STRATEGI
Informationssäkerhetsstrategi

Diarienummer	Fastställd/senast uppdaterad	Beslutsinstans	Ansvarigt politiskt organ	Ansvarig processägare
KFKS-2023-00210	Ange datum.	Kommunfullmäktige	Kommunstyrelsen	Stabschef
Strategi	Informationssäkerhetsstrategi			

Dokumentets syfte

Informationssäkerhetsstrategi säkerställer att Nacka kommuns prioriteringar och strategiska vägval uppnår en hög säkerhet för den information[1] som kommunen hanterar i sin verksamhet samt följer kommunens ambition och präglas av dess värderingar.

Dokumentet gäller för

Samtliga nämnder, enheter, produktionsverksamheter och kommunala bolag.

> Information finns i alla kommunens verksamheter och handlar om allt vi gör, exempelvis om vår personal, våra tjänster, vår ekonomi och det omgivande samhället med medborgare, företag, föreningar osv. Information är därför i sig en av kommunens viktigaste tillgångar.

Den ökade digitaliseringen skapar ett ökat it-beroende vars utsträckning behöver förstås och hanteras ur ett informationssäkerhetsperspektiv. För att skapa goda förutsättningar och god kvalitet i digitaliseringsprocessen krävs proportionerliga satsningar på informationssäkerhetsarbetet.

Informationssäkerhetsstrategin och kommunens styrmodell

Strategin bidrar till målet *stark och balanserad tillväxt* genom att skapa förutsättningar för trygghet och tillit för alla som lever och verkar i Nacka samt för Nacka kommun som organisation att möta en tilltagande digitalisering och utvecklingstakt. Detta skapar i sin tur hållbarhet, förutsägbarhet och förtroende vilket bidrar till målen *Attraktiva livsmiljöer* och *Bästa utveckling för alla.*

Ambitionen att vara bäst på att vara kommun och *Maximalt värde för skattepengar* uppnås genom att kommunens lösningar och tjänster är grundade i sunda säkerhetsbedömningar utifrån ett riskbaserat arbetssätt kring informationssäkerhet. Ett riskbaserat och kostnadseffektivt informations-

[1] informationstillgångar

säkerhetsarbete bidrar till målsättningen att vara bland de 10 bästa kommunerna när det gäller kvalitet och bland de 25 procent mest kostnadseffektiva.

Visionen om öppenhet och mångfald är Nacka kommuns grundpelare. För kommunens informationssäkerhetsarbete innebär visionen om öppenhet och mångfald att Nacka kommun alltid utgår från den aktuella informationens skyddsbehov och anpassar behandling och skyddsåtgärder efter interna och externa krav.

Utifrån kommunens *grundläggande värdering* ska informationssäkerhetsarbetet präglas av förtroende för medarbetares förmåga att hantera informationstillgångar på ett säkert sätt. Det innebär också förtroende för att verksamheten skapar förutsättningar för ett effektivt informationssäkerhetsarbete. Därmed är det centralt att den som hanterar information ges förutsättningar att avgöra dess skyddsvärde och när den är skyddsvärd.

Strategisk inriktning för kommunens arbete med informationssäkerhet

Informationssäkerhet är en förutsättning för kvalitet och tillförlitlighet i den kommunala verksamheten. Informationssäkerhetsarbetet i Nacka kommun ska skapa förutsättningar att förena öppenhet och mångfald med säkerhet, robusthet och respekt för den enskildes integritet.

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

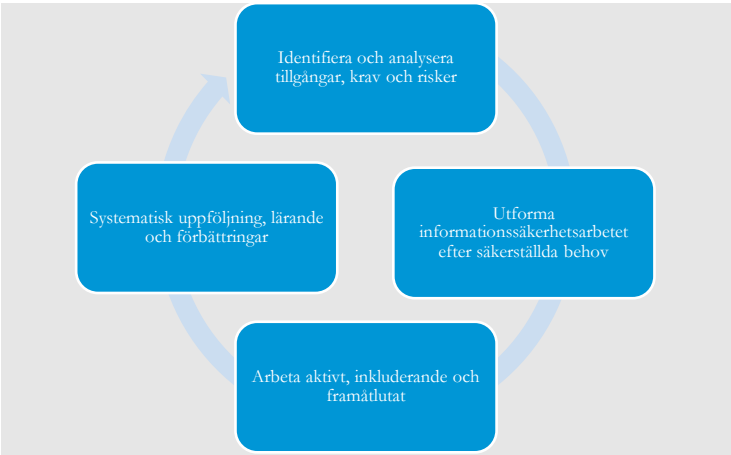
Nacka kommuns informationssäkerhetsarbete ska bedrivas systematiskt och riskbaserat. Det ska även finnas väl etablerade arbetssätt för att utforma och införa säkerhetsåtgärder som reducerar risker till en acceptabel nivå.

Arbetet ska präglas av ett förbyggande och proaktivt förhållningssätt, men också en god förmåga att kunna bidra i hanteringen av incidenter, allvarliga störningar och kriser [2].

Fyra strategiska inriktningarna som informationssäkerhetsarbetet ska bygga på

- identifiera och analysera tillgångar, krav och risker
- utforma informationssäkerhetsarbetet efter säkerställda behov
- arbeta aktivt, inkluderande och framåtlutat
- systematisk uppföljning, lärande och förbättringar

[2] Informationssäkerhetsarbetet i Nacka kommun ska bygga på en förmåga att kunna identifiera hot, sårbarheter och risker rörande våra informationstillgångar.



1. Identifiera och analysera tillgångar, krav och risker

Nacka kommun arbetar systematiskt med behovsanalyser[3] för att säkerställa att informationssäkerheten i verksamheten utformas med utgångspunkt i ett tydligt definierat nuläge. Analyserna identifierar kommunens informationstillgångar, förutsättningar, externa krav, risker samt intressenters behov.

2. Utforma informationssäkerhetsarbetet efter säkerställda behov

Det samlade resultatet från behovsanalyserna ska styra hur kommunens verksamheter utformar mål, handlingsplaner, säkerhetsåtgärder och prioriteringar inom informationssäkerhetsarbetet.

Kommunens verksamheter har ansvar för sin informationssäkerhet då de har bäst kunskap om hur känsliga och kritiska deras informationstillgångar[4] är. Att ha god kännedom om sin informationstillgång är grundläggande för att kunna bedöma dess skyddsvärde, behov av nödvändig dokumentation, styrning och krav vid upphandling samt förvaltning.

3. Arbeta aktivt, inkluderande och framåtlutat

Resultatet av handlingsplaner och konstaterade behov av säkerhetsåtgärder tas om hand av verksamheten på ett riskbaserat sätt för att prioritera och säkerställa ett systematiskt arbetssätt med tydligt uppsatta mål för informationssäkerhetsarbetet.

För att säkerställa ett riskbaserat arbetssätt genomförs informationsklassning för att värdera organisationens information utifrån dess konfidentialitet, riktighet och tillgänglighet. Informationsklassningen ska ske med en för kommunen enhetlig

[3] Behovsanalyserna utgörs av ett genomförande av verksamhetsanalys, omvärldsanalys, riskbild och gapanalys.
[4] Med informationstillgångar avses all information oavsett om den behandlas manuellt eller med informationsteknologi.

modell som anger olika nivåer av skyddskrav vari informationen ska klassas baserat på interna och externa krav.

Kommunen arbetar aktivt med att skapa och upprätthålla en god informationssäkerhetskultur. Inom ramen för detta arbete genomförs kontinuerligt informations- och utbildningsinsatser för att kunna nå och upprätthålla ett högt säkerhetsmedvetande.

4. Systematisk uppföljning, lärande och förbättringar

Verksamheten ska regelbundet följa upp efterlevnaden av sina mål, handlingsplaner, säkerhetsåtgärder[5] och prioriteringar för att säkerställa att avsedd verkan uppnåtts. Med avstamp i den regelbundna uppföljningen[6] samt resultatet av incidenthanteringen skapas ett nytt utgångsläge i det systematiska informationssäkerhetsarbetet. I det kontinuerliga lärandet och förbättrande arbetet är såväl incidenthantering som krisövningar en viktig del av kommunens utvecklingsarbete.

Verksamheterna följer årligen upp resultatet av föregående års informationssäkerhetsarbete vilket skapar en systematisk uppföljning som säkerställer styrningens lämplighet, tillräcklighet och verkan.

[5] Tekniska analyser, så som till exempel penetrationstester, sårbarhetsanalyser, och övervakning av IT-miljön, genomförs kontinuerligt för att utvärdera våra säkerhetsåtgärder.
[6] Uppföljningen utgörs av såväl erfarenheter från föregående års incidenter som resultatet av analysen av efterlevnaden.