Handlingsplan Informationssäkerhet och Dataskydd i Alingsås kommun 2022

Typ av styrdokument: Handlingsplan
Beslutande instans: Kommunstyrelsen
Datum för beslut: ÅÅÅÅ-MM-DD
Diarienummer: 2021.612 KS

Gäller för: Kommunövergripande
Giltighetstid: 2022-12-31
Revideras senast: 2022-12-15
Dokumentansvarig: Informationssäkerhetssamordnare

ALINGSÅS KOMMUN

Inledning
Alingsås kommun kommuns Informationssäkerhetspolicy innehåller kommunens långsiktiga övergripande mål (3-5 år) och inriktning med informationssäkerhet. Dessa mål är:

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.

Handlingsplan för informationssäkerhet 2022 kompletterar informationssäkerhetspolicyn och innehåller kortsiktiga mål (1 år) med tillhörande aktiviteter för att uppnå fullmäktiges långsiktiga målsättningar. Av policyn framgår att kommunstyrelsen årligen ska fastställa en handlingsplan för informationssäkerhetsarbetet.

Till denna handlingsplan adderas även arbetet med dataskydd. Detta arbete syftar till att de personuppgifter som kommunen hanterar ska behandlas i enlighet med dataskyddslagstiftningen. Informationssäkerhetsarbetet och dataskyddsarbetet bör samordnas då ett gott informationssäkerhetsarbete är en förutsättning för att följa dataskyddslagstiftningen.

Informationssäkerhetssamordnare, IT-säkerhetssamordnare och dataskyddsansvarig leder arbetet och verkställer tillsammans med kommunens verksamheter innehållet i denna handlingsplan.

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.

Om dataskydd

Sverige lyder under EU:s dataskyddsförordning, även förkortad GDPR. Ändamålet med dataskyddslagstiftningen är att erbjuda ett starkt skydd för fysiska personers uppgifter, vilket ytterst är en integritetsfråga. Kommunfullmäktige har i Policy för behandling av personuppgifter i Alingsås kommun fastställt vilka grunder som gäller för behandling av personuppgifter för att säkerställa att denna sker i enlighet med dataskyddsförordningen.

Grundläggande begrepp

En *personuppgift* är all slags information som kan hänföras till en fysisk person som är i livet. Det kan till exempel vara namn, adress, personnummer eller bild.

Med *behandling av personuppgifter* menas allt som görs när vi hanterar uppgifter om en person. Kommunen utför en rad olika uppgifter som kräver att personuppgifter behandlas. Till exempel behöver personuppgifter behandlas inom skolverksamhet, äldreomsorg och andra av kommunens verksamhetsområden. Kommunen behandlar personuppgifter inom varje nämnds verksamhetsområden baserat på de rättsliga grunderna allmänintresse, rättslig förpliktelse och myndighetsutövning men även baserat på avtal eller samtycke.

Respektive nämnd och styrelsen är *personuppgiftsansvarig* för de behandlingar som görs inom dess verksamhetsområde.

Grundläggande principer

Den som behandlar dina personuppgifter måste ta hänsyn till de *grundläggande principerna* i dataskyddsförordningen. Principerna gäller för all behandling och kan sägas vara kärnan i dataskyddsförordnigen.

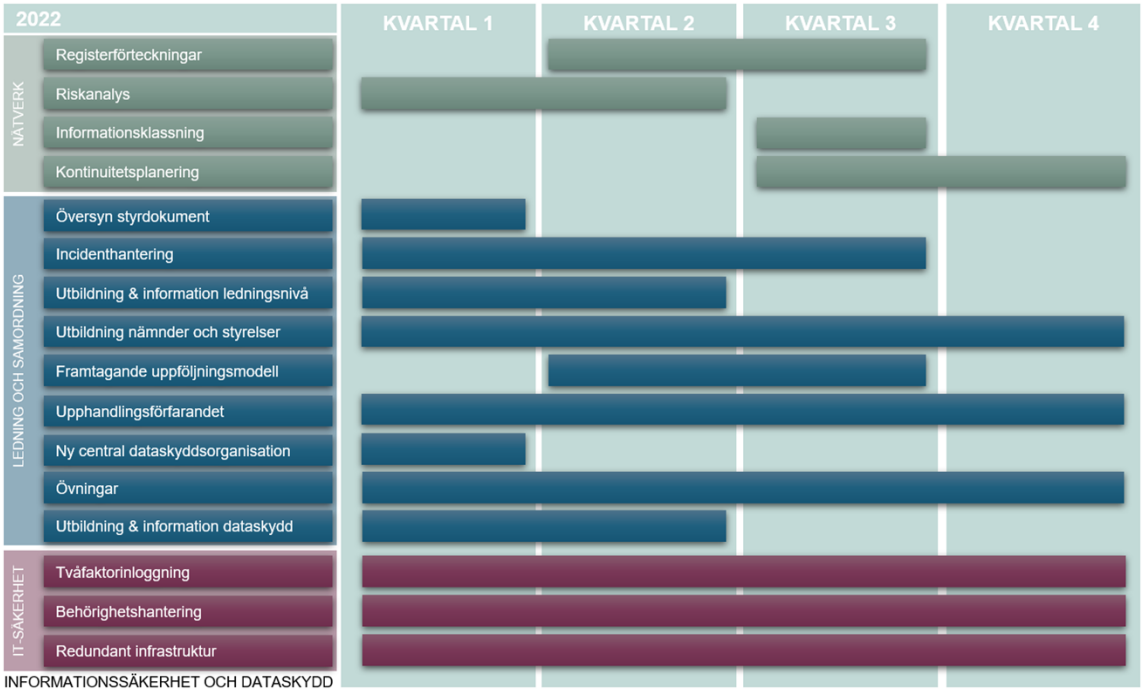
Principerna innebär bland annat att den personuppgiftsansvariga styrelsen/nämnden:

- bara får samla in personuppgifter för specifika, särskilt angivna och berättigade ändamål
- inte ska behandla fler personuppgifter än vad som behövs för ändamålen
- ska se till att personuppgifterna är riktiga
- ska radera dina personuppgifter när de inte längre behövs
- ska skydda dina personuppgifter, till exempel så att inte obehöriga får tillgång till dem och så att de inte förloras eller förstörs.

Förutsättningar

Genomförandet av handlingsplanen genererar inga direkta kostnader för verksamheten annat än resurser i form av arbetade timmar. Över tid kan utkomsten av genomfört arbete generera beslut kring säkerhetsåtgärder som innebär kostnader.

Handlingsplan 2022



Nätverk

Riskanalys
Verksamheter fortsätter bedriva analysarbete över sin information, arbetet bedrivs genom nätverk för informationssäkerhet och dataskydd. Analyser som per verksamhet ska genomföras under 2022 är riskanalys.

Informationsklassning
Varje verksamhet ska klassificera minst ett verksamhetskritiskt system eller manuell informationstillgång. Arbetet bedrivs genom nätverk för informationssäkerhet.

Kontinuitetsplanering
Kontinuitetshantering handlar om att planera för att upprätthålla sin verksamhet på en tolerabel, det vill säga för organisationen acceptabel, nivå oavsett vilken störning den utsätts för. Varje verksamhet ska upprätta en kontinuitetsplan för en informationstillgång.

Registerförteckningar
Registerförteckningarna togs ursprungligen fram 2018 i samband med ikraftträdandet av dataskyddsförordningen. Med anledning av rättsutvecklingen på området behöver respektive personuppgiftsansvarig revidera sin registerförteckning, med ledning och stöd från den centrala dataskyddsorganisationen. Korrekta, systematiska och uppdaterade registerförteckningar ligger sedan till grund för det fortsatta dataskyddsarbetet.

Ledning och samordning

Genomföra utbildnings- och informationsinsatser på ledningsnivå
Utbildning och information till ledningsgrupper gällande informationssäkerhet, dataskydd och Alingsås kommuns interna styrdokument för området.

Genomföra utbildnings- och informationsinsatser för nämnder och styrelser
Utbildning och information till nämnder och styrelser gällande informationssäkerhet, dataskydd och Alingsås kommunens interna styrdokument för området.

Ny central dataskyddsorganisation
Upprättande av ny dataskyddsorganisation inom kommunledningskontoret. Organisationens syfte är att vara kommunens centrala dataskyddssamordnare inom områdena registerförteckningar, personuppgiftsbiträdesavtal, tredjelandsöverföringar, personuppgiftsincidenter samt styrning och ledning. Organisationen ska stötta och lämna rådgivning till övriga förvaltningar inom dataskyddsområdet.

Genomföra utbildnings- och informationsinsatser för dataskyddsorganisationen
Utbildning av medarbetare med funktion i ny central dataskyddsorganisation.
Utbildning av medarbetare med funktion i den kommunövergripande dataskyddsorganisationen.

Översyn styrdokument
Befintliga styrdokument inom informationssäkerhetsområdet ska under 2022 genomgå en översyn och eventuell revidering.

Utvecklande av incidenthanteringsprocess
För att framgångsrikt minska konsekvenserna av incidenter behöver organisationen ha arbetssätt för att hantera alla situationer som avviker från det normala. Utvecklandet av en incidenthanteringsprocess för informationssäkerhet bör, så långt det är möjligt, inbegripas i befintliga incidenthanteringsprocesser.

Utveckla uppföljningsmodell
Genom övervakning, mätning och måluppföljning erhålls uppgifter som stödjer utvärdering av ifall informationssäkerheten och dataskydd i stort är ändamålsenligt utformad, har avsedd verkan, samt att säkerhetsåtgärder existerar och fungerar tillfredsställande. Utvecklandet av en uppföljningsmodell för informationssäkerhet och dataskydd bör, så långt det är möjligt, inbegripas i befintliga uppföljningsprocesser.

Utveckla upphandlingsförfarandet
Ett fördjupat samarbete med upphandlingsenheten med syftet att än bättre inbegripa frågor om dataskydd, informationssäkerhet och övrig säkerhet i upphandlingsprocessen. Regelbundna träffar för diskussion och uppföljning av metoder och tillvägagångssätt.

Övningar
För att bättre kunna möta de antagonistiska hot som finns behöver verksamheten testa och öva att valda säkerhetsåtgärder fungerar på ett tillfredställande vis. Ett exempel kan vara att genomföra penetrationstester mot valda delar av vår IT-miljö. Övningar inom informationssäkerhet, IT-säkerhet och dataskydd bör, så långt det är möjligt, inbegripas i kommunens övergripande övningsplan.

IT-säkerhet

Tvåfaktorsinlogg
Tvåfaktorsautentisering innebär ett extra krav utöver lösenord som visar på att en individ verkligen är den individen. Att använda sig av tvåfaktorautentisering ökar säkerheten på användarkonton och risken för att bli utsatt för exempelvis phisning och ID-kapning minskar. Under året ska tvåfaktorsinloggning införas på utvalda delar av IT-miljön.

Behörighetshantering
Rätt person ska komma åt de delar av ett system/verktyg som behövs för att kunna genomföra sitt uppdrag, varken mer eller mindre behörigheter ska ges. Ett verksamhetssystem ska väljas ut och utgöra en pilot för införande av behörighanteringssystem.

Systemredundans
För att säkerställa tillgängligheten av den information som Alingsås kommun har inom sin ägo ska systemredundans säkerställas. Detta innebär uppbyggnad av parallell IT-miljö på lämplig plats.