leder tillsammans med IT-säkerhetsansvarig och dataskyddsansvarig kommunens nätverk för informationssäkerhet och dataskydd.

IT-säkerhetsansvarig - har det övergripande ansvaret att säkerställa säkerheten i Alingsås kommuns IT-miljö och är stödjande vid kravställning på externa aktörer. Sammankallar och leder tillsammans med informationssäkerhetsansvarig och dataskyddsansvarig kommunens nätverk för informationssäkerhet och dataskydd.

IT-säkerhetsansvarig ansvarar på en övergripande nivå att:

- Identifiera, bedöma och hantera risker relaterade till IT-system och data.
- Utveckla och implementera riktlinjer som inkluderar regler för användning av IT-resurser samt tillhörande IT-incidenthantering
- Implementera tekniska lösningar för att skydda system och data, såsom brandväggar, antivirusprogram, kryptering och intrångsdetekteringssystem.
- Övervaka IT-system för att upptäcka och reagera på säkerhetsincidenter.
- Säkerställa att organisationen följer relevanta lagar, förordningar och standarder för IT-säkerhet. Genomföra regelbundna revisioner och kontroller för att bedöma säkerhetsåtgärdernas effektivitet.
- Implementera rutiner för säkerhetskopiering av data och återställning av system efter en incident eller katastrof.
- Hantera och kontrollera åtkomst till IT-resurser och information, inklusive autentisering och behörighetskontroller.

Dataskyddsansvarig– har det övergripande ansvaret att leda, utveckla och samordna arbetet med hantering av personuppgifter. Sammankallar och leder tillsammans med informationssäkerhetsansvarig och IT-säkerhetsansvarig kommunens nätverk för informationssäkerhet och dataskydd.

Dataskyddsansvarig ansvarar för:

- att kommunens styrande dokument inom området är aktuella
- att utveckla och förvalta metoder, vägledningar och annat stödmaterial inom dataskyddsområdet
- kompetensförsörjning och att öka medvetandet gällande dataskydd inom kommunen, t.ex. genom rådgivning och utbildning
- att stödja verksamheterna i frågor som rör dataskydd
- kontroll och uppföljning av dataskydd i kommunen
- omvärldsbevakning inom dataskyddsområdet

Nätverk för informationssäkerhet och dataskydd –samtliga förvaltningar, bolag och förbund är representerade i nätverket. Nätverket träffas fyra gånger per år. Nätverket syftar till erfarenhetsutbyte, ökad kompetens, gemensamt lärande samt genomförande av kommunstyrelsens årliga handlingsplan för informationssäkerhet och dataskydd.

Lokal samordnare för informationssäkerhet och dataskydd – ansvarar för att leda och samordna arbetet med informationssäkerhet och dataskydd i sin verksamhet. Vidare ansvarar lokal samordnare för att genomföra årliga aktiviteter i enlighet med Alingsås kommuns ledningssystem för informationssäkerhet. Utgör representant i kommunens nätverk för informationssäkerhet och dataskydd.

Lokal samordnare för informationssäkerhet och dataskydd ansvarar för att:

- Leda genomförandet av verksamhets- och riskanalys för egen verksamhet
- Leda genomförande av informationsklassningar för egen verksamhet
- Vara verksamhetens administratör för informationsklassningsverktyget KLASSA
- Verksamhetens behandlingsregister hålls uppdaterat.
- Leda genomförandet av konsekvensbedömning om dataskydd om så behövs.
- Stötta egen verksamhet vid hantering av incidenter.
- Bidra med information för kontroll och uppföljning av informationssäkerhet inom egen verksamhet.
- Ansvarar för framtagandet och uppföljning av lokal handlingsplan för informationssäkerhet och dataskydd.

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

Systemförvaltare – 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 ansvarar 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.

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 Integritetsskyddsmyndigheten (IMY). Alingsås kommun har del av dataskyddsombud via Göteborgsregionens kommunalförbund (GR).

8. Uppföljning

Efterlevnaden av denna policy och underliggande styrdokument ska regelbundet följas upp. Årligen följs arbetet med informationssäkerhet och dataskydd upp genom ledningens genomgång som redovisas i kommunstyrelsen. Lokalt arbete följs upp av respektive ledning. Informationssäkerhetsansvarig ska löpande rapportera läge och status gällande informationssäkerhet till säkerhetschef. Om särskilda skäl finns, som exempelvis allvarliga incidenter, brister eller behov, ska det motivera ytterligare rapporteringar. Vid behov granskas informationssäkerhetsarbetet av oberoende part.