

# **IT-säkerhetspolicy**

## **Danderyds kommun**

**September 2005**

**Boje Ericson**

# IT-säkerhetspolicy i Danderyds kommun

## Innehållsförteckning

<b>INNEHÅLLSFÖRTECKNING</b> .....	<b>2</b>
<b>1. ALLMÄNNA RIKTLINJER</b> .....	<b>3</b>
<b>2. MÅL MED SÄKERHETSARBETET</b> .....	<b>3</b>
<b>3. INRIKTNING AV SÄKERHETSARBETET</b> .....	<b>4</b>
<b>4. DEFINITIONER</b> .....	<b>4</b>
<b>5. ANSVAR</b> .....	<b>5</b>
5.1 KOMMUNSTYRELSEN .....	6
5.2 NÄMNDER .....	6
5.3 FÖRVALTNINGSCHEF.....	6
5.4 SYSTEMÄGARE.....	6
5.5 SYSTEMFÖRVALTARE.....	6
5.6 IT-SÄKERHETSANSVARIG.....	7
5.7 IT-AVDELNINGEN .....	7
5.8 LOKALA TEKNIKER .....	7
5.9 ANVÄNDARE.....	7
<b>6. SÄKERHETSdokUMENT - REGELVERK IT – REGELVERK TELEFONI</b> .....	<b>8</b>
<b>7. SÄKERHETSdokUMENT - INSTRUKTIONER FÖR ANVÄNDARE</b> .....	<b>8</b>
<b>8. INFORMATION - PUBLICERING</b> .....	<b>8</b>

## IT-säkerhetspolicy i Danderyds kommun

### 1. Allmänna riktlinjer

Behovet av snabb, säker och ändamålsenlig åtkomst har blivit i det närmaste en förutsättning för att användare skall kunna utföra sitt jobb på ett effektivt sätt. En förutsättning för åtkomst till systemen är att en god IT-säkerhet upprätthålls. IT-säkerhetspolicyn syftar till att höja kommunens allmänna säkerhetsmedvetande. Policyn utgör kommunens ramverk där ansvar, mål och ambitioner framgår. Samtliga kommunens IT-system och användare omfattas av policyn.

Säkerhet kostar pengar. *Det gäller därför att lägga säkerhetsribban på rätt nivå.* För att veta var rätt nivå är krävs särskilda riskanalyser för respektive verksamhet och system för att fastställa eventuella hotbilder. Man kan konstatera att otillräcklig nivå kan leda till ovälkomna händelser/incidenter och i värsta fall katastrof, medan en överdriven hög nivå kostar onödigt mycket i form av pengar och andra resurser.

Lagstiftningens krav och kraven från kommunens olika verksamheter gör att IT-verksamheten måste bedrivas så att:

- obehöriga ej kommer åt sekretessbelagda uppgifter
- obehöriga inte kan förvanska uppgifter i de olika systemen
- kommunen inte lider ekonomisk skada till följd av obehörigt intrång i olika system
- onödiga driftstopp inte uppkommer

Alla dessa krav gör att kommunen kontinuerligt måste bedriva ett aktivt IT-säkerhetsarbete. Kommunens IT-säkerhetspolicy anger grunden för detta arbete.

### 2. Mål med säkerhetsarbetet

IT-säkerhetsarbetet skall ha som mål att kommunens användare skall kunna använda IT-resurser utan oönskade störningar och med avsedd funktion.

Säkerhetsarbetet har som mer långsiktigt mål att

- säkerställa en god IT-säkerhet inom kommunen
- maximera tillgängligheten till befintligt nätverk
- maximera tillgängligheten till befintliga applikationer
- öka säkerhetsmedvetandet hos kommunens användare
- övervägande delen av alla användare skall få en introduktion i IT-säkerhet

Följande styrdokument skall finnas

- *IT-säkerhetspolicy*
- *Regelverk för IT*
- *Regelverk för Telefoni*
- *Instruktioner för användare*

Kommunstyrelsen fastställer IT-säkerhetspolicyn.

## IT-säkerhetspolicy i Danderyds kommun

Kommundirektören fastställer Regelverk för IT resp Telefoni.

Kommunens IT-strateg fastställer Instruktioner för användare.

Dokumentet skall finnas på kommunens Intranät och därmed vara tillgängliga för alla användare

### 3. Inriktning av säkerhetsarbetet

IT-säkerheten i kommunen skall säkerställa att information som överförs, lagras eller behandlas i kommunikationsnät, datasystem och datorer skall skyddas mot oavsiktlig, obehörig eller otillåten förändring eller förstöring samt obehörig eller otillåten åtkomst eller kopiering.

IT-säkerheten skall också säkerställa att kommunikationsnät, datasystem och datorer skyddas mot intrång, otillåten användning, stöld, skadegörelse och funktionsstörning.

Säkerhetsnivåer och skyddsåtgärder för IT-säkerheten skall utformas så att målen för IT-säkerheten uppnås till rimliga kostnader och utan att den dagliga verksamheten försvåras mer än nödvändigt.

Val och utformning av säkerhetsnivåer och skyddsåtgärder skall grunda sig på aktuell eller förväntad hotbild, på konsekvenserna av störningar för kommunen eller för anställda och allmänheten.

Bedömningar av hotbild och konsekvenser av störningar skall göras regelbundet och systematiskt.

Krav som ställs på IT-säkerhetsåtgärder ur verksamhetens perspektiv är t ex

- Efterlevnad av lagar, förordningar och avtal
- Säkerhetsutbildning
- Virussydd
- Beredningsplaner för avbrott och katastrof
- Fastställande av ansvar och befogenheter
- Rutiner för incidentrapportering

### 4. Definitioner

IT-säkerhet omfattar all säkerhet kring kommunens IT-verksamhet. Såväl administrativa som praktiska skyddsåtgärder avses. Till de administrativa åtgärderna kan räknas t ex IT-strategin, IT-säkerhetspolicyn, ansvarsfördelningen, bedömning av säkerhetsåtgärder, behörighetsregler, riskanalys och katastrofplan.

Driftmiljö, åtkomstskydd, behörighetsadministration, säkerhetskopiering m m betecknas som praktiska skyddsåtgärder.

## IT-säkerhetspolicy i Danderyds kommun

Information är en resurs som har ett värde liksom andra resurser i en organisation. Informationen måste därför få ett adekvat skydd. Informationssäkerhet syftar till att skydda information mot förekommande hot, förhindra avbrott i verksamheten och minska skador. Informationssäkerhet bidrar till att maximera värdet av organisationens resurser. IT-säkerhetsarbetet bidrar till detta.

Informationssäkerhet betyder

- *Tillgänglighet* till den information man som användare har rätt till
- *Riktighet* i den information som brukas, dvs säkerställer att data inte otillåtet ändras eller modifieras.
- *Sekretess* - endast användare med särskild behörighet har åtkomst till viss information, dvs säkerställer att ingen obehörig person kommer åt information
- *Spårbarhet* - kunna se vilka användare som gjort vad och när i respektive system

Informationssäkerhet är ett tämligen omfattande begrepp. Därför är det nödvändigt att fastställa vad som ingår och skall skyddas, dvs vad dessa dokument skall omfatta, nämligen

- data lagrat i/på databaser, band och skivor
- data sänt och mottaget via nätverk
- telefoni

För att nå framgång bör IT-säkerhetsarbetet kännetecknas av följande:

- *Lönsamhet* – de förslag som läggs fram skall löna sig att satsas på utifrån de analyser som genomförts med hänsyn tagen till säkerhetsbilden
- *Helhetssyn* – hänsyn skall tas till den komplicerade IT-verksamheten som finns och är integrerad inom hela kommunen
- *Systematik* – de åtgärder som vidtas skall vara väl genomtänkta, analyserade och beslutade

Genom att omvärlden hela tiden är i förändring krävs att IT-säkerhetsarbetet inom kommunen är en ständigt pågående process. Genom att följa upp arbetet med kontroller och revisioner kan uppdateringar och förändringar göras vid behov. Detta för att kunna upprätthålla en väl avvägd och kostnadseffektiv säkerhetsnivå.

### 5. Ansvar

*Den som har ansvar för en verksamhet har också ansvaret för säkerhetsfrågorna.* Det är även av stor vikt att organisationens ledning är engagerad i säkerhetsfrågorna om säkerheten skall kunna förbättras. Säkerhetsarbetet bör alltså styras från ledningen.

Alla användare skall, för att säkerhetsarbetet skall bli framgångsrikt, veta vem som har ansvaret för vad i organisationen och rollerna i säkerhetsarbetet.

För att kommunen skall kunna tillgodogöra sig de positiva effekterna av infört IT-stöd är det viktigt att ett aktivt säkerhetsarbete bedrivs. Framtagna lösningar skall präglas av automatik och integration. Det skall inte vara upp till varje användare/förvaltning att utifrån sina förutsättningar lösa säkerhetsproblematiken utan lösningarna skall administreras, styras och uppdateras från

## **IT-säkerhetspolicy i Danderyds kommun**

central nivå. Detta må också gälla beträffande övervakningen, dvs att beslutat regelverk efterlevs.

### **5.1 Kommunstyrelsen**

Kommunstyrelsen fastställer kommunens IT-säkerhetspolicy och ansvarar också för samordnings- och kontrollansvaret för IT-säkerhetsarbetet.

### **5.2 Nämnder**

Samtliga nämnder inom kommunen har ansvar för att gällande lagar och policies följs inom sina resp verksamhetsområden. Varje nämnd har huvudansvar för sin verksamhet och dess utveckling.

Nämnderna är enligt Personuppgiftslagen direkt personuppgiftsansvarig för personregister som förs för nämndens räkning.

### **5.3 Förvaltningschef**

Förvaltningschefen ansvarar för att personalen inom kontoret/förvaltningen får nödvändiga kunskaper för att IT ska kunna nyttjas på ett säkert och effektivt sätt.

De system som används inom en förvaltning har också förvaltningschefen ansvar för. Den som är chef för en verksamhet har också ansvaret för säkerhetsfrågorna.

### **5.4 Systemägare**

Alla system ska ha en systemägare som ansvarar för säkerheten i systemet. Detta ansvar kan delegeras till Systemförvaltaren.

Säkerhets- och skyddsåtgärder skall fastställas utgående från bedömning av hotbilden och av konsekvenserna av störningar. Skyddsåtgärder ska väljas så att nyttan är rimlig i förhållande till kostnaden för skyddet. Rutiner för förvaltning och datasäkerhetsarbete ska dokumenteras och kontinuerligt aktualiseras.

Varje Systemägare tar, utifrån sina egna unika förutsättningar, fram sina lokala handlingsplaner för att säkerställa sin förvaltning.

### **5.5 Systemförvaltare**

Med systemförvaltare avses den person, utsedd av Systemägaren, som dagligen styr verksamheten beträffande systemet.

## **IT-säkerhetspolicy i Danderyds kommun**

Systemförvaltaren har vanligtvis högre behörighet än vanliga användare av systemet. Rättigheterna och skyldigheterna skall ha tilldelats Systemförvaltaren genom beslut av systemägaren.

### **5.6 IT-säkerhetsansvarig**

IT-strategen är kommunens IT-säkerhetsansvarige som också svarar för efterlevnaden av utfärdade säkerhetsdokument. Denne har också ansvaret att se till att kontrollera att det säkerhetsmässiga regelverket följs.

### **5.7 IT-avdelningen**

IT-avdelningen samordnar kommunens IT-säkerhetsarbete.

IT-avdelningen ansvarar för virusprogram och brandväggar samt att varje dator i kommunens nätverk med automatik uppdateras med senaste version av virusprogram.

IT-avdelningen ansvarar för att dokumentation av nät och nätdelar föreligger och är uppdaterad till aktuell status.

Otillåten användning av kommunens datorer, som kommer till IT-avdelningens kännedom skall, genom IT-chefen, rapporteras till användarens förvaltningschef.

Delar av trafiken från och till datorer ska loggas regelmässigt. Stickprovskontroller av att information endast används av behörig personal skall ske. Överträdelser skall rapporteras till användarens förvaltningschef.

### **5.8 Lokala tekniker**

Lokala tekniker ansvarar för drift och förvaltning av lokala system och nätverk. Skall utrustning kopplas upp på det kommungemensamma nätverket krävs tillstånd från den centrala IT-avdelningen. Endast utrustning och datorer godkända av den centrala IT-avdelningen får användas.

### **5.9 Användare**

Anställda som utnyttjar IT i sitt dagliga arbete skall följa kommunens övergripande regler för IT-säkerhet och lokala regler för olika verksamhetssystem.

Alla användare skall vara väl informerade om IT-säkerhetsfrågornas betydelse så att de kan ansvara för att den personliga IT-användningen sker med bibehållande av hög säkerhet. Alla användare skall känna till Regelverk/Instruktioner så att de kan ta ett eget ansvar för IT-säkerheten vid den personliga IT-användningen.

## IT-säkerhetspolicy i Danderyds kommun

Alla personer som är verksamma inom kommunen skall rapportera incidenter till närmaste chef och/eller IT-säkerhetsansvarig.

Varje anställd inom kommunen ska ha kunskap om den informations-/IT-säkerhet som rör det egna tjänstestället och de informationssystem som används.

Den som åsidosätter informations-/IT-säkerheten kan allvarligt skada verksamheten, både vad gäller ekonomi och förtroendet för kommunens verksamhet. Därför är det viktigt att Regelverk och Instruktioner följs.

### 6. Säkerhetsdokument - Regelverk IT – Regelverk Telefoni

Som ett fortsatt steg i kommunens satsning på att höja säkerhetsmedvetandet har, utifrån IT-säkerhetspolicyn, två styrdokument för IT-säkerhetsarbetet, *Regelverk för IT resp Telefoni*, tagits fram. Dessa dokument innehåller bl a

- Regler för hur Internet får användas
- Regler för hur kommunens e-postsystem får användas
- Regler för hur den fasta telefonin skall hanteras
- Regler för hur den mobila telefonin skall hanteras

### 7. Säkerhetsdokument - Instruktioner för användare

Som ytterligare ett steg i kommunens satsning på att höja säkerhetsmedvetandet skall, utifrån IT-säkerhetspolicyn, ett styrdokument för IT-säkerhetsarbetet, *Instruktioner för användare*, tas fram. Detta dokument skall innehålla instruktioner på detaljnivå att utnyttja för användare, bl a

- Regler för hur nätverket får användas för att minimera riskerna att drabbas av virus
- Regler för hur virussyddet, -systemet skall administreras för att bli så optimalt som möjligt
- Regler för kommunens licenshantering
- Regler och riktlinjer för back-uptagning för i kommunen förekommande servrar
- Regler och riktlinjer för regelbundna restoretester för i kommunen förekommande servrar
- Regler för hur skolnätet skall administreras och förhålla sig till det administrativa nätet
- Regler och riktlinjer för hur användare får koppla in sig på det administrativa nätverket

### 8. Information - Publicering

Kommunens alla IT-säkerhetsdokument skall finnas samlade på Intranätet.