

Föreskrifter för informationssäkerhet inom Kulturnämnden 2007

1 Ärendet

Landstingsfullmäktige har fastställt informationssäkerhetspolicy för Stockholms läns landstings. Utifrån policyn har landstingsstyrelsen fastställt Riktlinjer för informationssäkerhet. Utifrån policy och riktlinjer skall varje nämnd fastställa lokala föreskrifter för informationssäkerheten. I föreliggande ärende tar kulturnämnden ställning till kulturförvaltningens förslag till föreskrifter för informationssäkerhet inom kulturnämnden.

2 Förslag till beslut

Kulturnämnden föreslås besluta

att godkänna Föreskrifter för informationssäkerhet inom kulturnämnden 2007 att gälla tills vidare,

att uppdra till förvaltningschefen att göra erforderliga instruktioner till föreskrifterna,

att uppdra till förvaltningen att senast den 31 december 2007 rapportera till kulturnämnden hur informationssäkerhetsarbetet inom kulturförvaltningen genomförs,

att Riktlinjer år 2000 för IT-säkerheten inom kulturnämnden upphör att gälla.

Bilaga

1 Föreskrifter för informationssäkerhet inom kulturnämnden 2007

2 Landstingets informationssäkerhetspolicy

Stockholms läns landsting

2007-02-08

3 Bakgrund

Kulturnämnden beslutade om riktlinjer för informationssäkerheten år 2000 som uppdaterades år 2003. Därefter har landstingsfullmäktige och landstingsstyrelsen antagit policy och riktlinjer. Landstingsfullmäktige antog 2003-11-11 informationssäkerhetspolicyn för SLL och landstingsstyrelsen (Ls) antog därefter, 2003-12-16, Riktlinjer för informationssäkerhet. I det senare dokumentet sägs bl a att ”Varje nämnd och styrelse är ytterst ansvarig för informationssäkerheten inom förvaltning respektive bolag. De ska därför anta egna föreskrifter för informationssäkerheten, i enlighet med informationssäkerhetspolicyn och dessa riktlinjer.”

Kulturnämnden har tidigare inte antagit några föreskrifter grundade på Ls:s riktlinjer från december 2003. Många andra verksamheter inom landstinget har, liksom kulturförvaltningen, haft svårt att översätta Ls:s riktlinjer till föreskrifter som passar den egna verksamheten. Kulturförvaltningen har under 2006 medverkat i ett landstingsövergripandenätverk som leds av landstingsstyrelsens förvaltning (LSF) rörande informationssäkerhetsarbetet.

Enligt Ls:s riktlinjer ankommer det på kulturnämnden att besluta om föreskrifter och förvaltningschefen att fastställa instruktioner om så erfordras. De riktlinjer som kulturnämnden fastställde 2003 föreslås upphöra och ersättas med föreslagna föreskrifter (bilaga 1).

4 Sammanfattning av landstingsstyrelsens riktlinjer för informationssäkerhet inom landstinget

Ls:s riktlinjer omfattar **all information** och informationshantering från utvecklingsarbete till löpande produktion och arkivering och oavsett hur den hanteras, digitalt, tryckt eller muntligt framförd. I praktiken finns i dag i stort sett all information digitalt varför informationssäkerhetsarbetet i huvudsak handlar om säkerhetsrutiner inom IT-området.

Riktlinjerna innehåller en informationssäkerhetsorganisation som reglerar ett antal funktioner eller ”roller” som skall finnas inom varje förvaltnings och bolag för att säkerställa informationen.

Som nämns ovan är **nämnd** ytterst ansvarig för informationssäkerheten inom förvaltningen. Det åligger varje nämnd att utfärda egna föreskrifter och sätta av medel för informationssäkerhetsarbetet. Nämnden kan utse personuppgiftsansvarig (se nedan).

2007-02-08

LS:s riktlinjer beskriver dels hur olika funktioner och roller skall fördelas i en informationssäkerhetsorganisation (avsnitt 2), dels hur säkerhetsarbetet skall bedrivas (avsnitt 3 – 11) inom områdena:

- Hantering av tillgångar och risker
- Åtkomst till information
- Driftsäkerhet
- Kommunikations- och nätverkssäkerhet
- Systemutveckling och –anskaffning
- Fysisk säkerhet
- Personal- och informationssäkerhet
- Kontinuitetsplanering
- Uppföljning och efterlevnad

Vad gäller säkerhetsorganisationen säger riktlinjerna sammanfattningsvis följande.

Förvaltningschefen ansvarar för att kommunicera föreskrifter och om så behövs, utfärda interna instruktioner till föreskrifterna m m.

Personuppgiftsombud:

Personuppgiftsombudet har till uppgift att tillse att personuppgifter behandlas på ett lagligt sätt. Ombudet skall anmäla missförhållanden som inte åtgärdas till Datainspektionen som är tillsynsmyndighet vad gäller behandling av personuppgifter. Genom att utse personuppgiftsombud behöver varje IT-system som innehåller personuppgifter inte anmälas till Datainspektionen.

Informationssäkerhetssamordnare:

Inom varje förvaltning skall det utses en Informationssäkerhetssamordnare som bl a koordinerar säkerhetsarbetet och följer upp efterlevnaden av policy, riktlinjer, föreskrifter och instruktioner. Informationssäkerhetssamordnaren skall rapportera till förvaltningschefen och vara kontaktperson mot landstingets informationssäkerhetschef.

Informationsägare:

För varje viktig informationstillgång skall det utses en Informationsägare som bl a skall klassificera informationen, göra riskanalyser samt ansvarar för användares åtkomsträttigheter.

Systemägare:

För varje IT-system skall det utses en systemägare som bl a skall besluta om utveckling, avveckling av systemet i fråga. Systemägaren skal utforma rutiner så att t ex incidenter och funktionsfel i systemet analyseras. Vid behov

2007-02-08

kan systemägaren utse **Systemförvaltare** till vilken det praktiska arbetet kan delegeras genom en dokumenterad förvaltningsöverenskommelse.

IT-chef/samordnare:

Ej obligatoriskt att inordna denna befattning enligt Ls:s riktlinjer. Däremot förutsätts de arbetsuppgifter som anges för funktionen bli utförda även om särskild tjänst inte tillsätts.

Informationsanvändare:

Varje person som i sin yrkesutövning hanterar information inom landstinget är Informationsanvändare.

Därutöver säger riktlinjerna att det kan inrättas ett **informationssäkerhetskollegium** för att samordna uppföljningen av att informationssäkerheten bedrivs effektivt.

5 Förvaltningens synpunkter

Ls:s riktlinjer förutsätter att ovan beskrivna roller innehas av olika individer inom förvaltningen. T ex så skall Informationssäkerhetssamordnaren ansvara för att följa upp att föreskrifter och instruktioner följs. Informationssäkerhetssamordnaren bör därför inte själv ha andra roller i informationssäkerhetsarbetet. Riktlinjerna förutsätter även att Systemägare och Informationsägare är olika individer.

Flertal medarbetare inom kulturförvaltningen arbetar inom konstverksamheten, bereder ärenden rörande kultur- och föreningsstöd, arbetar inom läns-hemslöjdskonsulentverksamheten eller med annat kulturinriktad verksamhet (Film Stockholm och Circonova). Ca en femtedel av personalen arbetar med gemensam administration så som ekonomi, IT, information och registrering/nämndsekretariat. Förutom förvaltningschefen, finns det ytterligare fem medarbetare med chefs-/arbetsledaransvar (exkl SLIF-kansliet som utgör kansli åt landstingets idrottsförbund).

Enligt förvaltningens mening är det inte praktiskt möjligt att fördela alla de funktioner som Ls:s riktlinjer anger på olika personer. Det skulle innebära att ett stort antal av medarbetarna skulle inta roller inom informationssäkerhetsarbetet som de inte har vare sig formell kompetens eller personliga egenskaper/intresse för att klara av och som dessutom skulle kräva tid som inte finns tillgänglig i dag. Ett alternativ är naturligtvis att inrätta nya befattningar och på så sätt utöka antalet anställda och skapa erforderligt utrymme och kompetens för att kunna arbeta enligt riktlinjerna. Förvaltningen före-

2007-02-08

slår dock inte detta som en förstahandsåtgärd i föreliggande utlåtande. I vissa avseenden kan det även ifrågasättas om säkerhetsarbetet inom kulturnämndens ansvarsområde kräver en sådan omfattning som anges i riktlinjerna; Kulturförvaltningen hanterar t ex inga sekretessbelagda uppgifter eller uppgifter som är av vitalt intresse för liv och hälsa eller allmänhetens säkerhet. Naturligtvis skall den information som framställs inom förvaltningen säkras så att inte obehörig kan ändra informationens innehåll men arbetet måste organiseras på ett förenklat sätt – anpassat till verksamhetens art, informationens innehåll, befintlig organisation inom kontoret och tillgängliga resurser i form av befintlig personal, deras kompetens samt ekonomiska medel.

Förvaltningen föreslår därför att kulturnämndens föreskrifter för informationssäkerhet bygger på ett förenklat förfarande jämfört med Ls:s riktlinjer vad avser Informationssäkerhetsorganisationen genom att ansvaret för säkerhetsarbetet i huvudsak följer ordinarie sk linjeorganisation inom förvaltningen. Det innebär att varje enhetschef/motsvarande ansvarar för informationssäkerheten i de system som används inom ansvarig enheten. Även med denna något förenklade ansvarsorganisation ställer riktlinjerna och föreskrifterna för informationssäkerhet krav på ett omfattande kontinuerligt säkerhetsarbete enligt avsnitten 3 – 11 i riktlinjerna.

Sammanfattningsvis innebär förvaltningens förslag till informationssäkerhetsföreskrifter följande.

5.1 Informationssäkerhetsorganisationen

Förvaltningschefen fastställer vilka befattningshavare som ingår i informationssäkerhetsorganisationen.

5.1.1 Personuppgiftsansvarig och personuppgiftsombud

Kulturnämnden är personuppgiftsansvarig. Nämnden utser personuppgiftsombud (behandlas i KUN senare under våren 2007).

5.1.2 Informationsägare och Systemägare

Förvaltningschefen utser informationsägare och systemägare för varje IT-system som används. Informationsägare och systemägare kan vara samma person. Som informationsägare och systemägare utses vanligtvis ordinarie enhetschef. Det praktiska arbetet som systemägare kan delegeras till systemförvaltare som utses av respektive systemägare

2007-02-08

5.1.3 *IT-chef/samordnare och Informationssäkerhetssamordnare*

Förvaltningschefen utser vem som skall fullgöra de uppgifter som enligt riktlinjerna ankommer på IT-chef/samordnare och Informationssäkerhetssamordnare. Särskilda befattningar för dessa funktioner inrätta ej. Med nuvarande arbetsorganisation kommer chefen för kanslienheten att utses. Eftersom chefen för kanslienheten även kan komma att utses till informationsägare och systemägare av system som i huvudsak används inom kanslienheten, kan chefen för kanslienheten komma att inta fyra olika roller i informationssäkerhetsorganisationen – en ordning som således inte stämmer överens med Ls:s riktlinjer.

För att genomföra säkerhetsanalyser och följa upp genomförandet av riktlinjer och föreskrifter för informationssäkerheten föreslår förvaltningen att externa konsulter används. Inte minst riskanalyser kräver särskild kompetens som inte finns inom förvaltningen. Samtidigt är användandet av externa konsulter förenat med kostnader. F n genomförs en riskanalys av konstdata-basen med hjälp av konsult som LSF tillhandahåller utan kostnader för kulturförvaltningen som en del i ett pilotprojekt rörande riskanalys inom ramen för det nätverksarbete som nämnts i avsnitt 3 ovan. Kostnader för konsultstöd vid riskanalys av samtliga system kan f n inte uppskattas. Förvaltningen har ett 20-tal IT-system.

Förvaltningen anser att den information som produceras inom förvaltningen normalt skall ges den lägsta säkerhetsklassificeringen. Undantaget är i första hand ekonomisystemet som bör ges en högre säkerhetsklass.

5.2 **Föreskrifternas utformning**

Förvaltningens förslag till informationssäkerhetsföreskrifter för kulturnämnden är integrerade i dokumentet med Ls:s riktlinjer för informationssäkerhet (bilaga 1). Kulturnämndens föreskrifter utgörs av innehållet i de texturor som finns i dokumentet. Därigenom hoppas förvaltningen att läsaren skall ha större möjlighet att koppla samman innehållet i kulturnämndens föreskrifter med Ls:s riktlinjer.

5.3 **Åtterrapporering till kulturnämnden**

De uppgifter som förtecknas i Ls:s riktlinjer och förslaget till föreskrifter för kulturnämnden är mycket omfattande även om vissa förenklingar gjorts i kulturnämndens föreskrifter vad avser informationssäkerhetsorganisationen. I dagsläget har förvaltningen svårt att bedöma hur omfattande de kontinuerliga arbetsuppgifterna blir inom informationssäkerhetsområdet. Förvaltningen kan därför inte med säkerhet säga att riktlinjer och föreskrifter kan följas

2007-02-08

utan personella förstärkningar. Kulturnämnden föreslås därför uppdra till förvaltningen att senast den 31 december 2007 rapportera till kulturnämnden hur informationssäkerhetsarbetet inom kulturförvaltningen genomförs.



Hans Ullström