Policy för informationssäkerhet i Grästorps kommun

Typ av styrdokument	Policy
Fastställd av	Kommunfullmäktige 2023-06-19, § 43
Uppdateras före	-
Dokumentansvarig	Informationssäkerhetssamordnare
Dokumentet finns på www.grastorp.se	

Innehåll

Inledning

Information är en av kommunens viktigaste tillgångar och en hörnsten i den dagliga verksamheten. Informationstillgångarna i kommunen måste därför hanteras och bevaras på ett tillfredsställande sätt.

Informationssäkerhet bygger på tre grundprinciper:

- **Konfidentialitet:** att informationen endast finns tillgänglig för behöriga.
- **Riktighet:** att informationen är korrekt, och inte kan ändras av obehöriga.
- **Tillgänglighet:** att informationen finns tillgänglig för behöriga när den behövs.

Definition av informationssäkerhet

Information är värdefullt och behöver därför skyddas efter behov. Ett bra informationssäkerhetsarbete är en förutsättning för effektiv och korrekt informationshantering. Informationen ska endast finnas tillgängliga för de som är behöriga att ta del av den. Informationen ska vara korrekt och inte kunna manipuleras eller förstöras av obehöriga. Informationen ska vara tillgänglig att användas av behöriga när den behövs. En korrekt och säker informationshantering skapar förtroende både inom och utanför kommunen.

Lagstiftning

På en övergripande nivå finns krav på informationssäkerhet i flertalet lagar som rör kommunen och dess verksamheter. Dataskyddsförordningen (GDPR) och säkerhetsskyddslagen är hörnstenar i informationssäkerhetsarbetet.

- **GDPR:** ställer krav på hanteringen av personuppgifter.
- **Säkerhetsskyddslagen:** ställer krav på verksamheter som är väsentliga för Sveriges säkerhet.

Intressenter

De myndigheter som stödjer och följer upp informationssäkerhetsarbetet innefattas bland andra av:

- MSB (Myndigheten för samhällsskydd och beredskap)
- SKR (Sveriges Kommuner och Regioner)
- IMY (Integritetsskyddsmyndigheten)
- Säkerhetspolisen

Syftet med en informationssäkerhetspolicy

Regeringens ”Nationell strategi för samhällets informations- och cybersäkerhet” (skr. 2016/17:213) fastslår att bland annat informationssäkerheten på kommunnivå är i behov av att utvecklas. En av målsättningarna i strategin är att statliga myndigheter, kommuner och landsting ska ha kännedom om hot och risker, ta ansvar för sin informationssäkerhet

och bedriva ett strukturerat och riskbaserat informationssäkerhetsarbete för att säkerställa den fortsatta digitaliseringen av samhället, samtidigt som vi hävdar Sveriges säkerhet och nationella intressen såsom mänskliga fri- och rättigheter och samhällets funktionalitet.

Kommunens informationssäkerhetspolicy gäller för all information som verksamheterna upprättar, hanterar och äger.

Kommunens systematiska informationssäkerhetsarbete ska grunda sig i standarden SS-EN ISO/IEC 27000 serien och utgöra kommunens ledningssystem för informationssäkerhet. Genom att införa ett systematiskt och riskbaserat ledningssystem för informationssäkerhet kommer kommunen leva upp till kravställande myndigheter och medborgarnas förväntningar i hanteringen av information. Informationssäkerhetsarbetet ska implementeras på samtliga nivåer i verksamheten genom riktlinjer och rutiner, vilket resulterar i att samtliga informationstillgångar skyddas på en acceptabel nivå.

Strategiska målsättningar

Systematiskt informationssäkerhetsarbete

Kommunens ledningssystem för informationssäkerhet ska bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete med stöd av standarden ISO 27000.

Kommunen ska utforma informationssäkerhetsarbetet så att det möter de lagkrav som berör kommunen.

Organisation

Kommunen ska upprätta en organisation med tydliga ansvarsfördelningar för genomförandet av det systematiska informationssäkerhetsarbetet. En riktlinje ska finnas som beskriver organisationen för informationssäkerhet.

Chefer, medledare och förtroendevalda

Samtliga inom kommunens verksamheter ska erbjudas utbildning inom informationssäkerhet relevant för deras befattning. Utbildning samordnas via informationssäkerhetssamordnaren. Chefer har ett ansvar att tillse att deras medledare har rätt förutsättningar för att hantera de informationstillgångar deras arbete kräver. En riktlinje för informationssäkerhet för medarbetare och förtroendevalda ska finnas.

Fysisk och teknisk säkerhet

Kommunen ska fastställa kraven på den fysiska och tekniska säkerheten i samtliga system som används i verksamheten. En riktlinje som beskriver fysisk och teknisk säkerhet ska finnas.

Upphandlingar

Kommunen ska fastställa de informationssäkerhetsrelaterade krav som ska ställas vid upphandlingar och i avtal med leverantörer som kommer hantera information inom verksamheten.

Kommunen ska kontrollera att leverantörerna följer de krav som ställs. En riktlinje för informationssäkerhet vid upphandlingar ska finnas.

Hantering av informationssäkerhetsincidenter

En rutin för informationssäkerhetsincidenter och avvikelser ska finnas. För att uppfylla vissa lagkrav på informationssäkerhet behöver rutiner för hur, var och när incidenter rapporteras till berörda myndigheter upprättas.

Efterlevnad

Efterlevnaden av informationssäkerhetsarbetet ska följas upp via internkontroll. Rutiner för internkontroll ska finnas.