



# IT-Säkerhets- policy:



*Arvidsjaur kommun*



## IT-säkerhetspolicy

|   |          |
|---|----------|
| <b>1. IT-SÄKERHETSPOLICYNS ROLL I IT-SÄKERHETSARBETET .....</b> | <b>2</b> |
| <b>2. MÅL FÖR IT-SÄKERHETSARBETET .....</b>                     | <b>2</b> |
| <b>2.1 LÅNGSIKTIGA MÅL.....</b>                                 | <b>2</b> |
| <b>2.2 ÅRLIGA MÅL .....</b>                                     | <b>3</b> |
| <b>3. ORGANISATION .....</b>                                    | <b>3</b> |
| <b>3.1 ÖVERGRIPANDE ANSVAR.....</b>                             | <b>3</b> |
| <b>3.2 ORGANISATION, ROLLER OCH ANSVAR.....</b>                 | <b>3</b> |
| <b>4. SÄRSKILDA RUTINER .....</b>                               | <b>3</b> |

## 1. IT-SÄKERHETSPOLICYNS ROLL I IT-SÄKERHETSARBETET

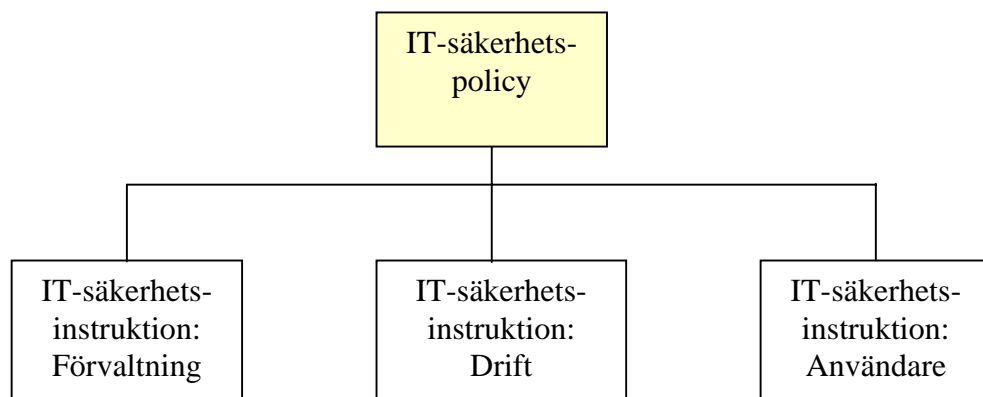
IT-säkerhet är en del i Arvidsjaurs kommuns lednings- och kvalitetsprocess som skall bidra till att ett IT-system kan användas på avsett sätt och med avsedd funktionalitet. Krisberedskapsmyndighetens (KBM) rekommendationer om basnivå för IT-säkerhet (BITS) skall gälla som ramverk för IT-säkerhetsarbetet.

Denna IT-säkerhetspolicy är en del av kommunens IT-verksamhet och redovisar kommunens viljeinriktning och stöd för IT-säkerhetsarbetet och syftar till att klarlägga:

- mål för IT-säkerhetsarbetet
- organisation, ansvar och roller inom IT-säkerhetsarbetet
- eventuella riktlinjer för områden som är av särskild betydelse

Policyn konkretiseras i IT-säkerhetsinstruktionerna:

- förvaltning
- drift
- användare



IT-säkerhetspolicy och IT-säkerhetsinstruktioner fastställs av kommunfullmäktige.

## 2. MÅL FÖR IT-SÄKERHETSARBETET

### 2.1 LÅNGSIKTIGA MÅL

För kommunens IT-säkerhetsarbete skall också gälla att:

- det stöder kommunens samlade utvecklingsarbete,
- det förebygger oväntade händelser i IT-systemen som kan leda till negativa konsekvenser,
- det säkrar en effektiv informationsförsörjning som bidrar till ökat skydd och stöd för medarbetare, samverkande partners, andra organisationer och tredje man,
- alla investeringar både i form av information (data) och teknisk utrustning skall skyddas i tillräcklig grad,
- kommunens information skall ses som en tillgång och skyddas i en grad som står i paritet med dess värde,
- det skall finnas tillgång till en gemensam, säker och väl definierad infrastruktur för extern och intern datakommunikation,
- kostnaderna för säkerhetsåtgärder skall vara rimliga i förhållande till risker.

De långsiktiga målen skall säkerställa att kommunen kan tillhandahålla relevant information som:

- är riktig, komplett och aktuell,
- efterfrågas och som kommunen har ett ansvar att tillhandahålla,
- endast delges behöriga personer och kan levereras vid rätt tidpunkt och till skäliga kostnader.

## **2.2 ÅRLIGA MÅL**

IT-säkerhetsarbetet skall också bedrivas så att det blir en integrerad del av kommunens normala verksamhet. *Årliga mål* för arbetet skall därför beslutas och framgå av verksamhetsplaneringen.

För de årliga målen bör anges:

- vad skall göras under året,
- behov av resurser för arbetet (personella och ekonomiska),
- tidplan (när och hur, sluttidpunkt),
- när och hur skall uppföljning, utvärdering och avrapportering ske,
- när och hur skall medarbetare informeras och utbildas.

## **3. ORGANISATION**

### **3.1 ÖVERGRIPANDE ANSVAR**

Det övergripande ansvaret för säkerheten i Arvidsjauras kommuns IT-verksamhet vilar på kommunfullmäktige.

### **3.2 ORGANISATION, ROLLER OCH ANSVAR**

Organisation, roller och fördelning av ansvar skall säkerställa att ett IT-system kan administreras och hanteras på ett sådant sätt att det under hela sin livstid bidrar till att stödja avsedd verksamhet och uppfylla IT-säkerhetspolicyns mål. Detta innebär att ett IT-system med alla dess delar är en resurs i en verksamhet på samma sätt som personal, lokaler, kontorsmaterial m.m.

Samtliga IT-system inom kommunen skall vara identifierade. Kommunstyrelsen godkänner dessa och utser systemägare för respektive IT-system. För dessa IT-system skall en systemsäkerhetsplan vara upprättad i enlighet med KBM:s IT-säkerhetsguide. Den interna organisationen för IT-säkerhetsarbetet, roller och fördelning av ansvar framgår av IT-säkerhetsinstruktion: Förvaltning.

## **4. SÄRSKILDA RUTINER**

Särskilda rutiner finns för tilldelning, uppföljning och uppdatering av behörighet, förvaring och avveckling av datamedia, e-post, Internet och distansarbete. Särskilda rutiner kan också vara aktuella för försöksverksamheter, prov och tester m.m. Rutiner för sådana områden framgår av IT-säkerhetsinstruktion Förvaltning.