

Beslutsfattare: Kommunstyrelsen

Beslutsdatum: 2009-06-23

Giltighetstid: Tillsvidare

## **POLICY FÖR IT-SÄKERHET I NYKÖPINGS KOMMUN**

## POLICY FÖR IT-SÄKERHET

IT ska användas för att bidra till hög kvalitet i verksamheten och drivas rationellt och kostnadseffektivt.

Tillgängligheten till IT-tjänster ska anpassas efter både verksamhetens och medborgarnas krav och behov.

Denna policy omfattar informationssäkerhet och policy för drift och förvaltning av Nyköpings kommuns informations- och IT-resurser.

Policyn beskriver Kommunstyrelsens vilja och mål för drift och förvaltning av Nyköpings kommuns IT-resurser och arbetet med informationssäkerhet. Policyn med tillhörande riktlinjer ska ge förtroendevalda, anställda, externa utförare och kontrakterad personal ett stöd kring informationssäkerhet i det dagliga arbetet på kommunen.

Policyn är fastställd av kommunstyrelsen och gäller från och med 2009-06-23.

Tillämpning av policyn beskrivs i Riktlinjer för IT-resurser inom Nyköpings kommun.

### 1 ROLLER OCH ANSVAR

Kommundirektören har det övergripande ansvaret för att verksamheterna i Nyköpings kommun tillämpar IT-policyn. Kommundirektören ansvarar även för samordning av arbetet med informationssäkerhet.

*Ansvarig för informationssäkerhet* utses av Kommundirektören

Under kommundirektören följer ansvaret linjeorganisationen.

*Systemägaren* utses av divisionschef eller chef för central enhet och är den som har ansvaret för att tillvarata verksamhetens krav. Systemägaren har det övergripande ansvaret för att IT-systemet stödjer verksamheten och verksamhetens mål. Systemägaren ansvarar även för IT-säkerheten i IT-systemet och för kontinuitetsplanen för det aktuella IT-systemet.

Kommundirektören utser systemägare för centrala system (system som driver infrastrukturen), IT-arkitektur i kommunens IT-miljö, säkerheten i Nyköpings kommuns centrala system och kommunikationsnät.

*Systemansvarig* utses av systemägaren och ansvarar för tilldelning av rättigheter för åtkomst till IT-systemet samt för uppföljning av de tilldelade rättigheterna. Tilldelning och uppföljning ska följa de riktlinjer som systemägaren har fastställt.

*Centrala Ledningslaget* beslutar om ägandet till IT-utrustning.

*IT-enheten* ansvarar för IT-infrastrukturen och standardisering av denna.

Anställda ansvarar för att följa det regelverk som finns kring IT-resurserna och informationssäkerheten. Alla anställda ansvarar för att ta del av sådan information och kunskap så att regelverket följs.

Var och en ska vara uppmärksam på och rapportera händelser som kan orsaka fel och brister i funktionalitet.

Den som använder kommunens informationstillgångar och IT-resurser på ett sätt som strider mot denna policy kan bli föremål för disciplinära åtgärder.

## **2 POLICY FÖR INFORMATIONSSÄKERHET**

### **2.1 Allmänt om informationssäkerhet**

Information är en av våra viktigaste tillgångar och hanteringen av den är en viktig del i arbetet.

Utgångspunkter i vårt arbete med informationssäkerhet är:

- Lagar, förordningar och föreskrifter
- Våra egna krav
- Avtal

Med informationstillgångar menas all elektronisk information, oberoende i vilken form eller miljö den förekommer.

Informationssäkerheten omfattar utan undantag Nyköpings kommuns elektroniskt lagrade informationstillgångar.

Med informationssäkerhet menas att uppnå rätt nivå av:

- tillgänglighet
- riktighet
- sekretess
- spårbarhet

Detta innebär att rätt information är tillgänglig för rätt person när den behövs, att den är spårbar och att informationen är och förblir riktig.

Informationssäkerheten är en integrerad del av verksamheten. Alla som hanterar informationstillgångar har ett ansvar att upprätthålla informationssäkerheten. Det är också ett ansvar för chefer på alla nivåer att aktivt verka för en positiv attityd till säkerhetsarbetet.

Var och en ska vara uppmärksam på och rapportera händelser som kan påverka säkerheten för våra informationstillgångar.

### **2.2 Mål**

För Nyköpings kommuns arbete med informationssäkerhet gäller att:

- förtroendevalda, anställda, personal hos externa utförare samt kontrakterad personal har kunskap om gällande regler för informationssäkerhet
- informationsförsörjningen är säker, effektiv och bidrar till ökat skydd. Den är ett stöd för förtroendevalda, anställda, personal hos externa utförare, kontrakterad personal, besökare och tredje man
- ingångna avtal är kända och följs
- förmågan att hantera krissituationer upprätthålls
- alla investeringar, både i form av information och teknisk utrustning har ett tillräckligt skydd
- det finns tillgång till en gemensam, säker och väl definierad infrastruktur för data- och telekommunikation

- hotbilden analyseras fortlöpande för varje enskilt informationssystem med betydelse för verksamheten,
- händelser som kan leda till negativa konsekvenser i informationssystemen förebyggs
- årliga mål för arbetet ska framgå av beslutad verksamhetsplan. För de årliga målen anges:
  - vad som ska göras under året och hur det ska göras
  - tidplan
  - behov av personella och ekonomiska resurser
  - när och hur uppföljning, utvärdering och avrapportering ska ske
- förtroendevalda och anställda ska fortlöpande informeras och utbildas i informations-säkerhet

## **2.3 Generella krav**

### **2.3.1. NYKÖPINGS KOMMUNS INFORMATIONSHANTERINGSSYSTEM**

Samtliga system ska vara identifierade och upptecknade. Av förteckningen ska framgå vem som är systemägare och systemansvarig. Alla system ska minst klara den basnivå som beskrivs enligt Krisberedskapsmyndighetens basnivå för informationssäkerhet BITS.

Vissa system är en förutsättning för att kunna bedriva Nyköpings kommuns verksamhet och för att kunna leverera tjänster till kommunens medborgare. För dessa ska en riskanalys upprättas med stöd av lämpliga verktyg för analys av informationssäkerhet. Analysen ska vara underlag för driftgodkännande.

### **2.3.2. UTBILDNING I INFORMATIONSSÄKERHET**

Förtroendevalda och anställda ska regelbundet utbildas så att informationssäkerheten upprätthålls.

### **2.3.3. INFORMATIONSKLASSNING**

Information som hanteras inom Nyköpings kommun ska klassificeras med avseende på sekretess, riktighet och tillgänglighet enligt organisationens klassningsmodell.

### **2.3.4. DISTANSARBETE**

För att medarbetare ska kunna arbeta effektivt ska möjlighet finnas att arbeta mobilt eller stationärt på distans. Förutsättningar och restriktioner för detta ska dokumenteras.

### **2.3.5. ANVÄNDNING AV INTERNET**

Vid användning av Internet exponeras Nyköpings kommun. Förutsättningar och restriktioner för användande av Internet ska dokumenteras.

### **2.3.6. INFORMATIONSOVERFÖRING**

Överföring av sekretessbelagd och övrig känslig information ska hanteras med gott omdöme, så att informationssäkerheten inte äventyras.

### **2.3.7. KONTINUITETSPLANERING**

För att bedriva verksamheten på en acceptabel nivå under både normala förhållanden och vid extraordinära händelser är kontinuitetsplaneringen av central betydelse. En kontinui-

tetsplan för driften av verksamheten ska finnas. Den ska vara baserad på de olika informationssystemens samlade krav och vara integrerad med övriga kontinuitetsplaner.

## **2.4 REVIDERING OCH UPPFÖLJNING**

Uppföljning genom årlig revision är en viktig del i arbetet med informationssäkerhet. Uppföljningen ska bevaka att:

- beslutade åtgärder är genomförda
- årliga mål är uppfyllda
- regler följs
- policyn för informationssäkerhet, säkerhetsinstruktioner och riskanalyser revideras vid behov.

## **3 POLICY FÖR DRIFT OCH FÖRVALTNING AV KOMMUNENS IT-RESURSER**

### **3.1 Allmänt om IT-resurser**

Med IT-resurser menas all IT- och telefoniutrustning, infrastruktur för data- och telefoni-kommunikation, IT- och verksamhetssystem och applikationer.

IT-investeringar ska göras effektivt och rationellt samt ha höga miljökrav.

IT kompetensen hos de anställda ska vara god så att kommunens IT resurser används effektivt.

I användningen av IT ska hänsyn tas till arbetsmiljön.

### **3.2 Mål**

För Nyköpings kommuns IT-resurser gäller att:

- samtliga anställda har god kunskap om gällande rutiner för användning
- miljöhänsyn ska tas i alla processer vid användning och investering av IT-resurser
- ingångna avtal (licens, upphandling) är kända och följs
- IT-resurser ägs centralt av IT-enheten i de fall då det bedöms som relevant
- alla investeringar i form av IT-resurser sker på ett kostnadseffektivt sätt
- det finns tillgång till en gemensam, säker, effektiv och väl definierad IT-infrastruktur
- händelser (incidenter) i IT-resurser som kan leda till konsekvenser för verksamheten förebyggs
- anställda informeras och utbildas kontinuerligt

### **3.3 IT-anskaffning**

IT-enheten ansvarar för att fastställa standard för hårdvara och system.

Beställning av IT-utrustning skall ske av behöriga beställare utsedda av divisionschef eller chef för centrala enheter.

Vid upphandling av system och applikationer svarar divisionen eller den centrala enheten för att systemet eller applikationen är godkänd av IT-enheten och för att IT-anskaffningen sker effektivt och rationellt.

### **3.4 Ansvar för verksamhetssystem och IT**

IT-enheten ansvarar för centrala system och för IT-infrastrukturen i kommunens samlade IT-miljö.

Divisionerna och de centrala enheterna ansvarar för sina verksamhetsspecifika system.

IT-enheten har ansvar för att systemen i kommunen konsolideras, standardiseras och samordnas inom och mellan divisionerna och de centrala enheterna.

För varje IT-system ska en systemägare, systemansvarig och tekniskt systemansvarig finnas utsedd.

### **3.5 Licens-hantering**

Kommunen ska uppfylla gällande lagkrav och ha god ordning på sitt licensinnehav .