



Söderköpings kommun

# Informationssäkerhetspolicy för Söderköpings kommun



## Innehåll

1	<b>Inledning</b>	3
2	<b>Mål för informationssäkerhetsarbete</b>	4
2.1	Långsiktiga mål	4
2.2	Årliga mål	5
3	<b>Organisation, roller och ansvar</b>	5
3.1	Övergripande ansvar	5
3.2	Roller och ansvar	6
	3.2.1 Systemägare	6
	3.2.2 Verksamhetsansvariga	6
	3.2.3 Systemansvarig	6
	3.2.4 IT-chef	6
	3.2.5 Systemtekniker	6
	3.2.6 Användare	6
	3.2.7 Informationssäkerhetsansvarig	7
	3.2.8 Informationssäkerhetssamordnare	7
3.3	Säkerhetsinstruktion	7
	3.3.1 Säkerhetsinstruktion Förvaltning	7
	3.3.2 Säkerhetsinstruktion Drift	7
	3.3.3 Säkerhetsinstruktion Användare	8
	3.3.4 Systemsäkerhetsplan	8
4	<b>Kontinuitetsplanering</b>	8
5	<b>Driftgodkännande av it-system</b>	8
6	<b>Revidering och uppföljning</b>	8



## 1 Inledning

Denna informationssäkerhetspolicy utgör det övergripande dokumentet för hur informationssäkerheten skall regleras inom Söderköpings kommun. Kommunfullmäktige har här reglerat ansvar och inriktning både beträffande befintliga system och system som kommer att installeras i framtiden.

Säkerhetsarbetet har sin utgångspunkt i rekommendationer och anvisningar från Myndigheten för samhällsskydd och beredskap, MSB. I rekommendationen BITS<sup>1</sup>, basnivå för informationssäkerhet, fastläggs grundkraven för en informationshantering som är en förutsättning för en organisations verksamhet.

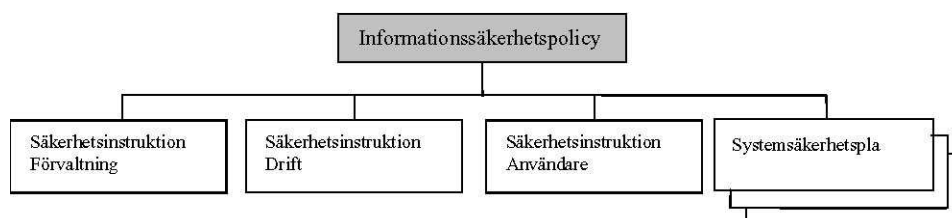
Bakgrunden till informationssäkerhetspolicyn är att informationshanteringen i systemen är en viktig förutsättning för att den dagliga verksamheten inom Söderköpings kommun skall fungera. Krav ställs på att systemen skall ha en hög tillförlitlighet, i vissa fall ställs också sekretesskrav och nästan alltid är hög tillgänglighet en förutsättning för att man skall kunna utföra sina arbetsuppgifter. Kommunen har dessutom en viktig roll i samband med svåra påfrestningar vid extraordinära händelser. Under dessa omständigheter kan det på vissa system ställas högre krav än normalt medan andra system inte kommer att behövas alls.

Informationssäkerhetspolicy är en del av organisationens it-verksamhet och redovisar ledningens viljeinriktning och stöd för informationssäkerhetsarbetet och syftar till att klarlägga:

- mål för informationssäkerhetsarbetet
- organisation, ansvar och roller inom informationssäkerhetsområdet
- riktlinjer för områden av särskild betydelse

Policyn konkretiseras i säkerhetsinstruktionerna:

- Förvaltning
- Drift
- Användare
- Systemsäkerhetsplaner



*Bild 1 Styrande dokument*

<sup>1</sup> BITS-konceptet är samlingsnamnet på MSB:s rekommendationer för hur en organisation kan ta ett helhetsgrepp på informationssäkerhetsarbetet.



Det är viktigt att poängtera att dessa dokument inte upphäver det normala linjeansvaret. Det är alltid nämnden/styrelsen som har det övergripande ansvaret för informationen i ett it-system. Dessa s.k. systemägare ansvarar för att basnivån för informationssäkerheten uppnås och att systemsäkerhetsplaner upprättas om systemen är samhällsviktiga/verksamhetskritiska. Systemsäkerhetsplanerna underlättar för den centrala it-driften eftersom här regleras vilka krav verksamheten ställer och vad som skall utföras.

Alla system skall driftgodkännas av verksamhetsansvarig för att verifiera att de krav som ställs också verkligen uppfylls.

Informationen är en av kommunens viktigaste tillgångar och hanteringen av den är en viktig del i arbetet. Med informationstillgångar avses all information oavsett om den behandlas manuellt eller automatiserat och oberoende av i vilken form eller miljö den förekommer. Kommunens informationstillgångar sammanfaller i princip med allmänna handlingar som regleras i grundlagen.

Informationssäkerhetspolicyn är kommunövergripande och gäller alla förvaltningar inom Söderköpings kommun.

## 2 Mål för informationssäkerhetsarbete

### 2.1 Långsiktiga mål

De långsiktiga målen för informationssäkerhetsarbetet är att säkerställa att Söderköpings kommun kan tillhandahålla relevant information som:

- endast delges behöriga personer och kan levereras vid rätt tidpunkt och till skäligen kostnader (*sekretess*)
- är riktig, komplett och aktuell (*riktighet*)
- efterfrågas och som organisationen har ett ansvar att tillhandahålla (*tillgänglighet*)
- inte medvetet eller omedvetet förstörs utan stöd i lag eller gallringsbeslut

*Målen för Söderköpings kommuns informationssäkerhetsarbete är att:*

samtliga samhällsviktiga och verksamhetskritiska it-system som finns inom organisationen ska vara identifierade och uppfylla basnivån för informationssäkerhet enligt BITS.

- för varje samhällsviktigt/verksamhetskritiskt it-system skall, utöver bassäkerheten, verksamhetsrelaterade krav och hotrelaterade krav fastställas i en systemsäkerhetsplan. Planen ska utgöra underlag för systemägarens beslut om driftgodkännande.
- säkerhetsåtgärder i it-systemen utformas och förvaltas på ett sådant sätt att kraven uppfylls enligt ovan
- en årlig uppföljning och kontroll av informationssäkerheten skall ske, bl.a. som underlag för verksamhetsplanering,



- alla system skall formellt driftgodkännas samt
- Söderköpings kommun skall kunna utföra sina uppgifter på ett tillfredsställande sätt även vid extraordinära händelser och höjd beredskap.

*För att uppnå dessa mål ska organisationens informationssäkerhetsarbete bedrivas så att:*

- lagar och föreskrifter följs
- det stöder organisationens 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 och tredje man
- alla investeringar både i form av information (data) och teknisk utrustning skyddas i tillräcklig grad
- organisationens information ses som en tillgång och skyddas i paritet med dess värde
- all personal ges kunskap om gällande informationssäkerhetsregler
- det finns tillgång till en gemensam, säker och väl definierad infrastruktur för extern och intern datakommunikation
- hotbilden för varje enskilt samhällsviktigt/verksamhetskritiskt it-system analyseras fortlöpande

## **2.2 Årliga mål**

Informationssäkerhetsarbetet ska bedrivas som en integrerad del av organisationens normala verksamhet. Årliga mål för arbetet ska därför beslutas och framgå av verksamhetsplaneringen.

För de årliga målen bör anges:

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

## **3 Organisation, roller och ansvar**

### **3.1 Övergripande ansvar**

Klart definierade ansvarsgränser och en tydlig organisation är en avgörande förutsättning för att Söderköpings kommun skall kunna leva upp till de krav som ställs i informationssäkerhetspolicyn. Säkerhetsansvaret följer den normala linjeorganisationen. Var och en, som är ansvarig för någon del av verksamheten, ansvarar också för informationssäkerheten inom sitt område.



### 3.2 Roller och ansvar

Organisation, roller och fördelning av ansvar ska 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 informationssäkerhetspolicyns mål. Detta innebär att ett it-system med alla dess delar är en resurs i en verksamhet på samma sätt som personal, lokaler, kontorsmaterial mm.

#### 3.2.1 *Systemägare*

Systemägaren är respektive nämnd/styrelse, vilka har det övergripande ansvaret för att systemet förvaltas på för verksamheten bästa sätt. Systemägaren fattar de avgörande besluten om ny-, vidareutveckling eller avveckling samt beslutar om säkerhetsplaner.

#### 3.2.2 *Verksamhetsansvariga*

Det operativa ansvaret för att it-systemen uppfyller verksamhetens krav vilar på verksamhetsansvarig, förvaltningschef. I detta ansvar ingår att bedöma den egna verksamhetens krav på säkerhet avseende sekretess, tillförlitlighet, tillgänglighet, spårbarhet samt att personalen har tillräckliga kunskaper för att hantera it-systemet på ett säkert sätt.

#### 3.2.3 *Systemansvarig*

Systemansvarig är en tjänsteman som utses av verksamhetsansvarig och har fått i uppdrag att bereda systemärenden samt att svara för administration, förvaltning och användning av ett it-system i verksamheten.

#### 3.2.4 *IT-chef*

IT-chef har det övergripande ansvaret för Söderköpings kommuns övergripande it-infrastruktur och att de olika it-systemens tekniska delar fungerar. IT-chef samverkar med verksamhetsansvarig vad avser drift och resursfördelning för respektive it-system.

#### 3.2.5 *Systemtekniker*

Systemtekniker innehar den tekniska kompetensen och ansvarar för att den dagliga driften upprätthålls enligt överenskommelse mellan verksamhetsansvarig och it-chef. Systemtekniker utgör utpekad person/personer på Söderköpings kommuns it-enhet.

#### 3.2.6 *Användare*

Varje användare ansvarar för att gällande regler och riktlinjer för informationssäkerhet följs. I detta ingår att noga ta del av och följa de säkerhetsregler som finns för de it-system den enskilde användaren använder.



### 3.2.7 *Informationssäkerhetsansvarig*

Informationssäkerhetsansvarig är kommunchefen.

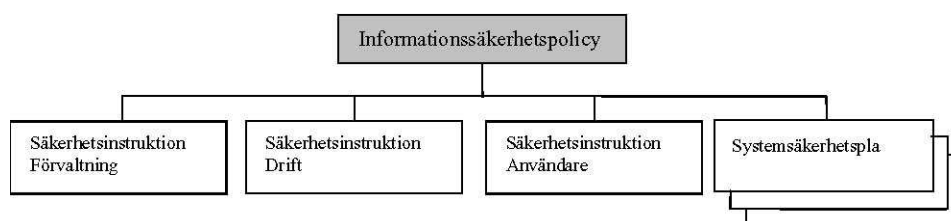
### 3.2.8 *Informationssäkerhetssamordnare*

Informationssäkerhetssamordnaren stödjer arbetet med att uppnå informationssäkerhetspolicyns mål.

Detta kan innebära aktivt deltagande i projekt, etablerande av interna och externa kontaktnät, utvärdering och deltagande i diskussioner kring metoder, plattformar eller it-system.

## 3.3 Säkerhetsinstruktion

Av säkerhetsinstruktionerna ska nedanstående områden och de särskilda riktlinjer, regler och rutiner som gäller för dessa framgå enligt följande:



### 3.3.1 *Säkerhetsinstruktion Förvaltning*

Informationssäkerhetsinstruktion förvaltning redovisar:

- det ansvar som ingår i de olika rollerna
- de riktlinjer som gäller för områden av särskild betydelse
- regler för systemutveckling, systemunderhåll, incidenthantering

Målgrupp: Systemägare, verksamhetsansvarig, systemansvarig och informations- säkerhetssamordnaren

*Fastställs av Kommunstyrelsen*

### 3.3.2 *Säkerhetsinstruktion Drift*

Informationssäkerhetsinstruktion drift redovisar:

- organisation och ansvar för drift av informationssystemen
- regler för säkerhetskopiering, lagring och driftadministration

Målgrupp: Systemansvariga, systemtekniker och it-chef.

*Fastställs av Kommunstyrelsen*



### 3.3.3 *Säkerhetsinstruktion Användare*

Informationssäkerhetsinstruktion användare redovisar:

- hur en användare ska verka för att upprätthålla en god säkerhet.

Målgrupp: Samtliga medarbetare.

*Fastställs av Kommunstyrelsen*

### 3.3.4 *Systemsäkerhetsplan*

- Reglerar krav som ställs på enskilda system som är samhällsviktiga/verksamhetskritiska.

*Fastställs av respektive systemägare*

## **4 Kontinuitetsplanering**

Av organisationens systemsäkerhetsplaner ska framgå de enskilda it-systemens krav på avbrotts- och katastrofplanering. Kraven ska vara sammanställda i systemsäkerhetsplanen för den tekniska infrastrukturen. Se Säkerhetsinstruktion Förvaltning.

## **5 Driftgodkännande av it-system**

Före verksamhetsansvarigs beslut om driftgodkännande ska en granskning göras för att kontrollera att säkerheten är tillgodosedd. Se Säkerhetsinstruktion Förvaltning.

## **6 Revidering och uppföljning**

Policy, Säkerhetsinstruktioner och Systemsäkerhetsplaner ska följas upp och vid behov revideras vid ny mandatperiod.