Handlingsplan informationssäkerhet och dataskydd i Alingsås kommun 2025–2026

Typ av styrdokument: Handlingsplan

Beslutande instans: Kommunstyrelsen

Datum för beslut: 2025-

Diarienummer: 2025.414 KS

Gäller för: Kommunövergripande

Giltighetstid: 2026-12-31

Revideras senast: 2026-12-15

Dokumentansvarig: Informationssäkerhetsansvarig

ALINGSÅS
KOMMUN

Inledning
Alingsås kommuns policy för informationssäkerhet och dataskydd innehåller kommunens långsiktiga övergripande mål (3–5 år) och inriktning. Dessa mål är:

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.
- skyddar personuppgifter

Handlingsplan för informationssäkerhet & dataskydd 2025–2026 kompletterar policyn 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 informationssäkerhets- och dataskyddsarbetet.

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 Myndigheten för samhällsskydd och beredskaps (MSB) metodstöd för systematiskt informationssäkerhetsarbete. Metodstödet består av fyra olika metodsteg som tillsammans bildar helheten av det systematiska informationssäkerhetsarbetet och utgör ett årshjul. Arbetet med dataskydd är inkluderat i årshjulet.

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.

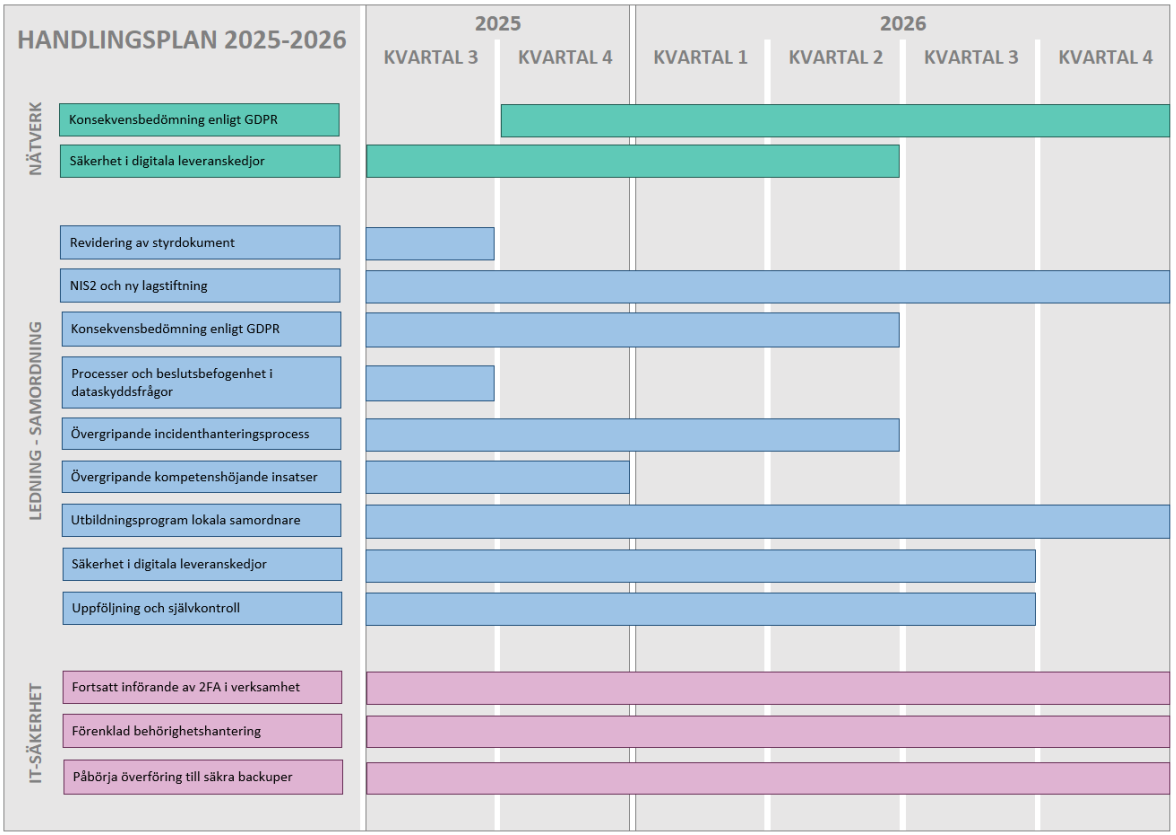
Ansvar
Ansvaret för informationssäkerhet följer ordinarie verksamhetsansvar. Varje nämnd och styrelse är personuppgiftsansvarig för de behandlingar av personuppgifter som utförs inom sitt verksamhetsområde.

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 2024 - Ledningens genomgång

Alingsås kommun genomför årligen en uppföljning av sitt arbete med informationssäkerhet- och dataskydd. Resultatet redovisas i dokumentet *Rapport informationssäkerhet & dataskydd 2024 – Ledningens genomgång.* Uppföljningen omfattar flera olika delar, såsom intern och extern revision samt olika typer av mätningar. Identifierade brister och svagheter omvandlas sedan till aktiviteter i denna handlingsplan.

Handlingsplan 2025 – 2026



Nätverk

Konsekvensbedömning enligt GDPR

Gör en bedömning av vilka personuppgiftsbehandlingar i behandlingsregistret som kräver en konsekvensbedömning och ta fram en prioriteringsordning och en tidsplan och för genomförande av konsekvensbedömningar. Det är en förutsättning att tidigare registerförteckning omarbetats till ett behandlingsregister innan detta arbete påbörjas.

Genomför minst 1-2 konsekvensbedömningar. Använd Integritetsskyddsmyndighetens (IMY) mall för bedömning om konsekvensbedömning ska göras samt mall för genomförande av konsekvensbedömning. Central organisation kommer att ge information samt erbjuda utbildning/workshop som stöd i arbetet.

Säkerhet i digitala leveranskedjor

Kraven på vår förmåga att säkerställa verksamhetens kontinuitet ökar på grund av växande hot, förändrade relationer mellan länder, skärpt lagstiftning inom området och det osäkra rättsläget gällande överföring av personuppgifter till USA. Säkerhet i digitala leveranskedjor handlar om att minimera risker i alla led för att kunna upprätthålla vår verksamhet.

- Genomför en inventering av beroenden till utländskt ägande för informationstillgångar/system som bedöms vara verksamhetskritiska för organisationens kärnverksamhet och uppdatera Verksamhetsanalys - informationstillgångar enligt ny mall. *Den insamlade informationen kommer att användas som underlag vid genomförande av Leveranskedjekollen (MSB) 2026.*

- Bedöm om det finns behov av att uppdatera verksamhetens riskanalys och kontinuitetsplan utifrån risker som kan komma att påverka säkerheten i kritiska leveranskedjor och verksamhetens kontinuitet. Exempel på potentiella risker är bristande kravställning gentemot aktuella leverantörer, beroenden och inlåsningseffekter som gör det svårt att byta leverantör samt risker kopplade till utländskt ägande.

Ledning och samordning

Revidering av styrdokument
Riktlinjer för informationssäkerhet ska under 2025 revideras och aktualiseras. Därtill ska framtagande av rutinbeskrivningar för moment inom ledningssystemet tas fram.

NIS2 och ny lagstiftning - Anpassning av ledningssystem och dess metoder för regelefterlevnad
Under 2025–2026 väntas NIS2 att implementeras genom en ny lag i Sverige. Den nya lagstiftningen kommer träffa fler kommunala verksamheter och därtill ställa hårdare krav på bland annat incidentrapportering, ledningens styrning, säkra leveranskedjor och kontinuitetshantering tillsammans med striktare tillsynsåtgärder och sanktionsmöjligheter vid bristande efterlevnad. Centrala stödfunktioner ska anpassa ledningssystem och dess metoder för att säkerställa regelefterlevnad. Därtill ska utbildning för berörda genomföras.

Konsekvensbedömning enligt GDPR
Ta fram en strategi för arbetet med konsekvensbedömningar samt utreda förutsättningar för att koppla konsekvensbedömningar till personuppgiftsbehandlingar i kommunens systemstöd för behandlingsregister. Tillhandahålla stöd till verksamheten i form av utbildningar/workshops avseende bedömning om en personuppgiftsbehandling innebär hög risk samt i arbetet med att genomföra konsekvensbedömningar.

Processer och beslutsbefogenhet i dataskyddsfrågor
En översyn av delegationsordningen och tillhörande rutiner kommer att genomföras för att säkerställa tydliga processer och beslutsmandat i dataskyddsfrågor.

Ta fram övergripande incidenthanteringsprocess
Alingsås kommun behöver utveckla sin förmåga att hantera incidenter, exempelvis en cyberattack. Arbetet handlar om att förbättra organisationens förmåga att minimera risken för att incidenter uppstår samt minska dess konsekvenser, utreda bakomliggande orsaker och därigenom förbättra skyddet så att liknande händelser inte inträffar i framtiden.

En kommungemensam incidenthanteringsmodell ska under 2025–2026 tas fram och implementeras. Modellen ska, så långt det är möjligt, inbegripa olika typer av incidenter (exempelvis personuppgiftsincident och informationssäkerhetsincident). Utifrån utkomsten av arbetet med incidenthanteringsprocess ska verksamheter ges lämplig utbildning i vad en incident är och hur den ska rapporteras.

Övergripande kompetenshöjande insatser
Alingsås kommun behöver fortsätta att utveckla arbetet med att ge alla som verkar i organisationen, utifrån sin roll och sitt uppdrag, höjd kunskap inom områdena informationssäkerhet och dataskydd. Vidare ska metoder för mätning av kunskapsnivåer utvecklas.

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 2025–2026. 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.

Säkerhet i digitala leveranskedjor
Utveckla arbetet med att säkerställa skyddet av information och personuppgifter vid nyanskaffning och upphandling.

Genomföra Leveranskedjekollen, MSB:s uppföljningsmodell som stödjer organisationer i att hitta arbetssätt för att säkra sina leverantörskedjor. Modellen fungerar som ett stöd i förberedelserna inför det ökade fokuset på säkra leveranskedjor som följer av NIS2.

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.

Under 2025-2026 görs nödvändiga förberedelser för att kunna genomföra MSB:s cybersäkerhetsmätningar avseende digitala leveranskedjor och OT-säkerhet under 2026. Leveranskedjekollen och OT-säkerhetskollen är nya mätningar som ingår i Cybersäkerhetskollen. Detta är ett initiativ från MSB för att mäta nivån på verksamhetens systematiska cybersäkerhetsarbete och för att ge stöd i förbättringsarbetet.

IT-säkerhet

Fortsatt införande av tvåfaktorsautentisering i verksamhet
Införande av tvåfaktorsautentisering har påbörjats under 2024 och arbetet fortlöper under 2025, med hänsyn till verksamheternas förutsättningar och med målet att omfatta merparten av våra verksamhetskritiska system.

Förenklad behörighetshantering
I syfte att förenkla behörighetshantering och säkerställa att endast behöriga användare har åtkomst till IT-miljön/informationssystem ska ett enklare förfarande för onboarding- och offboardingprocesser riktat mot specifika målgrupper utvecklas, med fokus på att säkerställa spårbarhet i behörighetsansökningar och vid förändringar samt avslut.

Påbörja överföring av verksamhetskritiska system till säkra backuper
Under 2024 har ett arbete med att skapa förutsättningar för systemredundans genomförts, i syfte att säkerställa tillgängligheten av den information som Alingsås kommun har inom sin ägo. Under 2025 påbörjas överföring av verksamhetskritiska system till säkra backuper.