



NORRTÄLJE
KOMMUN

FÖRFATTNINGSSAMLING

Informationssäkerhetspolicy för Norrtälje kommun

Antagen av kommunfullmäktige 2012-04-02 § 61



KF § 61

Dnr KS 11-1825 003

Antagande av informationssäkerhetspolicy för Norrtälje kommun

Beslut

Kommunfullmäktige beslutar:

att anta informationssäkerhetspolicy daterad den 20 januari 2012.

Bakgrund

Vid arbetet med att införa den nationella strategin för användning av IT i vård och omsorg har avsaknaden av en informationssäkerhetspolicy för Norrtälje kommun aktualiserats. Huvudsyftet med en informationssäkerhetspolicy med tillhörande riktlinjer och rutiner är att säkerställa att kommunens informationshantering sker enligt gällande lagar och förordningar. Vidare är antagande av en informationspolicy ett nödvändigt steg för att uppfylla de ”16 principer för samverkan” som kommunfullmäktige tidigare beslutat om.

Tjänstemannaberedning

Kommunstyrelsekontoret föreslår i skrivelse daterad den 19 januari 2012 att kommunfullmäktige beslutar att anta informationssäkerhetspolicy daterad den 20 januari 2012.

Politisk beredning

Arbetsutskottet har vid sammanträde den 8 februari 2012, § 32 föreslagit att kommunstyrelsen beslutar enligt kommunstyrelsekontorets förslag från den 19 januari 2012.

Kommunstyrelsen har vid sammanträde den 19 mars 2012, § 43, föreslagit enligt arbetsutskottets förslag.

Beslutande sammanträde

Kjell Jansson (M)

- bifall till kommunstyrelsens förslag

Expedieras till: Samtliga nämnder och kontor

Justerandes sign

Utdragsbestyrkande



NORRTÄLJE
KOMMUN

TJÄNSTEUTLÅTANDE
2012-01-19

Handläggare: Leif Klasson
Dnr: 2011-001825

Till Kommunstyrelsen

NORRTÄLJE KOMMUNSTYRELSE	
2012 -02- 01	
Datum	Dokumentnr

Informationssäkerhetspolicy för Norrtälje kommun

Förslag till beslut

Kommunstyrelsen beslutar föreslå kommunfullmäktige

Att anta föreliggande informationssäkerhetspolicy

Per Nordenstam
Kommundirektör

Leif Klasson
Avdelningschef

Sammanfattning

Huvudsyftet med informationssäkerhetspolicyen och de riktlinjer och rutiner för informationssäkerhetsarbetet som ska fastställas, är att säkerställa att kommunens informationshantering sker i enlighet med gällande rätt och grundläggande demokratiska principer som offentlighetsprincipen, principen om meddelarfrihet och tryckfrihetsförordningens bestämmelser om efterforskningsskydd.

Bakgrund

Arbetet med att införa den nationella strategin för användningen av IT i vård och omsorg har accentuerat bristen på en informationssäkerhetspolicy i Norrtälje kommun. En sådan policy, som hittills saknats i kommunen, skapar ramverk för att säkerställa att man hanterar informationstillgångar på ett korrekt sätt i alla kommunens verksamheter. Det är även ett nödvändigt steg för att uppfylla de ”16 principer för samverkan” som Kommunfullmäktige fattat beslut om.

POSTADRESS
Box 800, 761 28 Norrtälje
ORGANISATIONSNUMMER
212000-0217

BESÖKSADRESS
Estunavägen 14

TELEFON
0176-710 00
TELEFAX
0176-711 04

E-POST
kommunstyrelsen@norrtalje.se
WEBB
norrtalje.se

PLUSGIRO
3 20 65-5
BANKGIRO
451-7694



Beskrivning av ärendet

Huvudsyftet med informationssäkerhetspolicyn och de riktlinjer och rutiner för informationssäkerhetsarbetet som ska fastställas, är att säkerställa att kommunens informationshantering sker i enlighet med gällande rätt och grundläggande demokratiska principer som offentlighetsprincipen, principen om meddelarfrihet och tryckfrihetsförordningens bestämmelser om efterforskningsskydd.

Informationssäkerhetsarbetet utgår i första hand från lagar, andra författningar och föreskrifter, men också från kommunens egna krav och ingångna avtal mellan kommunen och annan part.

SKL's strategi för e-samhället innehåller 4 insatsområden och det fjärde avser infrastruktur och informationssäkerhet.

Informationssäkerhet reglerar inte bara hur vi arbetar med våra it-baserade informationssystem utan även andra former av information. Det är betydelsen av informationen som är styrande, inte systemen, organisationen eller tekniken.

Information 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 dess form eller miljön den förekommer i.

Policyn utgör högsta nivån i nedanstående styrande dokument som beskriver hur vi ska arbeta med informationssäkerhet. Strukturen är enligt följande;

- Informationssäkerhetspolicy. Beskriver den övergripande inriktningen.
- Regler och Riktlinjer som fastställs av Kommunstyrelsekontoret. Har sin utgångspunkt i informationssäkerhetspolicyn.
- Tillämpningar, rutiner och checklistor.
- Konsekvensbeskrivningar. Dessa håller på att arbetas fram i samarbete med KSL under 2012.

Kommunförbundet i Stockholms län (KSL) har ambitionen att i samarbete med kommunerna skapa mallar för styrande dokument som sedan kan återanvändas. Detta ska leda till utökad användning av gemensamma modeller, termer och begrepp och underlätta samverkan. Den här aktuella informationssäkerhetspolicyn har sin grund i detta arbete.



Dokumenterna är baserade på riktlinjer från Myndigheten för Samhälle och Beredskap (MSB) samt de modeller som tillämpas av Stockholms stad och Stockholms läns landsting. Samma klassningsmodeller och nomenklatur tillämpas men dokumenterna har anpassats för att kunna fungera i mindre verksamheter.

Rollfördelning för informationssäkerhetsarbetet:

Kommunstyrelsekontoret är övergripande ansvarigt för att samordna arbete och följa upp tillämpning.

Nämnd/bolagsstyrelse har ansvar för informationssäkerhetsarbetet inom den egna verksamheten. Nämnden utser systemägare och informationsägare att i sitt ställe ansvara för informationssäkerheten.

CIO har det övergripande och strategiska ansvaret att leda, utveckla och samordna informationssäkerhetsarbetet med hjälp av kommunens säkerhetschef. I uppdraget ingår även att genomföra revisioner inom verksamheten med avseende på informationssäkerhet.

Systemägarna har övergripande ansvar för respektive system och dess användning. Den som är utsedd systemägare kan vara den som har ansvaret för den verksamhet som aktuellt informationssystem stödjer.

Systemförvaltarna tar det funktionella (dagliga) helhetsansvaret för ett system. Systemförvaltaren fungerar i hög grad som systemägarens utförare och ser till att systemets funktionalitet samt planerade och beslutade aktiviteter genomförs och upprätthålls.

Informationsägarna har det övergripande och yttersta ansvaret för den information som används av ett eller flera system. Informationsägaren fattar de avgörande besluten om informationen behöver revideras.

Kommunarkivarien har tillsynsansvar för att informationen hanteras enligt bestämmelserna i tryckfrihetsförordningen, arkivlagen och offentlighets- och sekretesslagen.

IT-enheten utgör stöd.



Arbetet med informationssäkerhet ska integreras med normal system- och informationsförvaltning.

Remisshantering.

Informationssäkerhetspolicyen har varit på remiss till nämnder och bolag i koncernen. Kort kan sägas att alla som svarat är positiva till förslaget och vitsordar behovet. TioHundranämnden föreslår ett senareläggande av beslutet för att det skall finnas tid att anordna informations- och diskussionsseminarier i ämnet. Man önskar även genomförandeplan samt klargörande av ansvarsfrågor och några andra frågor som har med genomförandet att göra före beslut.

Kommunstyrelsekontoret ser att detta är relevanta synpunkter men att dessa bör behandlas i samband med planering av införandet och framtagande av slutliga riktlinjer. I praktiken tillkommer inget nytt ansvar utöver det som nämnderna redan har för sin verksamhet i med detta beslut utan det ger möjlighet att uppfylla och visa att man uppfyller detta ansvar.

Generellt kan sägas att för TioHundras verksamhet är det av vikt att denna policy och efterlevnaden av densamma kommer på plats snarast eftersom det är ett krav för att man skall ha rätt att använda de nödvändiga medicinska system som används i verksamheten.

Slut

Bilagor

1. Informationssäkerhetspolicy

Beslut skickas till

Den/de som berörs och ska ta del av beslutet



1. Informationssäkerhetspolicy

Norrtälje kommun är beroende av att medborgare, företag och övriga intressenter har ett starkt förtroende för verksamheten. Det är därför viktigt att information hanteras på ett säkert sätt och inte sprids felaktigt. En bra informationssäkerhet förbättrar förtroendet för kommunens verksamheter, håller ner direkta och indirekta kostnader samt minskar risken för rättsliga processer.

Denna informationssäkerhetspolicy gäller för informationssäkerhet inom Norrtälje kommun, och kompletterar kommunens övriga policies inom bland annat IT, dokumenthantering och kommunikation.

Denna policy beskriver kommunens mål och inriktning för informationssäkerhetsarbetet. Policyn med tillhörande riktlinjer ska ge verksamheten ett stöd kring informationssäkerhet i det dagliga arbetet inom kommunen.



2. Allmänt om informationssäkerhet

Information 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 dess form eller miljö den förekommer i.

Vårt arbete med informationssäkerhet utgår framförallt från

- lagar, andra författningar och föreskrifter
- kommunens egna krav
- avtal

Norrtälje kommun ska med avseende på informationssäkerhet följa lagar, andra författningar och rättspraxis på området. Kommunen ska också bevaka nya bestämmelser och ny rättspraxis och kontinuerligt uppdatera riktlinjer och rutiner när så krävs.

Det ska särskilt beaktas att kommunens riktlinjer och rutiner kring informationssäkerhetsarbetet inte står i strid med grundläggande demokratiska principer som offentlighetsprincipen, principen om meddelarfrihet och tryckfrihetsförordningens bestämmelser om efterforskningskydd.

Kommunen ska följa föreskrifter från myndigheter på informationssäkerhetsområdet. Kommunen bör också följa rekommendationer från MSB (Myndigheten för samhällsskydd och beredskap), SKL (Sveriges kommuner och landsting), KSL (Kommunförbundet Stockholms Län), Datainspektionen och andra myndigheter och kommungemensamma intresseorganisationer.

Informationssäkerheten omfattar Norrtälje kommuns informationstillgångar utan undantag.

Med informationssäkerhet avses att vissa definierade krav säkerställs beroende på vilken information som avses. Kraven kan sammanfattas i fyra punkter:

- **Riktighet** - som innebär att informationen ska vara tillförlitlig, korrekt och fullständig och inte ska kunna förändras av obehöriga, av misstag eller på grund av funktionsstörning.
- **Sekretess** - som innebär att tillgång till innehållet i all typ av information, handlingar och dokument ska kunna begränsas. Sekretess i det här sammanhanget kan också beskrivas som insynsskydd, konfidentialitet eller åtkomstbegränsning.
- **Spårbarhet** - som innebär att specifika aktiviteter eller händelser i efterhand ska kunna spåras till ett identifierat objekt som en användare, skrivare, dator eller system/program. Det ska gå att se vem som tagit del av informationen, vilka förändringar som har skett och av vem dessa har utförts.



- **Tillgänglighet** - som innebär att information och informationstillgångar ska kunna utnyttjas efter behov, i förväntad utsträckning och inom önskad tid utifrån de krav som ställs på verksamheten.

Informationssäkerheten är en integrerad del av verksamheten. Alla som hanterar informationstillgångar har ett ansvar att upprätthålla informationssäkerheten. Det är också ett ansvar för chefer på alla nivåer att aktivt verka för en positiv attityd till informationssäkerhetsarbetet.

Var och en ska vara uppmärksam på och rapportera händelser som kan påverka säkerheten för kommunens informationstillgångar.

Alla verksamheter inom Norrtälje kommun omfattas av denna informationssäkerhetspolicy. Detta gäller även externa verksamheter som anknyter till Norrtälje kommun till exempel konsulter eller olika typer av entreprenörer.

Den som använder kommunens informationstillgångar på ett sätt som strider mot denna policy kan bli föremål för disciplinära, alternativt rättsliga, åtgärder.

För Norrtälje kommuns informationssäkerhetsarbete gäller att:

- Personal har kunskap om gällande informationssäkerhetsregler.
- Informationsförsörjningen är säker, effektiv och bidrar till ökat skydd och stöd till verksamheten.
- Lagar, förordningar och föreskrifter är kända och skall följas
- Ingångna avtal är kända och följs.
- Krishanteringsförmågan upprätthålls.
- Alla investeringar både i form av information samt teknisk utrustning har skydd i tillräcklig grad.
- Det finns tillgång till en gemensam, säker och väl definierad infrastruktur för extern och intern datakommunikation.
- Hotbilden för varje enskilt informationssystem som är av vikt för verksamheten analyseras fortlöpande.
- Händelser i informationssystemen som kan leda till negativa konsekvenser förebyggs.
- Årliga mål för arbetet ska ingå i den normala verksamhetsplaneringen. För de årliga målen anges:
 - Vad som ska göras under året och hur det skall göras.
 - Tidsplan.
 - Behov av personella och ekonomiska resurser.
 - När och hur uppföljning, utvärdering och avrapportering ska ske.
 - Hur medarbetare ska informeras och utbildas.



3. Roller och ansvar

Kommunstyrelsekontoret är övergripande ansvarigt för att samordna arbete och följa upp tillämpning.

CIO har det övergripande och strategiska ansvaret att leda, utveckla och samordna informationssäkerhetsarbetet med hjälp av kommunens säkerhetschef. I uppdraget ingår även att genomföra revisioner inom verksamheten med avseende på informationssäkerhet.

Systemägarna har övergripande ansvar för respektive system och dess användning. Den som är utsedd systemägare kan vara den som har ansvaret för den verksamhet som aktuellt informationssystem stödjer.

Systemförvaltarna tar det funktionella (dagliga) helhetsansvaret för ett system. Systemförvaltaren fungerar i hög grad som systemägarens utförare och ser till att systemets funktionalitet samt planerade och beslutade aktiviteter genomförs och upprätthålls.

Informationsägarna har det övergripande och yttersta ansvaret för den information som används av ett eller flera system. Informationsägaren fattar de avgörande besluten om informationen behöver revideras.

Kommunarkivarien har tillsynsansvar för att informationen hanteras enligt bestämmelserna i tryckfrihetsförordningen, arkivlagen och offentlighets- och sekretesslagen.



4. Generella krav

4.1. Kommunens informationstillgångar

Samtliga informationstillgångar ska vara identifierade och förtecknade. Av förteckningen ska framgå vem som är systemägare eller informationsägare.

Alla informationssystem ska minst klara den basnivå för informationssäkerhet som kommunen rekommenderar (BITS – Basnivå för informationssäkerhet) och som utges av Myndigheten för samhällsskydd och beredskap (MSB).

Vissa informationssystem är en förutsättning för att kunna bedriva vår verksamhet. För dessa ska en riskanalys upprättas med stöd av kommunens verktyg för analys av informationssäkerhet (BITS Plus). Analysen ska utgöra underlag för driftgodkännande.

4.2. Informationssäkerhetsutbildning

All berörd personal ska regelbundet få den utbildning som behövs för att informationssäkerheten ska upprätthållas.

4.3. Informationsklassning

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

4.4. Användning av kommunens informationstillgångar

Samtliga anställda inom Norrtälje kommun som använder kommunens informationstillgångar är skyldiga att känna till och efterleva kommunens policy, regler och riktlinjer.

4.5. Kontinuitetsplanering

Kontinuitetsplaneringen är av central betydelse för att bedriva verksamheten på en acceptabel nivå under såväl normala förhållanden som vid extraordinära händelser. En kontinuitetsplan ska finnas baserad på de olika informationstillgångarnas samlade krav.

För respektive informationstillgång är systemägaren eller informationsägaren ansvarig för kontinuitetsplanen.

4.6. Revidering och uppföljning

Uppföljning ska genomföras kontinuerligt och är en viktig del i informationssäkerhetsarbetet för att bevaka att:

- Beslutade åtgärder är genomförda.
- Årliga mål är uppfyllda.
- Regler följs.
- Policy, säkerhetsinstruktioner och riskanalyser vid behov revideras.



5. Dokumentinformation

Information	
Område	KSK, Policydokument
Version / Status	0.3

Godkännandeprocess		
Roll	Namn	Datum
Godkännande och beslut	Kommunstyrelsen	
Godkännande och beslut om remiss	KSAU	
Granskad och godkänd	Måndagsberedning	
Konsulteras	Systemägare ekonomi resp. lönesystem.	
Informeras	Tommie Eriksson	
Författad	Leif Klasson	
Referensgrupp	Lars Anderman Mimmi Nyholm Örjan Rose'n Ann-Marie Alfredsson	

Historik				
Version	Status	Datum	Författare	Ändringssammanfattning
0.1	Utkast	2011-08-23	Leif Klasson	Nytt dokument
0.2-0.3	Författande	2011-09-01	Leif Klasson	Justerung efter synpunkter
0.90	Justerung efter kommentarer	2011-09	Leif Klasson	Justerat efter kommentarer från räddningschef och säkerhetschef
0.91	Korr. läsning	2011-09		
0.92	Måndagsberedning	2011-09		
0.95	KSAU	2011-10-11		
0,95	Remiss nämnder och Bolag	2011-12-09		
1,0	Genomgång av remissvar	2012-01-19		
1.0	Beslut KS			