# STRATEGI

# Informationssäkerhetstrategi

**Dokumentets syfte**
Anger kommunens prioriteringar och strategiska vägval inom informationssäkerhet.

**Dokumentet gäller för**
Samtliga nämnder, enheter, produktionsverksamheter och kommunala bolag.

Denna *informationssäkerhetsstrategi* tydliggör Nacka kommuns prioriteringar och strategiska vägval för att uppnå en hög säkerhet för den information som kommunen hanterar i sin verksamhet (informationstillgångar). I styrdokumentet *Så här arbetar vi med informationssäkerhet i Nacka kommun* beskrivs det praktiska arbetssättet för att uppnå en hög informationssäkerhet.

**Informationssäkerhetsarbetet är den process som säkerställer att kommunens informationstillgångar hanteras på ett säkert sätt.**
**Informationssäkerhetsarbetet ska bidra till att uppfylla kommunens vision, grundläggande värdering och ambition.**

Information är en av kommunens viktigaste tillgångar och hanteringen av den är därför av avgörande betydelse för kommunens arbete. Med informationstillgångar avses all information oavsett om den behandlas manuellt eller med informationsteknologi.

*Visionen om öppenhet och mångfald* är Nacka kommuns grundpelare. Öppenhet innebär att utgångspunkten för hantering av informationstillgångar är att all information är tillgänglig för alla. Därmed är det centralt att den som hanterar information kan avgöra när den är skyddsvärd, till exempel på grund av sekretess eller att den omfattar personuppgifter. Mångfald ger stor valfrihet vid val av produkter för att skapa flexibla säkerhetslösningar.

Utifrån kommunens *grundläggande värdering* ska informationssäkerhetsarbetet präglas av förtroende för medarbetares och leverantörers förmåga att hantera informationstillgångar på ett säkert sätt. Det innebär också förtroende för att verksamheten skapar förutsättningar för ett effektivt informationssäkerhetsarbete.

*Ambitionen att vara bäst på att vara kommun* betyder för informationssäkerhetsarbetet hög kvalitet i hantering av information och att det ska finnas stöd som gör det lätt att




POSTADRESS Nacka kommun, 131 81 Nacka | BESÖKSADRESS Stadshuset, Granitvägen 15 | TELEFON 08-718 80 00 | E-POST info@nacka.se | SMS 716 80 | WEBB www.nacka.se | ORG.NUMMER 212000-0167

göra rätt. Kommunen tar ansvar för sina informationstillgångar genom att säkerställa att den egna verksamheten och leverantörer uppfyller ställda säkerhetskrav.

## Struktur för informationssäkerhetsarbetet

Informationssäkerhetsarbetet ska skapa förutsättningar att förena öppenhet och mångfald med säkerhet och robusthet.

### Styrning, stöd och samordning

- *Kommunstyrelsen* har det övergripande ansvaret för kommunens informationssäkerhet.
- *Stadsledningskontoret* har ansvar för att hålla ihop stödja, samordna och följa upp. Stadsledningskontoret ska säkerställa att det finns funktioner som har förmåga att stötta, samordna och följa upp informationssäkerhetsarbetet samt att det finns ett användarnära stöd
- *Varje nämnd* har ansvar för att informationstillgångar inom dess ansvarsområden hanteras enligt gällande lagstiftning och informationsstrategin.
- *Leverantörer* ansvarar för att leverans sker i enlighet med lagar och avtal.

Informationssäkerhetsarbetet ska vara uppbyggt så att det ska vara lätt att hantera information korrekt. Det innebär följande.

- Det finns lättillgänglig kunskap om informationssäkerhet och hur information ska analyseras för att avgöra om den behöver skyddas.
- Det finns utbildning som är tillgänglig för alla.
- Det sker en kontinuerlig uppföljning av upp hur information hanteras i verksamheterna.
- Det är säkerställt att det finns en förmåga att upprätthålla säker informationshantering och krishanteringsförmåga och att detta kontinuerligt övas och följs upp.
- Det sker en löpande utvärdering uppföljning av system och rutiner.

## Roller inom informationssäkerhetsarbetet

Alla verksamheter som hanterar informationstillgångar har ett ansvar för att informationssäkerheten upprätthålls.

- *Informationsägarna* har det övergripande och yttersta ansvaret för den information som används av ett eller flera system. Informationsägaren fattar de avgörande besluten om hur, av vem och vilken information som ska registreras samt om informationen behöver revideras eller gallras.
- *Systemägarna* har övergripande ansvar för respektive system och dess användning. Systemägaren ansvarar för att system uppfyller informationssäkerhetskraven i förhållande till verksamheten behov och för

att dess innehåll klassificeras. Systemägaren är vanligtvis den person som har det övergripande ansvaret för ett system.

- *Systemförvaltarna* har det funktionella (dagliga) helhetsansvaret för ett system. Systemförvaltaren fungerar som systemägarens utförare och ser till systemets funktionalitet samt att planerade och beslutade aktiviteter genomförs och upprätthålls.

## Prioriteringar för säker informationshantering

För informationssäkerhetsarbetet i kommunen gäller följande prioriteringar.

- Alla informationstillgångar klassificeras utifrån fyra aspekter. Vid klassificeringen ska konsekvenserna av en oönskad påverkan på informationens kvalitet bedömas.
    - *Tillgänglighet*: Information ska kunna nyttjas efter behov, i förväntad utsträckning och av rätt person med rätt behörighet.
    - *Riktighet*: Information ska vara korrekt, tillförlitlig och fullständig.
    - *Konfidentialitet*: Endast den med rätt behörighet ska kunna ta del av viss information.
    - *Spårbarhet*: Aktiviteter som rör informationen, till exempel bearbetning eller ändringar, ska kunna spåras.
- Systemsäkerhetsanalyser görs för att säkerställa att system uppfyller kraven för rätt nivå av skydd för informationstillgångar.
- Tekniska analyser, så som till exempel penetrationstester, genomförs kontinuerligt.
- Kontinuitetsplanering genomförs för att analysera hotbilden mot informationstillgångar och därmed förebygga händelser som kan leda till negativa konsekvenser för verksamheten och den enskilda individen.
- Riskanalyser genomförs för att identifiera och bedöma risker vars konsekvenser kan leda till störningar i tillgången till information, allvarliga händelser eller extraordinära händelser.
- Alla informationssäkerhetsincidenter anmäls till utpekad funktion och hanteras enligt en definierad incidentprocess.

---