Beslutad:	Kommunfullmäktige, KF § 77, 2013-06-17
Gäller fr o m:	2013-06-17
Myndighet:	Kommunstyrelsen
Diarienummer:	KS/2013:15–003
Ersätter:	-
Ansvarig:	Informationssäkerhetsansvarig

Informationssäkerhetspolicy

Denna policy utgör det övergripande dokumentet för informationssäkerhetsarbetet inom Strängnäs kommun. Genom denna policy regleras ansvar och inriktning för säker behandling av information och för existerande och framtida informationssystem.

Informationssäkerhetspolicyn utgör ett bindande styrdokument och anger mål för säker informationsbehandling inom kommunens olika verksamheter. Policyn ska konkretiseras i kommunövergripande riktlinjer samt i varje verksamhets instruktioner och handböcker på sådant sätt att målsättningar kan uppfyllas.

Information som verksamheterna behöver för att lösa sina uppgifter är många gånger både känslig och kritisk till sin natur och finns i alla verksamheter och beslutande organ. Invånarna förväntar sig att verksamheterna och nämnderna behandlar information på ett betryggande sätt och att man har tillgång till nödvändig information även i händelse av krissituationer.

Kommunens information är därför inom flera verksamhetsområden av strategisk betydelse, och verksamheterna behöver beakta informationens konfidentialitet, tillgänglighet, riktighet och spårbarhet.

Informationssäkerhet definieras som:

- att rätt information är tillgänglig för rätt person, vid rätt tid och utan onödigt dröjsmål
- att konfidentiell information undanhålls obehöriga
- att information är och förblir riktig
- att åtkomst till, och förändringar av, information är spårbar

Definitioner

Information kan förekomma i många olika former – tryckt eller skrivet på papper, lagrad elektroniskt i IT-utrustning och på lagringsmedia, överföras med post och elektronisk utrustning, yttras i en konversation och del av en persons kunskap. IT-system/utrustning som behandlar information kallas för informationsbehandlande resurser och tillsammans med information utgör de kommunens informationstillgångar.

Konfidentialitet (sekretess) är förmågan att utestänga obehöriga från informationstillgångarna.

Tillgänglighet är förmågan att hålla informationstillgångarna och verksamhet tillgängliga och fungerande.

Riktighet är förmågan att verifiera att informationstillgångarna inte har förändrats otillbörligt.

Spårbarhet är förmågan att kunna spåra händelser till tidpunkt, person och plats.

Målgrupper

Denna policy vänder sig till kommunens samtliga anställda, förtroendevalda samt annan kontrakterad personal och samarbetspartners som kommer i kontakt med kommuns informationstillgångar. Policyn riktar sig också till kommunens invånare i syfte att informera om kommunens arbete inom informationssäkerhet.

Bolag där kommunen utövar ett rättsligt bestämt inflytande ska upprätta egen policy för informationssäkerhet som är i samklang med denna policy.

Målformulering

Information är i flera verksamheter den viktigaste tillgången och en förutsättning för att verksamheten ska kunna bedrivas på ett ändamålsenligt och effektivt sätt. Om information hanteras på ett felaktigt sätt kan kommunens verksamhet och varumärke påverkas negativt.

Det övergripande målet gällande informationssäkerhet är att säkerställa ett tillräckligt skydd för informationstillgångarna så att rätt information är tillgänglig för rätt person i rätt tid och på ett säkert sätt. Särskilt skyddsklassad och skyddsvärda informationstillgångar ska vara tillgängliga på ett spårbart sätt.

Långsiktiga mål för informationssäkerhetsarbetet;

- Samtliga verksamma inom kommunen ska ha ett högt säkerhetsmedvetande.
- Känslig information skall undanhållas obehöriga.
- Information skall kunna hållas tillgänglig över de tidsperioder som krävs, och skall förstöras på ett betryggande sätt vid gallring.
- För kommunen viktig verksamhet skall kunna bedrivas trots allvarliga störningar.
- Kritiska informationssystem och infrastruktur för tele- och datakommunikation skall ha hög tillgänglighet.
- Kritiska informationssystem och infrastruktur för tele- och datakommunikation skall ha skyddsfunktioner som motsvarar hotbilden.
- Kommunen skall ha en hög beredskap för att kunna hantera kriser.

Organisation, roller och ansvar

Kommunfullmäktige fastställer informationssäkerhetspolicyn.

Kommunstyrelsen har det övergripande ansvaret för informationssäkerhetsarbetet och att intern kontroll fungerar tillfredsställande. Kommunstyrelsen ansvarar också för att informationssäkerhetspolicyn årligen granskas och vid behov revideras.

Kommunstyrelsen ansvarar för att informationssäkerhetsarbetet bedrivs i linje med fastställd informationssäkerhetspolicy. För det ändamålet fastställer kommunstyrelsen de kommunövergripande riktlinjerna för informationssäkerhetsarbetet som krävs för att policyn ska uppfyllas.

Respektive nämnd, med tillhörande kontor eller enhet, är ansvariga för informationssäkerheten inom sitt/sina verksamhetsområden. Respektive nämnd ansvarar för att ta fram årliga mål och aktiviteter för att upprätthålla god informationssäkerhet.

Chefer på alla nivåer ansvarar för att informationssäkerhetsarbetet bedrivs enligt gällande policy och riktlinjer inom sitt respektive ansvarsområde.

Varje medarbetare ansvarar för att tillämpa gällande informationssäkerhetspolicy, riktlinjer och regler. Varje medarbetare ska också vara uppmärksam och rapportera händelser och avvikelser som kan påverka säkerheten, och aktivt verka för att förbättra säkerheten inom sin verksamhet.