

Policy

Gullspångs kommun

Informationssäkerhetspolicy



Beslutad av: Kommunfullmäktige

Datum och paragraf: 2017-06-21, § 98

Dokumentansvarig:
Informationssäkerhetssamordnare

Gäller från: 2017-06-21

Diarienummer: KS 2017–00314



**GULLSPÅNGS
KOMMUN**

Innehåll

Informationssäkerhetspolicy	3
Syfte och mål.....	3
Ansvar för informationssäkerhet och informationssäkerhetspolicy	3
Operationalisering av informationssäkerhetspolicyn	4
Informationsklassificering.....	4
Revision och uppdatering av policyn	4
Definitioner	4

Informationssäkerhetspolicy

I Gullspångs kommuns verksamheter finns stora informationsmängder. Informationen är inte sällan känslig om den sprids till obehöriga, bland annat med hänsyn till enskildas personliga integritet samt att information kan missbrukas för att störa samhällets funktionalitet eller för att tillskansa sig ekonomiska fördelar. Den kommunala verksamheten är därtill ofta beroende av att ha tillgång till rätt information i rätt tid för att på ett effektivt sätt kunna uppfylla sina åtaganden.

Sammantaget finns ett starkt behov av att skydda information från att spridas till fel personer, att skydda information från att förvanskas samt se till att information finns tillgänglig när den behövs i verksamheten. Kommunens informationssäkerhetsarbete ska bidra till det.

Informationssäkerheten ska vara en integrerad del av kommunens verksamheter. Alla som i någon utsträckning hanterar informationstillgångar har ett ansvar att upprätthålla informationssäkerheten.

För att inrikta detta arbete har en informationssäkerhetspolicy upprättats. Policyn och tillhörande styrdokument omfattar kommunens alla informationstillgångar.

Syfte och mål

Policyns syfte är att den kommunala verksamheten med hjälp av informationstillgångar ska kunna bedrivas på ett effektivt och säkert sätt.

Målet med informationssäkerhetspolicyn är att alla kommunens informationstillgångar ska omfattas av en tillräcklig skydds nivå med hänsyn till konfidentialitet, riktighet, tillgänglighet och spårbarhet. Rätt information ska finnas tillgänglig när den behövs för behörig person och på ett spårbart sätt.

Ansvar för informationssäkerhet och informationssäkerhetspolicy

Kommunfullmäktige beslutar om informationssäkerhetspolicy för Gullspångs kommun. Kommunens nämnder och styrelser ansvarar för att informationssäkerheten upprätthålls inom respektive verksamhet. Kommunstyrelsen har uppsiktsplikt över nämnder och styrelser.

Nämnder och styrelser är ansvariga för att informationstillgångar inom underliggande verksamheter omgärdas av ett tillräckligt skydd. Respektive nämnd och styrelse ska analysera behovet av, och eventuellt ta fram, egna rutiner för underliggande verksamheter till stöd för denna policy.

Verksamhets- och bolagschefer kan av nämnd/styrelse delegeras det operativa ansvaret för informationssäkerhetsarbetet.

En chefsbefattning i kommunen innebär ansvar för att underställd personal är informerade och utbildade i regler kring informationssäkerhet. Det innebär också ansvar för att regler följs inom chefsbefattningens ansvarsområde. I ansvaret ligger också att personer som inte är

anställda av men arbetar med och åt kommunen har tillräckligt god kunskap om kommunens regler för informationssäkerhet.

Alla kommunanställda har ansvar för att sätta sig in i och följa aktuella rutiner och regler för informationssäkerhet.

Den som använder kommunernas informationstillgångar eller i övrigt agerar på ett sätt som strider mot denna policy eller övriga styrdokument avseende informationssäkerhet kan bli föremål för åtgärder från kommunens sida.

Operationalisering av informationssäkerhetspolicyn

Hur informationssäkerhetspolicyns syfte och mål ska nås konkretiseras genom riktlinjer och instruktioner. Dessa styrdokument antas av kommunchefen vad gäller kommunövergripande styrning. Styrdokument som gäller särskilda rutiner inom enskilda verksamhetsområden antas av verksamhets- eller bolagschef.

Informationsklassificering

Kommunens informationstillgångar ska klassificeras med hänsyn till konfidentialitet, riktighet, spårbarhet och tillgänglighet. Därigenom kan lämpliga skydds krav ställas för respektive informationstillgång. För tillgångar som bedöms vara särskilt viktiga ska en ägare utses och riskanalyser upprättas. Verksamhets- och bolagschef är ansvarig för att informationsklassning görs.

För de verksamhetssystem som i informationsklassificeringen konstateras vara kritiska för verksamheten ska en systemsäkerhetsplan upprättas och hållas uppdaterad. För informationstillgångar med höga krav på tillgänglighet inkluderar det en avbrottsplan. Verksamhets- och bolagschef är ansvarig för att det görs.

Revision och uppdatering av policyn

Kommunchefen är ansvarig för att behovet av revision av informationssäkerhetspolicyn årligen analyseras samt att vid behov föreslå revideringar av den till kommunfullmäktige.

Nämnder och styrelser är ansvarig för att efterlevnaden av informationssäkerhetsarbete kontrolleras och att en årlig rapport lämnas till kommunstyrelsen.

Definitioner

Informationstillgångar: en viss informationsmängd/typ av information som är skyddsvärd. Kan vara ett verksamhetssystem om det är starkt knutet till just en typ av information, exempelvis ett journalsystem inom vård- och omsorgsområdet.

Konfidentialitet: information är endast tillgänglig för dem som är behöriga att ta del av och använda den.

Riktighet: informationen skyddas mot oönskad och obehörig förändring eller förstörelse.

Spårbarhet: ändringar av information är möjlig att följa i efterhand.

Tillgänglighet: informationen finns tillgänglig enligt verksamhetens krav.