Mariestads kommun

Policy för informationssäkerhet och dataskydd

Mariestads kommunkoncern

Mariestads kommun

Typ av styrdokument: Policy
Beslutsinstans: Kommunfullmäktige
Datum för antagande: 2025-11-24
Diarienummer: 2025/298, ersätter 2019/99
Dokumentet gäller för: Mariestads kommunkoncern
Giltighetstid: Tills vidare
Tidpunkt för aktualisering: 2029 eller vid behov
Dokumentansvarig: Säkerhetschef

Mariestads kommun

Innehåll

1. Inledning **4**
1.1. Omfattning **4**
1.2. Syfte **4**

2. Informationssäkerhet och dataskydd **5**

3. Mål och lagstiftningens ramar **6**

4. Ansvarsfördelning **7**
4.1.1. Kommunfullmäktige 7
4.1.2. Kommunstyrelse 7
4.1.3. Nämnder och bolagsstyrelser 7
4.1.4. Chefer 7
4.1.5. Förtroendevalda, medarbetare och övriga 7

1. Inledning

Inom kommunkoncernens olika verksamheter hanteras information som är viktig för verksamheten, samhället och kommuninvånarna. För att verksamheten ska fungera effektivt och medborgarna känna förtroende behöver informationen hanteras säkert, korrekt och i enlighet med gällande lagstiftning. Informationssäkerhet och dataskydd är därför en integrerad del av kommunkoncernens styrning och kvalitetsarbete.

1.1. Omfattning

Denna policy omfattar all information som Mariestads kommuns samtliga nämnder och majoritetsägda bolag äger och hanterar. Policyn riktar sig till samtliga medarbetare, förtroendevalda, elever, extern part och övriga inom kommunkoncernens verksamheter som till någon del hanterar information.

1.2. Syfte

Syftet med denna policy är att ange kommunkoncernens övergripande riktning för informationssäkerhet och dataskydd. Policyn ska:

- Skapa en gemensam grund för alla verksamheter
- Tydliggöra prioriteringar och ansvarsfördelning
- Säkerställa att lagstiftningens krav omsätts i praktiken

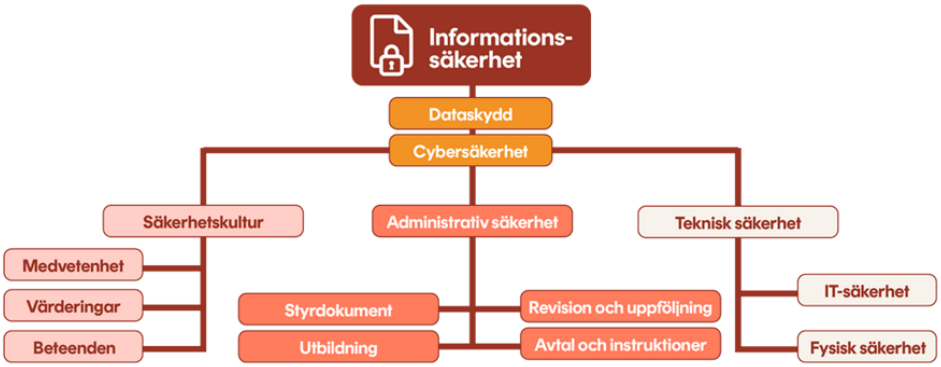
Policyn är vägledande för alla nämnder, styrelser, förvaltningar och bolag, och ligger till grund för underliggande riktlinjer och anvisningar.

2. Informationssäkerhet och dataskydd

Kommunkoncernens informations- och dataskyddsarbete ska bedrivas riskbaserat, systematiskt, ändamålsenligt och effektivt genom ett ledningssystem för informationssäkerhet och dataskydd (LIS/D). Ledningssystemet utgår ifrån den vedertagna standardserien för informationssäkerhet ISO/IEC 27000. Genom denna policy åtar sig kommunkoncernen att dels ständigt förbättra ledningssystemet, dels uppfylla tillämpliga krav inom området.

Information är medieoberoende och kan till exempel vara text, ljud, bilder, film och kan hanteras digitalt med stöd av IT, papper eller direkt av oss människor i form av tal.

Informationssäkerhet kan beskrivas utifrån följande områden: administrativ säkerhet, teknisk säkerhet och säkerhetskultur, se bild nedan. Dataskydd definieras som skyddet av den personliga integriteten för individer genom att personuppgifter hanteras lagenligt och korrekt.



Med informationssäkerhet avses förmågan att skydda information från förlust utifrån följande tre aspekter; Konfidentialitet, Riktighet och Tillgänglighet. Se bild nedan:



3. Mål och lagstiftningens ramar

Kommunkoncernens arbete med informationssäkerhet och dataskydd utgår från gällande lagstiftning, framför allt:

- Dataskyddsförordningen (GDPR) och dataskyddslagen
- Offentlighets- och sekretesslagen samt offentlighetsprincipen
- Säkerhetsskyddslagen
- Cybersäkerhetslagen träder i kraft i januari 2026 och genomför NIS2-direktivet i svensk rätt. Lagen innebär skärpta krav på informations- och cybersäkerhet, ledningens ansvar samt rapportering av incidenter.
- MSB:s föreskrifter och metodstöd för systematiskt informationssäkerhetsarbete

Nedanstående mål är kommunkoncernens sätt att säkerställa att dessa krav efterlevs.

Kommunkoncernens arbete med informationssäkerhet och dataskydd ska säkerställa att:

- **Arbetet bedrivs systematiskt och enhetligt**
  Kommunkoncernen har en gemensam styrning och ett strukturerat arbetssätt som följs i alla verksamheter.
- **Information är skyddad från att den skapas tills den inte längre behövs**
  Information ska kartläggas, klassificeras, ha tydligt ägarskap och ges ett skydd som motsvarar dess värde och risker.
- **Personuppgifter hanteras korrekt**
  Behandlingen av personuppgifter ska alltid följa lagstiftningen och värna den enskildes fri- och rättigheter.
- **Risker hanteras och verksamheten är robust**
  Identifierade risker ska ha tydligt ansvar och hanteras, och kommunen ska kunna fortsätta sin verksamhet även vid störningar eller incidenter.
- **Kompetens och kultur utvecklas**
  Alla medarbetare och förtroendevalda ska ha kunskap och förståelse för informationssäkerhet och dataskydd, så att säker hantering blir en naturlig del av arbetet.

Mariestads kommun

4. Ansvarsfördelning

Ansvaret för informationssäkerhet följer det ordinarie verksamhetsansvaret och sträcker sig på så sätt från den politiska ledningen, genom tjänstemannaorganisationen och till varje enskild medarbetare. Den som är ansvarig för en viss verksamhet (förvaltning, avdelning, enhet, process, projekt och så vidare) är också formellt ansvarig för informationssäkerheten i verksamheten.

4.1.1. Kommunfullmäktige

Kommunfullmäktige fastställer policy för informationssäkerhet och dataskydd och uttrycker därigenom inriktningen för kommunkoncernens arbete med informationssäkerhet och dataskydd.

4.1.2. Kommunstyrelse

Kommunstyrelsen har uppsiktsplikt över nämndernas och bolagens arbete med informationssäkerhet och dataskydd. Kommunstyrelsen ansvarar för att kommunfullmäktiges beslut verkställs och att det finns en fungerande styrning (ledningssystem) som stödjer ett systematiskt och ändamålsenligt arbete. Kommunstyrelsen fastställer kommunkoncernövergripande styrande dokument inom området och är personuppgiftsansvarig för sina egna verksamheter.

4.1.3. Nämnder och bolagsstyrelser

Varje nämnd och bolagsstyrelse är formellt ägare av den information som uppstår, inkommer eller hanteras inom sina verksamheter, och är ytterst ansvarig för att informationssäkerheten och dataskyddet håller rätt och relevant nivå. Nämnderna och bolagsstyrelserna ska även tillse att tillräckliga resurser finns för arbete med informationssäkerhet och dataskydd.

Nämnderna och bolagsstyrelserna är också personuppgiftsansvariga, vilket innebär att de har det yttersta ansvaret för personuppgiftsbehandlingar inom sin verksamhet samt utser Dataskyddsombud för sina verksamheter.

4.1.4. Chefer

Alla chefer i kommunkoncernen ansvarar för att verksamheten bedrivs i linje med kommunkoncernens policy för informationssäkerhet och dataskydd inklusive underliggande styrdokument.

4.1.5. Förtroendevalda, medarbetare och övriga

Samtliga förtroendevalda, medarbetare och övriga uppdragstagare som hanterar kommunkoncernens informationstillgångar har ett ansvar att följa kommunkoncernens policy för informationssäkerhet och dataskydd samt underliggande styrdokument.