

Bilaga 1 - Uppföljning Handlingsplan informationssäkerhet och dataskydd i Alingsås kommun 2022

Handlingsplan 2022

2022	KVARTAL 1	KVARTAL 2	KVARTAL 3	KVARTAL 4
NÄTVERK	Registerförteckningar			
	Risakanalys			
	Informationsklassning			
	Kontinuitetsplanering			
LEDNING OCH SAMORDNING	Översyn styrdokument			
	Incidenthantering			
	Utbildning & information ledningsnivå			
	Utbildning nämnder och styrelser			
	Framtagande uppföljningsmodell			
	Upphandlingsförfarandet			
	Ny central dataskyddsorganisation			
	Övningar			
	Utbildning & information dataskydd			
	IT-SÄKERHET	Tvåfaktorinloggning		
Behörighetshantering				
Redundant infrastruktur				

INFORMATIONSSÄKERHET OCH DATASKYDD

Nätverk

Risakanalys

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

Status: Genomfört. De flesta verksamheter har genomfört en inledande risakanalys där tre verksamhetskritiska informationstillgångar analyserats. Arbetet har inneburit identifiering av hot och sårbarheter gentemot respektive informationstillgång och till det framtagning av åtgärdsförslag för att reducera identifierade risker.

Informationsklassning

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

Status: Ej påbörjat. Momentet flyttas över till 2023. Flertalet förvaltningar har under året genomfört informationsklassningar kopplat till upphandling eller annat utvecklingsarbete, dock har arbetet inte gått genom nätverket vilket blir fallet 2023.

Kontinuitetsplanering

Kontinuitetsplanering 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.

Status: Genomfört. Mot bakgrund av förhöjd hotbild gällande cyberattacker har varje verksamhet under våren utifrån ett informationssäkerhetsperspektiv fått kontinuitetsplanera sin mest kritiska verksamhet. Därtill har varje förvaltning (såväl som på AVR och Alingsås) genomfört en övning med scenariot att hela Alingsås kommun IT-miljö ligger nere under en månad.

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.

Status: Pågående. Information om att det ska göras en översyn är lämnad till representant för respektive förvaltning. Då aktiviteten låg under kvartal 2 och 3 var förslag att göra det under semesterperioden. Socialförvaltningen har återkopplat önskan om stöd i processen, i övrigt ingen återkoppling. Arbetet fortsätter under 2023.

Ledning och samordning

Genomföra utbildnings- och informationsinsatser på ledningsnivå

Utbildning och information till ledningsgrupper gällande informationssäkerhet, dataskydd och Alingsås kommuns interna styrdokument för området.

Status: Genomförd. Besök har gjorts i de flesta ledningsgrupper någon gång under året. Aktiviteten information till ledningsgrupper förs in i planerat årshjul.

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.

Status: Genomförd. Besök har gjorts i de flesta nämnder/styrelser någon gång under året. Aktiviteten information till nämnder/styrelser förs in i planerat årshjul.

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.

Status: Genomförd. Ny central dataskyddsorganisation är implementerad. Efter vissa justeringar från ursprungsplanen är rollerna satta och bedöms kunna fungera väl och hålla över tid. Fem träffar har ägt rum under året. Samtliga deltagare har genomlyst respektive ansvarsområde och identifierat vilka behov av åtgärder som finns. Möten kommer fortsätta att hållas kontinuerligt.

Genomföra utbildnings- och informationsinsatser för dataskyddsorganisationen

Utbildning av medarbetare med funktion i ny central dataskyddsorganisation.
Utbildning av medarbetare med funktion i den kommunövergripande dataskyddsorganisationen.

Status: Genomförd. Dataskyddsorganisationen kommer även att fortlöpande erbjudas utbildning inom dataskydd generellt och inom respektive ansvarsområde specifikt.

Översyn styrdokument

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

Status: Ej påbörjat. Hela styrdokumentensstrukturen ska ses över och därefter avgöra om revidering ska ske eller ej. Flyttas över till årshjul.

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.

Status: Delvis påbörjad. IT-avdelningen har processer och tillvägagångssätt att hantera incidenter. Vi bör också titta på hur dokumentation sker och hur de förhåller sig till övriga incidenter (t ex personuppgiftsincidenter). Vi behöver framåt hitta en gemensam terminologi och definiera begreppet incident. Aktiviteten flyttas till 2023 års handlingsplan.

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.

Status: Påbörjad. Uppföljning av områdena informationssäkerhet & dataskydd kommer från 2023 delvis att ingå i Alingsås kommuns befintliga uppföljningsprocesser (delårsbokslut och årsredovisning). Informationsinhämtning sker i samlad form. Aktiviteten ingår även 2023 års handlingsplan.

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.

Status: Påbörjad. Stående möten hålls med upphandlingsenheten och representanter för informationssäkerhet & dataskydd och säkerhet. Vi har påbörjat ett samarbete för att inbegripa områdena informationssäkerhet och dataskydd i upphandlingsförfarandet. Aktiviteten ingår även 2023 års handlingsplan.

Övningar

För att bättre kunna möta de antagonistiska hot som finns behöver verksamheten testa och öva att valda säkerhetsåtgärder fungerar på ett tillfredsställande 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.

Status: Påbörjad. Varje förvaltning/bolag/förbund har givits möjligheten att öva sin kontinuitetsplanering. Mötesledare har varit personal från säkerhetsenheten på kommunledningskontoret. Merparten av verksamheterna har genomfört övningen.

IT-säkerhet

Tvåfaktorsautentisering

Detta 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 phishing och ID-kapning minskar. Under året ska tvåfaktorsinloggning införas på utvalda delar av IT-miljön.

Status: Pågår. Förutom investering i stödjande IT-infrastruktur har även tillhörande utveckling av en generisk tjänst för nyttjande inom Alingsås kommun tagits fram. Upphandling av tillhörande tjänster och programvara har genomförts. Respektive verksamhet kan nu påbörja arbetet med planering, anpassning och implementation av förhöjd säkerhet. Aktiviteten ingår även 2023 års handlingsplan.

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 behörighetssystem.

Status: Pågår. Övergripande hantering av höga behörigheter har tagits fram och en förstudie har genomförts. Under kommande år planeras ett fokus på behörighetshantering för kritisk IT-infrastruktur samt genomförande av en behörighetskontroll. Parallellt pågår arbete med att effektivare hantera anställningsförfarandet samt avslut av anställning med koppling till behörigheter och roller. Aktiviteten ingår även 2023 års handlingsplan.

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.

Status: Pågår. I arbetet med ny räddningsstation i Alingsås kommun följer möjligheten till en geografiskt åtskild IT-infrastruktur. Detta säkerställer skyddet av verksamhetskritisk information. Investeringar i kommunikationsutrustning och annan IT-infrastruktur är till större delen genomförd tillsammans med planering för implementation under kommande år. Aktiviteten ingår även 2023 års handlingsplan.