DANDERYDS KOMMUN
Kommunledningskontoret
Lars Winberg

Tjänsteutlåtande
2011-03-16
Rev. 2011-08-12

KS 2010/0096

Styrdokument för informationssäkerhet 2011-2014

Informationssäkerhet är en del i kommunens hantering av verksamhetens information.

I föreliggande förslag till styrdokument för informationssäkerhet finns dels en policy för arbetet med informationssäkerhet, dels strategier för insatser kopplade till kommunens övergripande mål. Dokumentet anger vidare hur ansvarfrågorna föreslås hanteras och vilka de viktigare rollerna är i informationssäkerhetsarbetet.

Det övergripande styrdokumentet ska följas av informationssäkerhetsinstruktioner för förvaltningar och för kontinuitets- och driftsarbete. För den enskilda användaren finns instruktioner på användarnivå.

Förslaget till styrdokument för informationssäkerhet har tagits fram av säkerhetschefen i samarbete med IT-chefen och informationschefen. Förvaltningscheferna har beretts tillfälle att komma med synpunkter på förslaget.

Vid kommunstyrelsens sammanträde 2011-04-14 återremitterades ärendet till kommunstyrelsens arbetsutskott för vidare beredning. Förslaget till styrdokument har därför förändrats jämfört med tidigare förslag.

Kommunledningskontorets förslag till beslut
Kommunstyrelsen föreslår kommunfullmäktige besluta

1 Kommunfullmäktige godkänner Styrdokument för informationssäkerhet 2011-2014.

Johan Haesert
Kommundirektör

Lars Winberg
Säkerhetschef

Bilagor:
1. Styrdokument för informationssäkerhet 2011-2014, daterat 2011-08-12

Expedieras:
Samtliga nämnder.

DANDERYDS KOMMUN

2011-08-12

STYRDOKUMENT FÖR INFORMATIONSSÄKERHET 2011-2014

Text med kursiv stil är tillägg sedan behandlingen i KS i april 2011.

1. Bakgrund

Detta dokument fastställs av kommunfullmäktige och gäller för all verksamhet inom kommunen. Detta betyder att det inte finns utrymme att besluta om lokala regler som avviker från detta.
Informationssäkerhet är den del i organisationens lednings- och kvalitetsprocess som avser hantering av verksamhetens information och styrdokumentet redovisar ledningens viljeinriktning och mål för arbetet med informationssäkerhet.

Styrdokumentet har tagits fram utifrån MSBs (tidigare Krisberedskapsmyndighetens) rekommendationer. Dessa grundar sig i sin tur på internationella standards med den svenska beteckningen SS-ISO/IEC 17799.

2. Allmänna synpunkter

Syftet med detta dokument är att fastställa en övergripande policy, strategi, roller och ansvar för en basnivå kring informationssäkerhet. Med informationstillgångar avses all information oavsett om den behandlas manuellt eller automatiserat och oberoende av dess form eller miljö den förekommer i.
Informationssäkerheten omfattar kommunens informationstillgångar utan undantag. *Med informationstillgångar menas både information och de resurser som används för att hantera informationen. Informationssäkerhet handlar därmed om mer än att säkra informationssystem. Även andra resurser, inte minst människors förmåga, är viktiga komponenter i informationssäkerhetsbegreppet.*

Begreppet informationssäkerhet innebär – säkerhet för informationstillgångar avseende förmåga att upprätthålla önskad konfidentialitet, riktighet, tillgänglighet och spårbarhet.

Informationssäkerhet är ett medel som bidrar till att uppnå kommunens övergripande mål.

Konkreta insatser för att koppla kommunens mål till informationssäkerheten är närmare beskrivna i avsnittet "Strategi".

3. Policy

Det som sägs under rubriken Policy är av övergripande karaktär. I ett kommande dokument kommer instruktioner för informationssäkerhetsarbetet att visa hur denna policy ska tillämpas.

Kommunens informationssystem
Informationssystem definieras som ett system som samlar in, lagrar, bearbetar och distribuerar information och som därigenom stödjer kommunikation inom och mellan organisationer. Samtliga informationssystem ska vara identifierade och förtecknade. Av förteckningen ska framgå vem som är systemägare. För de informationssystem som stödjer kommunens

samhällsviktiga verksamhet *och för system som krävs för att kommunen ska uppfylla krav på samhällsservice* ska en riskanalys upprättas. Analysen ska utgöra grund för driftgodkännande.

Informationsklassning
Klassificering av information är en grundläggande aktivitet för att information och resurser ges nödvändigt skydd.

Informationen ska klassificeras utifrån den funktion och betydelse för verksamheten som den har och de konsekvenser det medför om informationen skulle hanteras felaktigt, försvinna eller komma i orätta händer.

Information som hanteras i kommunen ska klassificeras med avseende på sekretess, riktighet, tillgänglighet och spårbarhet.

Elektronisk post
Sekretessbelagd information får inte skickas via e-post.

Distansarbete
För att personalen ska kunna arbeta effektivt ska möjlighet finnas att arbeta mobilt eller stationärt på distans. Förutsättningar och restriktioner för detta ska dokumenteras.

Internet
Vid användning av internet exponeras kommunens namn och av detta skäl är det därför av vikt att med omdöme avgöra vilka hemsidor som får besökas. *Hemsidor med rasistiskt, våldsinriktat eller sexuellt innehåll får inte besökas. Undantag från detta kan beviljas av chef om informationen på sådana sidor kan ha relevans för arbetsuppgifterna.*

Loggning
Alla aktiviteter i kommunens informationssystem ska loggas. Detta för att eventuellt missbruk ska kunna upptäckas men även för att kunna spåra och åtgärda fel i systemen.

4. Strategi

Strategiska insatser för informationssäkerhetsarbetet
Följande konkreta insatser är prioriterade och grupperas efter kommunens mål enligt nedan.

Bra och attraktiv kommun
Verksamhetsprocesser med medborgaren, brukaren och näringslivet i centrum

- Informationsförsörjningen ska vara säker, effektiv och bidra till ökat skydd för medarbetare, kommunens partners och tredje man.
- Händelser i informationssystemen som kan leda till negativa konsekvenser för kommunens verksamhet förebyggs. Beskrivs i "Informationssäkerhetsinstruktion för Kontinuitet och Drift".

Danderyds kommun säkerställer också verksamhetsprocesser med medarbetaren i centrum genom följande åtgärder

- Personalen har kunskap om gällande informationssäkerhetsregler som rör det egna tjänstestället och de informationssystem som där används. Beskrivs i "Informationssäkerhetsinstruktion för Användare"
- Krishanteringsförmågan upprätthålls och är hög. Beskrivs i "Informationssäkerhetsinstruktion för Kontinuitet och Drift".
- Bedömningar av hotbild och konsekvenser av störningar i de digitala systemen görs regelbundet.

<u>God ekonomisk hushållning och låg kommunalskatt</u>

Metoder och riktlinjer

- Säkerhetsnivåer och skyddsåtgärder säkerställs och utformas så att säkerheten kan uppnås till rimliga kostnader.
- Ingångna avtal ska vara kända och följas. Ordning och reda och gemensamma riktlinjer för avtalshantering och bevakning är grunden för detta. Brister leder till förlust av kapital.
- Investeringar i form av digitala- och mobila system och teknisk utrustning anpassas till krav för skydd och säkerhet i tillräcklig grad.

Styrning och organisation av informationssäkerheten

Drift och kontinuitetsplanering

För att motverka konsekvenserna vid en kris eller ett allvarligt avbrott i framför allt de samhällsviktiga verksamheterna, måste kontinuitetsplaner göras. Informationssäkerhetens roll i dessa är att säkerställa att inte störningar i informationssystemen ger upphov till avbrott i dessa verksamheter. Skulle avbrott ändå ske ska bl.a. informationssäkerhetsrutiner se till att ett så snabbt återställande av de samhällsviktiga verksamheterna sker.

Ansvar och roller

Systemförvaltningens organisation utgörs i huvudsak av rollerna systemägare, systemförvaltare och säkerhetschef.

Roller

- **Kommunstyrelsen** har det politiska ansvaret för styrdokument för informationssäkerhet och att detta följs.
- **Kommundirektören** har det övergripande ansvaret för informationssäkerheten och är ansvarig för att systemägare utses för respektive informationssystem.
- **Säkerhetschefen** utses av och är direkt underställd kommundirektören samt har det operativa ansvaret för samordning av informationssäkerhetsarbetet.
- **Systemägaren** är den som har ansvaret för den verksamhet som aktuellt informationssytem stödjer.
- **Informationsägaren** har det övergripande och yttersta ansvaret för den information som används av ett eller flera system. Denna roll finns i allmänhet bara i stora system som berör flera verksamheter.
- **Systemförvaltaren** utses av respektive systemägare och ansvarar för den dagliga användningen av informationssystemen samt för utbildning av användare av systemen.
- **IT-chefen** ansvarar för att uppfylla kommunens kontinuitetsplan för IT-stödet.
- **Användare** ska följa kommunens regelverk för informationssäkerhet och rapportera störningar och/eller fel i systemen till systemförvaltaren för systemet. Incidenter ska rapporteras till säkerhetschefen.

- **Extern tjänsteleverantör** ansvarar för att produktionsmiljö, dator- och kringutrustning uppfyller kommunens säkerhetskrav och ska samråda med säkerhetschefen i informationssäkerhetsfrågor. Leverantören ska ha en utsedd person ansvarig för säkerhetsfrågor.

5. Uppföljning

Detta dokument är giltigt t o m 2014-12-31. Dokumentet skall revideras vid behov. Uppföljning och dokumentation är en avgörande del av informationssäkerhetsarbetet. Uppföljningen skall bevaka:

- Att beslutade åtgärder är genomförda
- Att årliga mål är uppfyllda
- Att instruktioner följs
- Att systemsäkerhetsplaner och styrdokument revideras vid behov
- Att 16 principer för samverkan i IT-frågor i Stockholms län tillämpas. (KS 2010-06-14)

6. Koppling till andra dokument

Detta styrdokument, liksom kommunens övriga styrdokument, ska bidra till att stödja utvecklingen av en effektiv och säker verksamhet i enlighet med kommunens övergripande mål. Den av kommunfullmäktige beslutade krisledningsplanen ska också ses som ett övergripande dokument till styrdokumentet för informationssäkerhet.

Dokumentet är också ett styrande dokument parallellt med "Strategi för IT". Dessa strategiska dokument kompletterar varandra.

IT-strategin belyser behov och åtgärder avseende IT för att stödja utvecklingen av en effektiv verksamhet i enlighet med kommunens övergripande mål. Strategi för informationssäkerhet belyser behov och åtgärder för att säkerställa att kommunens information, i vidare mening, finns tillgänglig och inte förstörs, förvanskas, eller röjs för obehöriga.

Detaljerade riktlinjer för "Informationssäkerhetsinstruktion för Förvaltning" och "Informationssäkerhetsinstruktion för Användare" fastställs av kommundirektören och revideras vid behov.
SLA, Service Level Agreements, revideras vid behov.