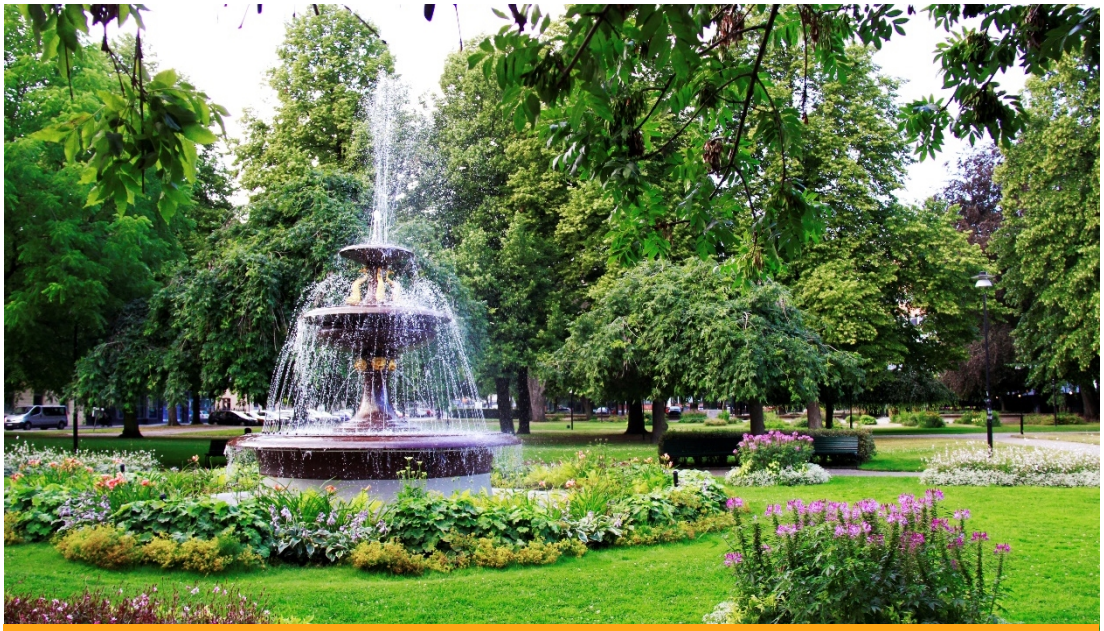
Policy

Policy för Informationssäkerhet

Diarienummer KS 2025/0756



Beslutad av: Kommunfullmäktige

Beslutdatum: Den 25 september 2025

Gäller för: Kommunkoncernen

Ansvarigt kontor för uppföljning Tillväxt och utvecklingskontoret

Dokumentet ersätter: Riktlinje för informationssäkerhet i Norrköpings kommun KS 2017/1530

TILLVÄXT OCH UTVECKLINGSKONTORET

Policy för informationssäkerhet

Denna informationssäkerhetspolicy redovisar Norrköpings kommunfullmäktiges principer för informationssäkerhetsarbetet.

Inledning

Att den information som kommunen hanterar i relation till kommuninvånare, företag och organisationer samt inom vår egen organisation är korrekt utgör en grund för tillit och förtroende.

Informationssäkerhet är den samlade benämningen på de organisatoriska, administrativa, tekniska och fysiska åtgärder som ska vidtas i syfte att skydda kommunens information mot de hot som den kan utsättas för.

Målsättningen med kommunens informationssäkerhetsarbete är att skydda kommunen, dess verksamhet och invånare som annars riskerar att skadas genom bristande informationssäkerhet.

Informationssäkerhetspolicyn samt dess tillhörande styrdokument syftar till att uppfylla de legala, etiska och verksamhetsmässiga krav som uppställs på kommunen.

Vidare ska informationssäkerhetspolicyn samt dess tillhörande styrdokument tydliggöra hur ledning och styrning av informationssäkerheten ska ske.

Omfattning

Informationssäkerhetsarbetet ska ske genom systematiskt och långsiktigt arbete och omfatta hela kommunkoncernen och alla informationstillgångar som finns inom den.

Principer för informationssäkerhet

Kommunens informationssäkerhetsarbete ska säkerställa att **rätt information är tillgänglig för rätt person vid rätt tidpunkt**, med bevarad **riktighet, konfidentialitet och tillgänglighet**. Arbetet ska skydda kommunens informationstillgångar mot förlust, missbruk, obehörig åtkomst och andra säkerhetshot – samtidigt som det skapar **förtroende hos medborgare, anställda och samverkansparter**.

Principen för informationssäkerhet är enkelt uttryckt att rätt information ska vara tillgänglig för rätt person i rätt tid. Principen ska uppfyllas genom framtagande, implementering och efterlevnad av denna policy samt av tillhörande styrande och stödjande dokumentation för informationssäkerhet.

Kommunstyrelsen ansvarar för det strategiska arbetet med informationssäkerhet. Med detta menas bland annat att kommunstyrelsen anger vad som ska skyddas, hur en verksamhet ska avgöra lämplig skyddsnivå samt hur det faktiska skyddet uppnås.

Kommunstyrelsen ska säkerställa att kommunen har administrativ, teknisk och fysisk säkerhet implementerad och väl känd i organisationen.

Kommunstyrelsen ges i uppdrag att konkretisera denna policy genom en riktlinje vari ramarna för kommunens ledningssystem för informationssäkerhet ska framgå. Riktlinjerna och därtill hörande stöddokumentation ska ge förutsättningar för kommunens verksamheter att leva upp till kommunens informationssäkerhetsarbete samt därmed också säkerställa att kommunen lever upp till de krav som uppställs i Cybersäkerhetslagen och annan lagstiftning.

Administrativ, teknisk och fysisk säkerhet

Kommunens informationssäkerhetskrav innefattar såväl administrativ säkerhet som teknisk och fysisk säkerhet. Den administrativa säkerheten består av styrning, organisation, roller och ansvar, liksom regelverk, processer och systematik. En viktig del är också revision och uppföljning.

Den tekniska säkerheten är den delen som generellt beskrivs som IT-säkerhet. Här återfinns nätverk, servrar, arbetsstationer, hård- och mjukvara samt serverrum och utrymme för reservkraft, säkerhetskopior med mera.

Den fysiska säkerheten hör till stor del ihop med den tekniska säkerheten, och syftar till hur vi skyddar vår organisations materiel, system och personal rent fysiskt.

Kommunstyrelsens ansvar innefattar samtliga ovanstående delar.

Riskbaserat informationssäkerhetsarbete

För att upprätthålla ett informationssäkerhetsarbete som är aktuellt över tid ska nämnder och styrelser ha ett riskbaserat förhållningssätt i sitt informationssäkerhetsarbete. Det innebär att verksamheten genom riskanalyser ska identifiera, bedöma och följa upp de informationssäkerhetsrisker som kan uppstå i verksamheten.

Organisation, ansvar och roller

Samtliga anställda, förtroendevalda, elever, konsulter etc. omfattas av policyn och dess tillhörande styrdokument.

Kommunstyrelsen ansvarar enligt vad som framkommit ovan, för att ta fram och konkretisera denna policy genom informationssäkerhetsriktlinjer.

Den nämnd/styrelse som ansvarar för viss information kallas informationsägare. Informationsägaren ansvarar för att verksamhetens krav på informationssäkerhet fastställs genom informationsklassning.

Informationsägaren ansvarar för att resultatet från informationsklassningen tas omhand och efterlevs, exempelvis genom att tekniska säkerhetskrav som framkommit vid informationsklassningen överlämnas till digitaliseringsenheten och tas omhand vid upphandling.

Uppföljning

Kommunens informationssäkerhetsarbete ska årligen följas upp såväl inom kommunstyrelsen och samtliga nämnder som på övergripande nivå.