ARBOGA KOMMUN

Informationssäkerhetspolicy

Arboga kommun

Antagen av Kommunfullmäktige 2023-XX-XX §XX

Innehåll

1 Inledning

Information är en av kommunens viktigaste tillgångar och hanteringen av den är en viktig och naturlig del i alla verksamheters dagliga arbete, samt en förutsättning för att verksamheterna ska nå sina mål.

Att information som kommunen hanterar i relationer med medborgare, företag och organisationer såväl som inom vår egen organisation är korrekt, utgör en grund för tillit och förtroende. Det är även viktigt att information är tillgänglig när den behövs och att känslig information skyddas för att vi ska kunna fullgöra vårt uppdrag i samhället.

Informationssäkerhet begränsas inte till säkerhet i IT-system utan omfattar information i alla dess former och oavsett hur information lagras, transporteras, bearbetas och kommuniceras. Information kan till exempel vara i form av text, ljud, bilder och film, och kan hanteras med stöd av IT, papper eller direkt av oss människor i form av tal.

2 Syfte

Denna informationssäkerhetspolicy är ett övergripande dokument som redovisar Arboga kommuns mål och principer kring informationssäkerhet samt hur ansvaret i dessa frågor är fördelat.

Denna policy är ett levande dokument och revideras vid behov.

3 Definition

Informationssäkerhet handlar om att skapa och upprätthålla rutiner och lämpligt skydd av information utifrån tre vedertagna aspekter:

- **Konfidentialitet**: att information inte tillgängliggörs eller avslöjas till obehörig
- **Riktighet**: att information är korrekt, aktuell och fullständig
- **Tillgänglighet**: att information är åtkomlig och användbar av behörig.

Information har i olika grad krav på sig gällande de tre aspekterna. Kraven kan härledas från rättsliga krav eller från Arboga kommuns egna målsättningar. Dessutom har självklart medborgare, företag och andra aktörer i vår omvärld behov och förväntningar som ställer krav på vår informationssäkerhet.

3.1 Personuppgifter, GDPR

Roller och ansvar gällande personuppgiftsbehandlingar enligt data-skyddsförordningen (GDPR) regleras i Policy för personuppgifts-behandlingar, dnr KS 172/2018.

4 Mål

Informationssäkerhet har inget egenvärde, utan ska bidra till att Arboga kommun når sina övergripande visioner och mål. Arboga kommun ska uppnå och upprätthålla en informationssäkerhet som:

- innebär en robust, säker och tillförlitlig informationshantering,
- bidrar till att uppsatta mål nås gällande exempelvis kvalitet, effektivitet och personlig integritet,
- motsvarar medborgares och externa verksamheters behov och förväntningar,
- efterlever krav i lagar, förordningar, föreskrifter och avtal.

5 Målgrupp

Policyn omfattar förtroendevalda, chefer, medarbetare och uppdragstagare inom Arboga kommun och dess helägda bolag.

6 Principer

6.1 Riskorienterad informationssäkerhet

Utifrån riskbedömningar eller informationssäkerhetsklassificeringar ska information skyddas på en **lämplig** teknisk och organisatorisk (interna rutiner och instruktioner) nivå beroende på informationens skyddsvärde. Sekretess, känslig och verksamhetskritisk information ska således ha ett starkare skydd än annan information.

Riskbedömningen eller klassificeringen ska ske utifrån ovanstående definition av informationssäkerhet och bör göras, om möjligt, redan under förarbetet av införskaffandet/upphandlingsfasen så att rätt krav kan ställas tidigt i processen.

6.2 Verksamhetsdriven informationssäkerhet

Verksamheterna har ansvar för sin informationssäkerhet och har bäst kunskap om hur känslig och kritisk deras information är, och kan därmed fastställa informationens skyddsvärde.

En verksamhetsdriven informationssäkerhet innebär att verksamheter utifrån informationens skyddsvärde ställer krav på de aktörer som hanterar informationen, exempelvis kommunens IT-avdelning eller externa systemleverantörer, men det innebär också ett ansvar att se till att medarbetare och uppdragsgivare följer de rutiner och anvisningar som finns och att det finns ett grundskydd för all information i verksamhetens lokaler.

7 Ansvar och roller

Ansvaret för informationssäkerhet följer det ordinarie verksamhetsansvaret.

Kommunfullmäktige uttrycker sin viljeinriktning avseende kommunens arbete med informationssäkerhet i denna policy.

Kommunstyrelsen ansvarar för att följa upp kommunens informationssäkerhetsarbete.

Kommundirektör har det övergripande ansvaret för informationssäkerheten.

Säkerhetsskyddschef ansvarar för informationssäkerheten i verksamhet som har betydelse för Sveriges säkerhet och lyder under säkerhetsskyddslagen, till exempel om kommunen har ett skyddsobjekt eller förvarar så kallade hemliga handlingar.

IT-chef har det operativa ansvaret för att uppfylla de krav som verksamheterna ställer på den gemensamma tekniska IT-infrastrukturen.

Nämnderna/styrelserna Varje enskild nämnd/bolagsstyrelse ansvarar för den information, de dokument och de informationssystem som finns inom det egna verksamhetsområdet.

Förvaltningschef eller VD ansvarar för att ge förutsättningar så att lämplig informationssäkerhet upprätthålls för den information som finns inom det egna verksamhetsområdet.

Om verksamheten definieras som samhällsviktig av MSB och därmed faller under NIS-direktivet ansvarar förvaltningschef eller VD för att verksamheten uppfyller de krav som då tillkommer, så som ledningssystem för informationssäkerhet, väl etablerade rutiner och verktyg för incidentrapportering, internkontroller med mera.

Det åligger varje verksamhetsansvarig att tillse att sina medarbetare har ett säkerhetsmedvetande och tillräcklig förståelse och kunskap för att en erforderlig informationssäkerhet i verksamheten kan uppnås.

Systemförvaltare ska omvärldsbevaka risker och hot och har det operativa ansvaret att planera för och införa såväl tekniska som organisatoriska säkerhetsåtgärder på lämplig nivå utifrån informationens skyddsvärde. Om systemförvaltare saknas ligger ansvaret hos systemägaren (oftast verksamhetsansvarig).

Informationsägare ansvarar för att riskbedöma eller informationssäkerhetsklassificera sin information samt att förmedla detta till systemförvaltaren eller till upphandlingsenheten i ett tidigt skede.

Medarbetare, förtroendevalda, elever och uppdragstagare ansvarar för att följa de informationssäkerhetsanvisningar och instruktioner som finns samt att alltid agera säkerhetsmedvetet och arbeta aktivt för att sekretess och personuppgifter inte röjs.