Bromölla kommun

KOMMUNAL FÖRFATTNINGSSAMLING **Nr 005.1**

Antagen/Senast ändrad	**Gäller från**	**Dnr**
KF 2026-06-15 § 86	2026-06-16	2026/341

INFORMATIONSSÄKERHETSPOLICY

_____

Dokumentnamn:	Giltighetstid:		Gäller för:
Informationssäkerhetspolicy	**Tills vidare**		**Kommunen**
Dokumentansvarig:	Dokumenttyp:		Version:
Informationssäkerhetssamordnare	**Policy**		**1.0**
Fastställd av:	Informationsklass:	Godkänt datum:	Dnr:
Kommunfullmäktige	**Öppen**	**2026-06-15**	**2026/341**

Informationssäkerhetspolicy

Definition av informationssäkerhet

Information är en av flera skyddsvärda tillgångar i kommunen och ska hanteras utifrån grundprinciperna för bevarandet av egenskaperna:

- **Konfidentialitet** – att informationen endast är tillgänglig för behöriga personer, processer och enheter
- **Riktighet** – att information är korrekt, fullständig och skyddad mot auktoriserad eller oavsiktlig ändring
- **Tillgänglighet** – att **i**nformationen och tillhörande tjänster är åtkomliga och användbara när verksamheten behöver dem
- **Spårbarhet** – att det i efterhand går att fastställa specifika händelser till identifierbar individ eller objekt

Denna informationssäkerhetspolicy anger riktningen för informationssäkerhetsarbetet inom kommunen. Policyn ska vara ett stöd och vägledning för våra anställda i arbetet med att hantera verksamhetens informationstillgångar.

Informationssäkerhetspolicyn kompletteras med underliggande riktlinjer för informationssäkerhet som tillsammans med policyn utgör kommunens ledningssystem för informationssäkerhet.

Strategiska mål

Det åligger kommunen att uppfylla nuvarande och tillkommande lagkrav. Cybersäkerhetslagen berör kommunen från januari 2026 och kräver tillämpning av ett systematiskt informationssäkerhetsarbete som stödjer ständiga förbättringar.

Kommunens ledningssystem för informationssäkerhet utgår ifrån de grundläggande kraven i standarden ISO/IEC 27000, NIS 2 och Cybersäkerhetslagen.

Tillämpning

Informationssäkerhetspolicyn omfattar all information, oavsett om den hanteras digitalt eller analogt, samt alla de system och den infrastruktur som används för att behandla informationen. Policyn gäller för samtliga kommunens medarbetare och förtroendevalda.

Principer för informationssäkerhetsarbetet

Informationssäkerhetsarbetet ska bedrivas så att det stödjer kommunens arbete med digitalisering samtidigt som det skyddar kommunens, medarbetarnas och medborgarnas informationstillgångar utifrån informationstillgångens skyddsvärde.

Det systematiska informationssäkerhetsarbetet ska bidra till att kommunen upprätthåller en nivå av informationssäkerhet som

- grundar sig i ett riskbaserat arbetssätt
- innebär en säker och lagenlig informationshantering
- möjliggör digitaliseringssatsningar och utförande av myndighetsuppdrag

- har en tillräcklig kompetensnivå
- har en positiv effekt på kvalitet och effektivitetsmål
- bidrar till en god säkerhetskultur och uppmuntrar till engagemang hos samtliga medarbetare och, förutom att följa gemensamma regler, motiverar dem att delta i att ständigt förbättra informationssäkerheten

Roller och ansvar för informationssäkerhetsarbetet

Kommunfullmäktige fastställer informationssäkerhetspolicy och uttrycker därigenom viljeinriktningen för kommunens arbete med informationssäkerhet.

Kommunstyrelsen har det övergripande ansvaret för att leda, samordna och utveckla kommunens informationssäkerhetsarbete. Samtidigt ansvarar respektive nämnd för hur informationssäkerheten bedrivs inom deras verksamhetsområden.

Grundprincipen är att ansvaret för informationssäkerheten följer det ordinarie verksamhetsansvaret. Detta gäller från kommunledningen till den enskilde medarbetaren, och innebär att den som är ansvarig för en viss verksamhet också är ansvarig för informationssäkerheten inom verksamheten.

Medarbetare och förtroendevalda hanterar kommunens informationstillgångar och har ett ansvar att följa kommunens informationssäkerhetspolicy och underliggande styrdokument för informationssäkerhet.

Funktion för informationssäkerhet

Kommunen säkerställer att det finns en funktion med ansvar för att samordna och driva informationssäkerhetsarbetet. Hur denna funktion organiseras avgörs av respektive kommun utifrån behov, storlek och förutsättningar. Det övergripande ansvaret för informationssäkerhet följer alltid det ordinarie verksamhetsansvaret.

Funktionen för informationssäkerhet ansvarar för att:

- analysera omvärlden och den egna organisationen ur ett informationssäkerhetsperspektiv samt säkerställa att detta integreras i kommunens arbete med verksamhetsanalys
- säkerställa att informationssäkerhetsarbetet utgår från identifierade risker samt relevanta förändringar i omvärlden
- utveckla och etablera arbetssätt för informationssäkerhet, inklusive planer, styrdokument, metodstöd och systemstöd
- ge stöd och vägledning till verksamheterna i att tillämpa och efterleva informationssäkerhetsarbetet
- följa upp och genomföra kontroller av kommunens interna informationssäkerhetsarbete

Styrning och efterlevnad

Kommunstyrelsen ska tillse att informationssäkerhetsarbetet bedrivs effektivt, inklusive hantering av risker, omhändertagande av informationssäkerhetsbrister, rapportering av avvikelser och i förekommande fall incidentrapportering till berörda myndigheter. Genom god intern kontroll, revisioner och via ledningens förbättringsarbete övervakar kommunstyrelsen att

informationssäkerhetsarbetet är ändamålsenligt. För att utöva sin tillsynsplikt, håller sig kommunstyrelsen informerad om arbetet med informationssäkerhet genom minst årlig rapportering.