Handlingsplan informationssäkerhet och dataskydd i Alingsås kommun 2023

Typ av styrdokument: Handlingsplan
Beslutande instans: Kommunstyrelsen
Datum för beslut: 2023-xx-xx § x
Diarienummer: **xx**KS

Gäller för: Kommunövergripande
Giltighetstid: 2023-12-31
Revideras senast: 2023-12-15
Dokumentansvarig: Informationssäkerhetsansvarig

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.

Alingsås kommuns ska följa lagstiftning gällande hantering av personuppgifter och arbetet med att uppnå regelefterlevnad sammanfattas som dataskydd.

Handlingsplan för informationssäkerhet & dataskydd 2023 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.

Informationssäkerhets- och dataskyddsarbetet är samordnat för effektivare resursanvändning då områdena i många delar tangerar varandra.

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

Om informationssäkerhet

Informationssäkerhet handlar om att hindra information från att läcka ut, förvanskas och förstöras. Det handlar också om att rätt information ska finnas tillgänglig för rätt personer, och i rätt tid. Information ska inte kunna hamna i orätta händer och missbrukas.

Alingsås kommuns arbete med informationssäkerhet är uppbyggt utifrån MSB:s metodsstöd för systematiskt informationssäkerhetsarbete. Metodstödet består av fyra olika metodsteg som tillsammans bildar helheten av det systematiska informationssäkerhetsarbetet och utgör ett årshjul. Till årshjulet har även arbetet med dataskydd lagts till.

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 principer

Den som behandlar 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.

Ansvar

Ansvaret för informationssäkerhet följer ordinarie verksamhetsansvar och respektive nämnd och styrelse är personuppgiftsansvarig för de behandlingar som görs inom dess verksamhetsområde.

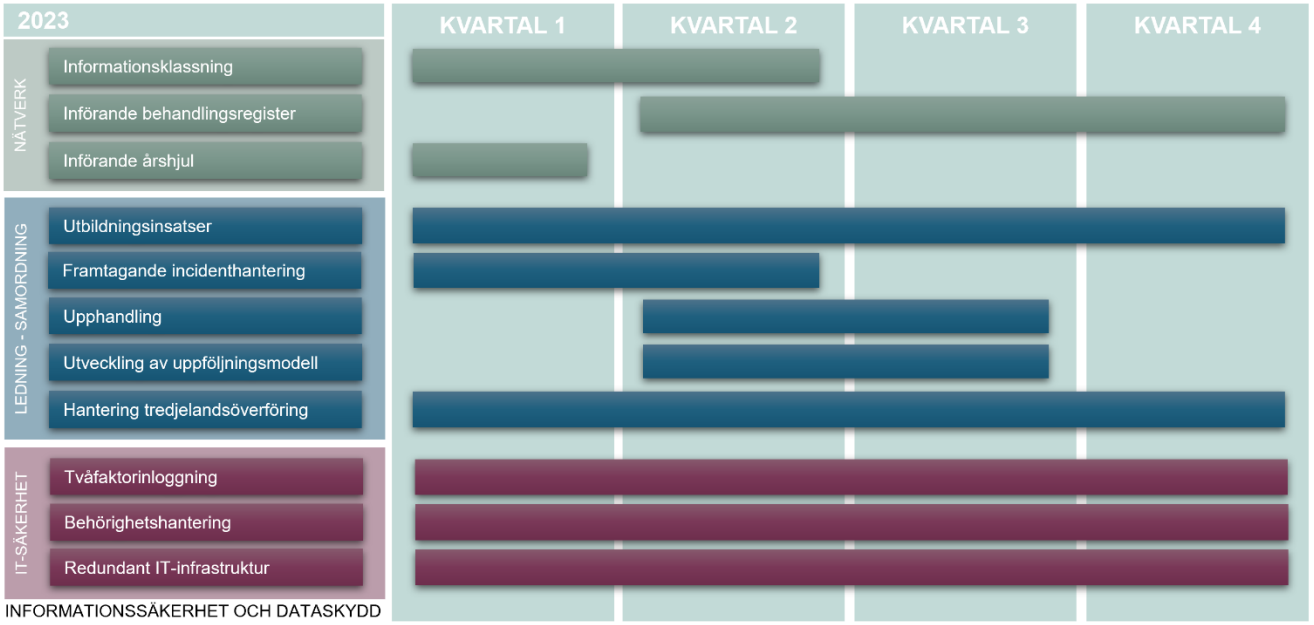
Förutsättningar

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.

Rapport informationssäkerhet och dataskydd 2023 - Ledningens genomgång

Alingsås kommun följer upp sitt informationssäkerhet- och dataskyddsarbete årligen, resultatet återfinns i dokumentet *Rapport informationssäkerhet & dataskydd 2023 – Ledningens genomgång.* Uppföljningen består av flera olika delar, exempelvis intern och extern revision mätningar av olika slag. Brister och svagheter identifieras och sedan görs dessa till aktiviteter i denna handlingsplan.

Handlingsplan 2023



Nätverk

Informationsklassning

Att klassificera information och därigenom utarbeta lämpligt skydd av information är en viktig del i ett systematiskt informationssäkerhetsarbete.
Varje verksamhet ska klassificera minst ett verksamhetskritiskt system eller manuell informationstillgång. Arbetet bedrivs genom nätverk för informationssäkerhet.

Övergång från registerförteckningar till behandlingsregister

Varje personuppgiftsansvarig ska ha ett register över de personuppgiftsbehandlingar som sker inom dennes verksamhet. Ett stort arbete kommer att bedrivas under 2023 för att byta sätt som denna information redovisas. Sedan registerförteckningarna ursprungligen togs fram 2018 har ett perspektivskifte skett angående hur informationen i förteckningarna ska kategoriseras och redovisas. Perspektivskiftet innebär att all information om respektive personuppgiftsbehandling knyts till själva behandlingen istället som idag till vilket system som behandlingen sker i. Kommunens dataskyddsombud har lämnat rekommendation om att genomföra en sådan övergång från registerförteckningar till behandlingsregister.

Under 2023 ska kommunledningskontorets dataskyddsorganisation tillsammans med IT-avdelningen förbereda för en övergång från nuvarande redovisning i separata textfiler till att informationen återfinns i ett specialbyggt verksamhetssystem.

När det första arbetet är gjort från kommunledningskontoret sida och verksamhetssystemet är igång kommer respektive personuppgiftsansvarig behöva överföra den information som idag återfinns i registerförteckningarna till det nya systemet. Kommunledningskontoret kommer att stötta förvaltningarna i detta arbete, bl.a. genom workshops.

När informationen från dagens registerförteckningar återfinns i verksamhetssystemet kommer den att vara sökbar på ett helt nytt sätt, göra det möjligt att sammanställa information samt dra nytta av annan information som också finns i systemet. Förändringen kommer också att göra att ansvariga för informationen endast kommer att behöva uppdatera förändrad information på ett ställe, istället för som idag på ett flertal platser.

Årshjul

Flera genomförda aktiviteter under 2021 och 2022 har varit att komma igång med olika

metoder som ingår i ett systematiskt informationssäkerhetsarbete. Dessa aktiviteter kommer framöver återfinnas i ett årshjul och genomföras på regelbunden basis, det som skapar systematik i arbetet. Årshjulet ska under 2023 implementeras i kommunen.

Ledning och samordning

Övergripande kompetenshöjning inom informationssäkerhet och dataskydd – flera utbildningsinsatser
Alingsås kommun behöver fortsätta och utveckla arbetet med att ge alla som verkar i organisationen höjd kunskap inom områdena informationssäkerhet och dataskydd.
Under 2023 ska mätning av medarbetares kunskaper före och efter genomförda utbildningar genomföras för att se om utbildningsinsatser har avsedd effekt. Vidare ska fler sätt för medarbetare att få till sig kunskap utvecklas.

Ta fram övergripande incidenthanteringsprocess
Alingsås kommun behöver utveckla sin förmåga att hantera incidenter, exempelvis en IT-attack. Incidenthanteringsarbetet handlar om att förbättra organisationens förmåga att minimera risken för att incidenter uppstår, minska incidenters konsekvenser, utreda orsakerna till incidenten och därigenom förbättra skyddet så att liknande incidenter inte inträffar i framtiden.
En kommungemensam incidenthanteringsmodell ska under 2023 tas fram och implementeras. Modellen ska, så långt det är möjligt, inbegripa olika typer av incidenter (exempelvis personuppgiftsincident, informationssäkerhetsincident osv).

Fördjupat samarbete kring upphandling
Under 2023 ska ett fördjupat samarbete med upphandlingsenheten påbörjas 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 och dokumentera arbetssätt.

Utveckling av kommunövergripande 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.
Under 2023 ska uppföljningsmodell fortsatt utvecklas och dokumenteras.

Strukturerat arbete gällande tredjelandsöverföringar
Som rättsläget ser ut idag är det inte tillåtet för personuppgiftsansvariga att låta de personuppgifter som denna ansvarar för behandlas i länder utanför EU som inte uppfyller en adekvat skyddsnivå. Flera stora tjänster som används inom kommunen innebär idag en otillåten överföring till, eller åtkomst från, tredjeland. Under 2023 ska kommunledningskontoret dataskyddsorganisation stötta respektive personuppgiftsansvarig i att ta fram en plan för hur dessa behandlingar ska avslutas samt en tidsplan för när det ska ske.

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.