Handlingsplan informationssäkerhet och dataskydd i Alingsås kommun 2024

Typ av styrdokument: Handlingsplan
Beslutande instans: Kommunstyrelsen
Datum för beslut: 2024-02-05 § 23
Diarienummer: 2023.554 KS

Gäller för: Kommunövergripande
Giltighetstid: 2024-12-31
Revideras senast: 2024-12-15
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 2024 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 säker informationshantering

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 informations- och personuppgiftsansvarig för de behandlingar som görs inom dess verksamhetsområde.

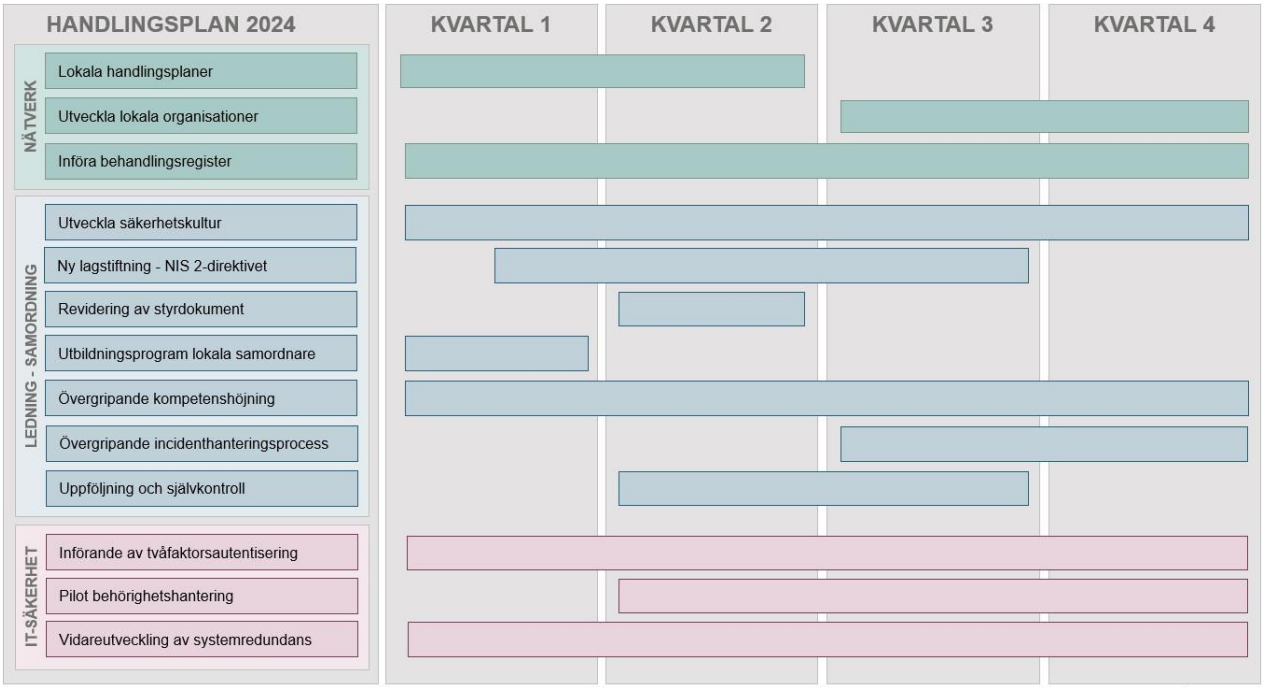
Förutsättningar

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 2024



Informationssäkerhet och dataskydd | Alingsås kommun

Nätverk

Lokal handlingsplan för informationssäkerhet och dataskydd

Som ett led i att möjliggöra det systematiska arbetet i nämnder och styrelser ska varje verksamhet under första delen av 2024 ta fram en lokal handlingsplan som anger fokusområden för verksamhetens arbete under året. Kommunkoncernens olika verksamheter har kommit olika långt i arbetet med informationssäkerhet och dataskydd och arbetet behöver anpassas till respektive verksamhets utgångspunkt och förutsättningar.

Utveckla lokal informationssäkerhets- och dataskyddsorganisation hos respektive verksamhet

För att få genomslag och framgång i arbetet med informationssäkerhet och dataskydd i verksamhet behöver en lokal organisation skapas där fler funktioner är involverade i arbetet. Den lokala organisationen leds av nätverksmedlemmarna. Hur organisationen formas hos respektive förvaltning bestäms av lokala behov och förutsättningar. Centrala stödfunktioner finns för rådgivning kring uppbyggnaden.

Införa behandlingsregister hos respektive personuppgiftsansvarig

Med hjälp av utvecklat systemstöd ska varje personuppgiftsansvarig under 2024 övergå från nuvarande registerförteckning till behandlingsregister. Centrala stödfunktioner kommer att ge information samt hålla workshops för att visa hur övergången ska ske och stötta i arbetet.

Ledning och samordning

Utveckla säkerhetskultur
Under 2024 ska aktiviteter genomföras för att främja säkerhetskulturen inom kommunorganisationen.

Ny lagstiftning - NIS 2-direktivet - Anpassning av ledningssystem och dess metoder för regelefterlevnad
Hösten 2024 väntas NIS 2-direktivet träda i kraft och ersätta nu gällande NIS-direktiv. Den nya lagstiftningen kommer träffa fler kommunala verksamheter och därtill ställa hårdare krav på bland annat incidentrapportering, ledningens styrning, striktare tillsynsåtgärder, sanktionsmöjligheter vid bristande efterlevnad m.m. Centrala stödfunktioner ska anpassa ledningssystem och dess metoder för att säkerställa regelefterlevnad. Därtill ska utbildning till berörda verksamheter genomföras.

Revidering av styrdokument
Befintliga styrdokument inom informationssäkerhet och dataskydd ska under 2024 revideras och aktualiseras. Därtill ska framtagande av rutinbeskrivningar för moment inom ledningssystemet ske.

Framtagande av utbildningsprogram för lokala samordnare för informationssäkerhet och dataskydd
Ett utbildningsprogram för lokala samordnare för informationssäkerhet och dataskydd ska tas fram och lanseras under 2024. Målgruppen har behov av utökad kunskap inom områdena för att kunna leda arbetet lokalt i sin verksamhet. Utbildningsprogrammet ska bestå av teori och praktiska moment.

Övergripande kompetenshöjning inom informationssäkerhet och dataskydd
Alingsås kommun behöver fortsätta och utveckla arbetet med att ge alla som verkar i organisationen höjd kunskap inom områdena informationssäkerhet och dataskydd. Fler sätt för medarbetare att få till sig kunskap ska utvecklas, däribland ska analog information tas fram för verksamheter som i liten utsträckning arbetar digitalt. Vidare ska metoder för mätning av kunskapsnivåer 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 2024 tas fram och implementeras. Modellen ska, så långt det är möjligt, inbegripa olika typer av incidenter (exempelvis personuppgiftsincident, informationssäkerhetsincident osv).

Utifrån utkomsten av arbetet med incidenthanteringsprocess ska verksamheter ges lämplig utbildning i vad en incident är och hur den ska rapporteras.

Utveckling av uppföljning och självkontroll
Det är av vikt att genomförda aktiviteter och säkerhetsåtgärder har den verkan som är avsedd. Uppföljning och självkontroll behöver utvecklas vidare för att möjliggöra slutsatser kring aktiviteters och säkerhetsåtgärders effekt.

IT-säkerhet

Påbörja införande av tvåfaktorsautentisering i verksamhet
Tvåfaktorsautentisering innebär ett extra krav utöver lösenord som visar på att en individ verkligen är den individen. Under 2024 ska vi identifiera relevanta verksamhetskritiska system och påbörja införande av tvåfaktorsinloggning för dem.

Genomföra pilot gällande 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. Lämpliga verksamhetssystem ska väljas ut och utgöra pilot för införande av behörighanteringssystem.

Vidareutveckling av systemredundans
För att säkerställa tillgängligheten av den information som Alingsås kommun har inom sin ägo ska systemredundans säkerställas. Under 2024 ska investering och införande av IT-infrastruktur ske, vilket ska säkerställa drift av de fem mest verksamhetskritiska funktionerna inom IT-miljön.