

## Landstingsstyrelsens förslag till beslut

---

### Informationssäkerhetspolicy för Stockholms läns landsting

Föredragande landstingsråd: Ingela Nylund Watz

#### Ärendet

Landstingskontorets förslag till informationssäkerhetspolicy för Stockholms läns landsting.

#### Förslag till beslut

Landstingsstyrelsen föreslår landstingsfullmäktige besluta

*att* anta informationssäkerhetspolicy för landstinget

*att* nu gällande IT-säkerhetspolicy skall upphöra att gälla.

#### Behandling i landstingsstyrelsen

Landstingsrådsberedningen behandlade ärendet den 29 januari 2003

Landstingsstyrelsen behandlade ärendet den 18 februari 2003.

#### Ärendet och dess beredning

**Landstingskontoret** har i tjänsteutlåtande den 27 november 2002 (bilaga) föreslagit landstingsstyrelsen föreslå landstingsfullmäktige besluta *att* anta informationssäkerhetspolicy för landstinget, *att* nu gällande IT-säkerhetspolicy, fastställd av landstingsfullmäktige i maj 1997, därmed skall upphöra att gälla.

#### Bilagor

- 1 Informationssäkerhetspolicy
- 2 Landstingskontorets tjänsteutlåtande

**Bilagor**

# **Informationssäkerhetspolicy**

**för**

**Stockholms läns landsting**



**Förslag**  
November  
2002

## **1 MOTIV**

Information är en viktig strategisk resurs för Stockholms läns landsting. En i alla avseenden tillförlitlig informationsförsörjning är avgörande för landstingets förmåga att uppnå sina verksamhetsmål. Den totala mängden information samt utbytet av information inom och mellan olika verksamheter i landstinget, med externa organisationer, allmänheten, förtroendevalda och andra intressenter, ökar i omfattning.

Det är därför mycket betydelsefullt att informationshanteringen skyddas från såväl avsiktliga som oavsiktliga störningar. Den information som rör enskilda personers sociala, medicinska och andra personliga förhållanden, måste skyddas noga mot såväl oönskad förändring som förlust och avslöjande. Detta gäller också den information som rör ekonomiska och andra verksamhetsspecifika uppgifter av betydelse.

Användningen av modern informationsteknik (IS/IT) skapar förutsättningar för landstinget att, genom hög tillgänglighet till information, klara behovet av effektiviseringar och att förbättra servicen till länets invånare. Beroendet av komplexa tekniska informationssystem innebär emellertid också ökad sårbarhet. Det är därför nödvändigt att, utifrån ett verksamhetsperspektiv, ställa rätt krav på säkerhetslösningar vid upphandling, utveckling och användning av informationssystem och att fortlöpande kontrollera att dessa krav efterlevs.

Denna policy beskriver de övergripande principer som skall gälla för informationssäkerheten i Stockholms läns landsting.

## **2 OMFATTNING**

Informationssäkerhetspolicyn gäller för all informationshantering i Stockholms läns landsting.

## **3 INNEBÖRD**

### **3.1 Skyddsområden**

Informationssäkerheten är den samlade effekten av organisatoriska, administrativa och tekniska åtgärder som vidtagas för att skydda informationen mot de hot den kan utsättas för. Åtgärder skall vidtas inom följande skyddsområden.

- **Tillgänglighet**, d v s skydd mot störningar som, avsiktligt eller oavsiktligt, innebär att behörig åtkomst till information ej kan tillgodoses i specificerad omfattning.
- **Konfidentialitet** (inkl sekretess och integritet), d v s skydd mot händelser eller åtgärder som, avsiktligt eller oavsiktligt, ger oönskad förändring, förlust eller avslöjande av information.
- **Riktighet** (kvalitet), d v s skydd mot händelser som gör information eller informationssystem olämpliga för sitt syfte.
- **Spårbarhet**, d v s åtgärder som innebär att händelser i en informationshanteringsprocess kan dokumenteras och utgöra underlag för analys och uppföljningar.

### 3.2 Skyddsåtgärder

För vart och ett av dessa skyddsområden skall organisatoriska, administrativa och tekniska skyddsåtgärder beskrivas och införas. Skyddsåtgärder skall dokumenteras på ett sådant sätt att praktiska möjligheter ges att kontrollera att erforderlig skyddsnivå uppnås.

Val av skyddsåtgärder skall vara verksamhetsanpassade och baseras på informationens betydelse och de konsekvenser som bristande säkerhet kan innebära för alla som är intressenter i en viss informationshantering. Lagar och förordningars krav skall utgöra lägsta nivå vid specificering av skyddsåtgärder.

## 4 ANSVAR

Ansvar för informationssäkerheten skall vara kopplat till det delegerade verksamhetsansvaret. Det betyder att varje person som är ansvarig för en verksamhet också är ansvarig för informationssäkerheten inom den verksamheten.

Landstingsfullmäktige fastställer den informationssäkerhetspolicy som skall gälla för landstinget.

Landstingsstyrelsen ansvarar enligt sitt reglemente för att landstingets informationssäkerhetspolicy och riktlinjer för informationssäkerheten utarbetas och hålls aktuella. Landstingsstyrelsen ansvarar också för samordningen av informationssäkerhetsarbetet i landstinget.

Landstingsstyrelsen och varje annan nämnd och styrelse är ansvarig för informationssäkerheten inom sitt verksamhetsområde och skall därför utarbeta och anta egna föreskrifter och instruktioner för informationssäkerheten i enlighet med den policy och de riktlinjer som landstingsfullmäktige och landstingsstyrelsen lämnat. Det åligger också nämnd/styrelse att avsätta medel för informationssäkerhetsarbetet samt att löpande följa upp informationssäkerheten och vidta åtgärder för att uppnå tillräcklig intern kontroll.

Landstingsrevisorernas uppgift är att granska att den interna kontrollen är tillräcklig.

Varje anställd ansvarar för att uppställda säkerhetsregler följs samt att funktionsstörningar och fel i informationssystem, utrustningar och informationsinnehåll rapporteras enligt fastställda rutiner.

För varje informationsmängd skall finnas en informationsägare som ansvarar för alla delar av informationssäkerheten d v s tillgänglighet, skydd mot obehörig åtkomst, spårbarhet och informationens riktighet.

För varje informationssystem skall finnas en systemägare som ansvarar för informationssystemets säkerhet. Systemägaren skall utse en systemförvaltare som ges uppdraget att, inom givna ekonomiska ramar, ta det funktionella ansvaret för informationssystemet.

Den som ingår avtal som leder till informationsanvändning eller informationsutbyte ansvarar för att kraven på informationssäkerhet specificeras i avtalet.

## **5 RIKTLINJER, FÖRESKRIFTER OCH INSTRUKTIONER**

Denna policy skall konkretiseras i riktlinjer, föreskrifter och instruktioner. Dessa dokument bör så långt möjligt utformas och inbördes ordnas i enlighet med vedertagen europeisk och svensk standard för informationssäkerhet.

### **Landstingskontoret**

Kontoret har anfört följande:

Stockholms läns landsting finansierar stora och informationsintensiva verksamheter, som drivs i egen regi eller av privata producenter, inom såväl vård- som trafikområdena. Politiska beslut och avtal mellan landstinget och producerande enheter är styrande för vad som utförs och hur detta görs.

Landstingsledningen har, med särskilt fokus på vårdens behov, initierat ett omfattande utvecklingsarbete som bl a skall resultera i ökad kvalitet i alla ärendeprocesser och därmed också effektivitet och kvalitet i enskilda verksamheter. En väl fungerande informationsförsörjning, där kraven på hög tillgänglighet till information samt informationens korrekthet, aktualitet och fullständighet, är en avgörande framgångsfaktor. Samtidigt ökar också kraven på att skydda informationen mot obehörig åtkomst, oönskad förändring, förlust eller avslöjande.

Som ett första steg i ambitionen att, utifrån en enhetlig syn på landstingets krav på säker informationshantering, underlätta för alla aktörer att ta sitt ansvar för säkerheten i informationsförsörjningen, har landstingskontoret utarbetat ett förslag till en informationssäkerhetspolicy för Stockholms läns landsting.

Förslaget till informationssäkerhetspolicy har remitterats för yttrande till landstingets samtliga förvaltningar och bolag samt till personalorganisationerna och de större privata vårdproducenterna. Av totalt 45 remissinstanser har 23 inkommit med synpunkter. Huvuddelen av dessa har varit uttalat positiva och de synpunkter som lämnats har i tillämpliga delar arbetats in i det slutliga förslaget. Flera remissinstanser har också påtalat behovet av att landstingskontoret snarast utarbetar landstingsgemensamma riktlinjer för informationssäkerheten som underlag för lokala föreskrifter och instruktioner.