

# Informationssäkerhets- och dataskyddspolicy

<b>Beslutad av:</b>	Kommunfullmäktige
<b>Beslutsdatum:</b>	2025-12-15
<b>Beslutsparagraf:</b>	KF § 220
<b>Dokumentansvarig:</b>	Säkerhetschef
<b>Dokumentet gäller för:</b>	Ale kommun, kommunkoncernen
<b>Diarienummer:</b>	2025/635
<b>Giltighetstid:</b>	2026-01-01 – tillsvidare

## Innehåll

Informationssäkerhets- och dataskyddspolicy.....	0
<b>1 Inledning och syfte .....</b>	<b>2</b>
1.1 Syfte och omfattning.....	2
<b>2 Informationssäkerhetens och dataskyddets omfattning .....</b>	<b>2</b>
<b>3 Principer och mål med informationssäkerhets- och dataskyddsarbetet .....</b>	<b>3</b>
3.1 Roller och ansvar .....	4
3.2 Dispenser och undantag.....	5

## I Inledning och syfte

Policy för informationssäkerhet och dataskydd är ett övergripande dokument som fastställer och redovisar kommunens övergripande mål och inriktning med arbetet med informationssäkerhet och dataskydd och omfattar samtliga nämnder.

Behovet av informationssäkerhet ökar i takt med att våra medborgare förväntar sig effektiv kommunikation samt att kommunen hanterar och lagrar information som rör dem, exempelvis personuppgifter på ett säkert sätt.

Brister inom informationssäkerhet kan medföra att information går förlorad, förvanskas eller att störningar uppstår i kommunens verksamheter.

Genom att säkerställa en god nivå av systematiskt informationssäkerhetsarbete möjliggörs att gällande lagkrav följs, kritisk verksamhet upprätthålls och att informationsläckage förhindras.

### I.1 Syfte och omfattning

Informationssäkerhets- och dataskyddspolicyn syftar till att skydda Ale kommuns samhällsviktiga och digitala tjänster genom att säkerställa tillgänglighet och motståndskraft mot cyberhot. Den främjar en gemensam styrning och kultur för informations- och cybersäkerhet i hela kommunen.

Arbetet med informationssäkerhet skyddar verksamheten mot skador och avbrott, medan dataskyddet värnar individens rätt till skydd av personuppgifter. Genom ett förebyggande och strukturerat arbetssätt stärks förmågan att möta lagkrav, bevara förtroendet och minska risken för oönskade händelser.

Policyn gäller för alla som hanterar kommunens information – inklusive anställda, extern personal och ombudsmän – och ställer krav på korrekt och säker hantering av både information och personuppgifter.

## 2 Informationssäkerhetens och dataskyddets omfattning

Informationssäkerhet omfattar all information som hanteras inom kommunens verksamhet. Oavsett om informationen behandlas manuellt eller automatiserat och oberoende av i vilken form eller miljö den förekommer. Informationen kan behandlas i en dator, på papper eller i ett samtal. Av all information som kommunen hanterar utgör en stor del behandling av personuppgifter vilket ställer krav på kommunens dataskyddsarbete.

Ett väl fungerande informationssäkerhetsarbete är en förutsättning för dataskyddsarbetet. Genom att samordna informationssäkerhetsarbetet och dataskyddsarbetet skapas därför goda förutsättningar att uppfylla de krav som ställs. Ett systematiskt informationssäkerhets- och dataskyddsarbete skapar också förutsättningar för verksamhetsutveckling inom flera områden.

Arbetet med informationssäkerhet innebär att vidta fysiska, tekniska, administrativa och organisatoriska åtgärder för att uppnå eller bevara rätt skydd av informationstillgången. Informationssäkerhet handlar om att skapa och upprätthålla lämpliga rutiner och skydd av information utifrån följande aspekter:

- **Konfidentialitet** - Att information inte tillgängliggörs eller avslöjas för obehöriga
- **Tillgänglighet** - Att information kan nås när den behövs av behöriga användare
- **Riktighet** - Att information är korrekt, aktuell, fullständig och spårbar.

### 3 Principer och mål med informationssäkerhets- och dataskyddsarbetet

Arbetet med informationssäkerhet och dataskydd hos Ale kommun ska bedrivas systematiskt och riskorienterat. Skyddet av information ska anpassas efter tillämpliga lagar och förordningar, informationens värde och aktuell hotbild. Informationssäkerhets- och dataskyddsarbetet ska bedrivas som en integrerad del av vår normala verksamhetsplanering, utifrån vilken årliga mål sätts, budgeteras och följs upp. Arbetet ska ha fokus på förebyggande och proaktiva aktiviteter, men samtidigt säkerställa att det finns kapacitet att hantera incidenter, allvarliga störningar och kriser, när sådana väl inträffar.

En säker informationshantering är en förutsättning för, och syftar till att främja, ett högt förtroende från våra kommunmedlemmar, anställda och övriga intressenter. Långsiktigt uppnår vi detta genom:

- Ett systematiskt, riskbaserat, dokumenterat och kommunicerat ledningssystem för informationssäkerhet som tar sin utgångspunkt i standarden ISO/IEC 270001 samt övriga gällande nationella lagar och förordningar inom området.
- Alla medarbetare och förtroendevalda ska erbjudas relevant utbildning inom informationssäkerhet och dataskydd. Information och utbildning bidrar till att upprätthålla en hög säkerhetskultur inom kommunen och ger förutsättningar för berörda att leva upp till informationssäkerhets- och dataskyddspolicyn och övriga styrdokument.
- Kommunövergripande rutiner, regler och anvisningar ska efterlevas så att informationen är skyddad mot oavsiktlig och avsiktlig förvanskning
- Samtliga informationstillgångar ska vara identifierade, förtecknade och klassade. Genom klassificering värderas och prioriteras informationstillgångar utifrån verksamhetens krav på konfidentialitet, riktighet och tillgänglighet.
- Riskbaserat arbetssätt där riskhantering ligger till grund för val av säkerhetsåtgärder.
- Ansvar för informationssäkerhet följer det ordinarie verksamhetsansvaret. Det betyder att varje nämnd eller bolag och varje medarbetare som är ansvarig för en verksamhet eller uppgift också har att ansvara för informationssäkerheten i utförandet.

Informationssäkerhets- och dataskyddspolicyn bidrar till att uppfylla kommunfullmäktiges mål om ett tryggare Ale, ökad kundnytta och en effektivare organisation. Genom att skapa gemensam styrning och stärka motståndskraften mot cyberhot skyddas både samhällsviktiga tjänster och invånarnas personuppgifter. Policyn tydliggör ansvar och krav för säker informationshantering inom hela kommunen, vilket minskar risker och stärker förtroendet för kommunens verksamhet.

### 3.1 Roller och ansvar

Ansvaret för att säkerställa en korrekt informationshantering följer det ordinarie verksamhetsansvaret. Alla som arbetar Ale kommun har ett ansvar att känna till och följa gällande styrdokument avseende informationssäkerhet och dataskydd. Vidare finns det ett antal roller som har ett dedikerat ansvar för att övervaka och följa upp informationssäkerhets- och dataskyddsaspekter inom sitt område:

- **Kommunfullmäktige** har det övergripande ansvaret för kommunens informationssäkerhet. Genom att kommunfullmäktige fastställer informationssäkerhets- och dataskyddspolicy uttrycker de därigenom viljeinriktningen för kommunens arbete med informationssäkerhet och dataskydd.
- **Kommunstyrelsen** verkställer Kommunfullmäktiges beslut och har det övergripande ansvaret för att säkerställa att kommunens arbete med informationssäkerhet och dataskydd bedrivs i enlighet med gällande lagstiftning, förordningar och interna riktlinjer. I detta ansvar ingår att leda, samordna och utveckla kommunens strategiska och operativa arbete inom området. Kommunstyrelsen ska säkerställa att ett ändamålsenligt och effektivt ledningssystem för informationssäkerhet och dataskydd etableras, förvaltas och tillämpas inom hela organisationen. Vidare ansvarar kommunstyrelsen för att ta fram och fastställa styrande dokument som reglerar och ger stöd åt koncernens samlade informationssäkerhetsarbete. Genom detta ansvar ska kommunstyrelsen verka för att informationssäkerhet och dataskydd integreras i kommunens verksamhet på ett systematiskt och rättssäkert sätt.
- **Nämnder och kommunala bolag** säkerställer att informationssäkerheten håller rätt och relevant nivå inom deras respektive verksamheter. Nämnderna är personuppgiftsansvariga vilket innebär att de har det yttersta ansvaret för att personuppgiftsbehandlingen inom respektive nämnds verksamhetsområde. Nämnderna ansvarar också för att tillräckliga resurser finns allokerade.
- **Informationsägare** är den som äger och ansvarar för att informationen är riktig och tillförlitlig samt för det sätt informationen sprids och hanteras. Informationsägaren är därmed riskägare för den information som ska hanteras i IT-systemet/lösningen.
  - **Förvaltningschefer** är ytterst ansvariga för informationssäkerheten inom sin egen verksamhet, alltså informationsägare och riskägare. Respektive förvaltningschef/bolagschef ansvarar för att informationssäkerhetsarbetet bedrivs i linje med fastställd policy för informationssäkerhet och dataskydd.

- **Övriga chefer / Respektive chef** ansvarar för att informationssäkerhetsarbetet på enheten leds, följs upp och rapporteras.
- **Medarbetare och förtroendevalda** hanterar kommunens informationstillgångar och har ett ansvar att följa kommunens informationssäkerhets- och dataskyddspolicy och underliggande styrdokument för informationssäkerhet.

### 3.2 Dispenser och undantag

Ansökan om avsteg från policyn ska ställas till Ale kommuns utvecklingsledare för informationssäkerhet. Undantag får aldrig vara permanenta utan ska ha en giltighetstid på, som längst, 2 år. Om behov av undantag kvarstår ska ärendet beredas på nytt och nytt beslut fattas om eventuellt godkännande.