

Författning 6.15

Antagen av kommunfullmäktige § 98, 2021



Staffanstorps
kommun

Informationssäkerhetspolicy

Skapat datum	2020-03-02
Senast ändrad	2021-07-05

Innehållsförteckning

1. Inledning och bakgrund.....	3
2. Syfte.....	3
3. Mål.....	3
4. Roller och ansvar	4
5. Informationsklassning	4
6. IT-säkerhet.....	4
7. Principer för arbetet.....	4
8. Revidering.....	5

1. Inledning och bakgrund

Information är en mycket viktig resurs och en förutsättning för Staffanstorps kommun för att kunna bedriva en ändamålsenlig verksamhet. 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. Idag används informationssystem som effektiviserar kommunikationen inom kommunen och gör att mängden information ökar i hög fart.

Den tekniska utvecklingen medför även att alltmer information lagras i molntjänster i stället för på lokala servrar eller i fysisk pappersform. Denna utveckling innebär att kraven blir fler och större för hur information både behandlas och säkerställs. Staffanstorps kommun arbetar aktivt för att upprätthålla kraven och för att garantera en informationssäker hantering inom verksamheten.

Informationssäkerhetspolicyn omfattar all sorts information oavsett om det är information i molntjänster, i datorer, i telefonsamtal/sms, fysiska samtal, på papper eller annat. Policyn är antagen av Kommunfullmäktige och gäller hela kommunkoncernen.

Informationssäkerhet handlar om att skapa och upprätthålla lämpliga rutiner och skydd av information utifrån fyra 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
- **Spårbarhet:** att informationsbearbetning ska kunna härledas till vem och när.

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

2. Syfte

Denna policy har som syfte att tydliggöra kommunledningens syn på vad som krävs för säker informationshantering inom Staffanstorps kommuns nämnder och bolag. Kontinuerligt informationssäkerhetsarbete är nödvändigt för att kunna uppfylla kommunens uppdrag och mål. Syftet med informationssäkerhetsarbetet är att skydda kommunens verksamhet mot avbrott och minska skador genom att förebygga och minimera verkan av oönskade händelser. Policyn gäller som ovan nämnt för all sorts information.

3. Mål

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

- innebär en robust, säker och tillförlitlig informationshantering,
- möjliggör ett aktivt medverkande i det digitala samhället,
- bidrar till att uppsatta mål nås gällande exempelvis kvalitet, effektivitet och personlig integritet,
- motsvarar medborgares och externa verksamheters behov och förväntningar,
- uttrycks i aktuella styrdokument som policy och riktlinjer,
- efterlever krav i lagar, förordningar, föreskrifter och avtal.

4. Roller och ansvar

Alla som i någon utsträckning hanterar informationstillgångar har ett ansvar att upprätthålla informationssäkerheten.

Ansvaret för respektive verksamhets informationssäkerhet följer verksamhetsansvaret.

Staffanstorp kommuns policy för informationssäkerhet antas av **kommunfullmäktige**.

Kommunstyrelsen ansvarar för att följa upp kommunens arbete med informationssäkerhet.

Kommundirektören ansvarar inför kommunstyrelsen att verksamheterna effektivt följer och upprätthåller policyn för informationssäkerhet.

Säkerhetschefen och **informationssäkerhetssamordnare (CISO)** har ansvar för att stötta verksamheterna i informationssäkerhetsarbetet.

Informationsägare är ansvarig för att informationen är riktig och tillförlitlig samt för det sätt informationen sprids. Informationsägaren ansvarar för att riskanalys och klassning genomförs för informationstillgångensamt ställer krav på systemägare för att skyddet i informationssystemet är tillräckligt.

Systemägare är ansvarig för att informationssystemen och dess leverantörer uppfyller kommunens policy för informationssäkerhet. **Systemförvaltare** är i sin tur ansvarig för användningen i informationssystemen.

Varje anställd, förtroendevalda, konsulter, entreprenörer etc i kommunen har ett ansvar att följa denna policy samt de riktlinjer och gällande lagar som finns för informationssäkerhet. Ansvaret sträcker sig ner på rutinnivå för den anställde genom att följa fastställda rutinbeskrivningar vid informationshantering samt att rapportera fel och störningar i system. Ovan nämnda parter ska även vara väl förtrodda med gällande lagstiftning och internastyrdokument.

5. Informationsklassning

Kommunens informationstillgångar ska klassificeras med hänsyn till krav på konfidentialitet, riktighet, spårbarhet och tillgänglighet. Därigenom kan lämpliga skydds krav ställas upp för respektive informationstillgång. Handlingsplaner ska göras för åtgärder som ska följas upp. För de tillgångar som bedöms vara särskilt viktiga ska en riskanalys upprättas.

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 kontinuitetsplan.

6. IT-säkerhet

Fysisk säkerhet ska finnas för att skydda IT-tillgångar för obehörig åtkomst eller störningar samt skador på lokaler, utrustning och information. Om kommunens interna fysiska säkerhet inte uppfyller systemets säkerhetskrav, ska erforderlig risk- och sårbarhetsanalys utföras.

Systemsäkerhet ska finnas för att säkerställa åtkomst utifrån verksamhets- och lagkrav.

7. Principer för arbetet

Staffanstorp kommun ska arbeta med informationssäkerhet på ett sätt så att ovanstående mål uppfylls. Arbetet med informationssäkerhet ska gentemot kommunens verksamheter vara normerande, stödande

och kontrollerande. Viktiga förmågor i det arbetet är att kunna identifiera hot, sårbarheter och risker rörande Staffanstorps kommuns informationstillgångar samt att kunna utforma och införa säkerhetsåtgärder som reducerar dessa risker till en acceptabel nivå.

Arbetet med informationssäkerhet inom Staffanstorp kommun ska:

- bygga på en helhetssyn som utgår från information, men som också innefattar processer, människor och teknik,
- vara systematiskt och bygga på den etablerade standardserien SS-ISO/IEC 27000 med målet att skapa ett ledningssystem för informationssäkerhet (LIS),
- löpande ses över och förbättras, eftersom Staffanstorp kommun och dess omvärld, inklusive hotbild, är under ständig förändring,
- vara förebyggande och proaktivt, men också ha en god förmåga att kunna hantera incidenter, allvarliga störningar och kriser som ändå kan inträffa,
- bygga på Staffanstorps kommuns värderingar och ta hänsyn till verksamheters behov, externa krav samt rådande hotbild,
- vara väl kommunicerat till verksamheten; all personal ska fortlöpande få information och utbildning för att nå och upprätthålla ett högt säkerhetsmedvetande och för att kunna leva upp till denna policy och underliggande riktlinjer för informationssäkerhet,
- ske i aktiv samverkan med det omgivande samhället såsom myndigheter, företag och nätverk, särskilt sådana som är normgivande inom informationssäkerhet som t.ex. SKR (Sveriges kommuner och regioner), MSB (Myndigheten för samhällsskydd och beredskap) och SIS (Swedish Standards Institute).
- beaktas vid anskaffning, utveckling och avveckling av datasystem,

8. Revidering

Informationssäkerhetspolicyen revideras vid behov och ansvarig för detta är kommunens säkerhetschef.