JÖNKÖPINGS KOMMUN

kommunfullmäktige ☒
kommunstyrelsen ☒
övriga nämnder ☐
förvaltning ☐

Program för informationssäkerhet

Fastställt av kommunfullmäktige 2008-10-02 § 302
komplettering gjord av kommunstyrelsen 2011-11-02 § 336

Policy avseende informationssäkerhet

1 Syfte

Syftet med denna policy är att utgöra ett övergripande och gemensamt regelverk för Jönköpings kommun avseende informationssäkerhet. Informationssäkerhet är den del i kommunens lednings- och kvalitetsprocess som avser hantering av verksamhetens information. Informationssäkerhetspolicyn och särskilda informationssäkerhetsinstruktioner styr Jönköpings kommuns informationssäkerhetsarbete.

Information är en av Jönköpings kommuns viktigaste tillgångar och utgör en förutsättning för att kunna bedriva verksamheten. Den totala mängden information samt utbytet av information inom och mellan olika verksamheter i kommunen, 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.

Mycket av våra informationstillgångar är samlade i våra IS/IT-system. Krav ställs dels på att systemen ska ha en hög tillförlitlighet, i vissa fall ställs också sekretesskrav och nästan alltid är hög tillgänglighet en förutsättning för att man ska 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. Dessutom ska i många fall samverkan med andra myndigheter ske.

Informationssäkerhetspolicyn redovisar kommunfullmäktiges viljeinriktning och mål för informationssäkerhetsarbetet. Policyn konkretiseras i riktlinjer och instruktioner.

2 Omfattning

Informationssäkerhetspolicyn omfattar alla verksamheter, förvaltningar och avdelningar inom Jönköpings kommun. Informationssäkerhetspolicyn gäller för all informationshantering i Jönköpings kommun.

Med informationstillgång avses all information oavsett i vilken form eller hur den behandlas, t.ex. fysiskt på papper, muntligt eller elektroniskt lagrad i IS/IT-system. All information som skapas eller används i anknytning till Jönköpings kommuns verksamhet ska skyddas mot hot oavsett driftsmiljö.

Med informationssäkerhet avses
- att rätt information är tillgänglig för rätt person när den behövs och på ett spårbart sätt
- att informationen är och förblir riktig
- att informationen skyddas från otillbörlig åtkomst

Med informationssäkerhet avses vidare såväl administrativ säkerhet som teknisk säkerhet. Administrativ säkerhet avser säkerhet vid behandling och/eller lagring av information. Med teknisk säkerhet avses säkerhet genom tekniska lösningar. Teknisk säkerhet kan uppdelas i fysisk säkerhet och IT-säkerhet. Fysisk säkerhet avser fysiskt skydd för t.ex. datamedia. Begreppet IT-säkerhet avser säkerhet för information i informationsbehandlande tekniska system. IT-säkerhet kan därtill uppdelas i datasäkerhet och kommunikationssäkerhet. Datasäkerhet avser skydd av data och IT-system mot t.ex. obehörig åtkomst. Kommunikationssäkerhet avser säkerhet i samband med överföring av data.

Utgångspunkter i vårt arbete med informationssäkerhet är lagar, förordningar, föreskrifter, vårt interna regelverk och våra egna krav samt ingångna avtal.

3 Mål

För vårt informationssäkerhetsarbete ska gälla att:

- all personal har kunskap om gällande informationssäkerhetsregler
- att informationsförsörjningen är säker, effektiv och bidrar till ökat skydd och stöd för medarbetare, samverkande partners och tredje man
- upprätthålla ett högt förtroende hos medborgarna
- ingångna avtal är kända och följs
- krishanteringsförmågan upprätthålls
- alla investeringar både i form av information och 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 vår verksamhet analyseras fortlöpande
- händelser i informationssystemen som kan leda till negativa konsekvenser förebyggs

4 Generella krav

4.1 Jönköpings kommuns informationssystem

Samtliga informationssystem ska vara identifierade och förtecknade. Av förteckningen ska framgå vem som är systemägare. Vissa informationssystem är en förutsättning för att kunna bedriva vår verksamhet. För dessa ska en riskanalys upprättas.

4.2 Distansarbete

För att anställda ska kunna arbeta effektivt ska möjlighet finnas, där behov finns, att arbeta mobilt eller stationärt på distans. Förutsättningar och restriktioner för detta ska dokumenteras.

4.3 E-post

Hantering av information som är känslig ur spridningssynpunkt, är enbart tillåten då det finns särskilda funktioner för att förhindra obehörig åtkomst. En hot- och riskanalys skall utföras och val av teknik och nivå bedöms utifrån analysens resultat. Om dessa funktioner saknas får inte denna information hanteras i e-postsystemet.

4.4 Kontinuitetsplanering

Kontinuitetsplanering är av central betydelse för att bedriva verksamheten på en acceptabel nivå under såväl normala förhållanden som vid extraordinära händelser. En kontinuitetsplan ska finnas för driften av IS/IT-verksamheten baserad på de enskilda IS/IT-systemens krav på avbrotts- och katastrofplanering.

5 Ansvar

Stadsdirektören har det övergripande ansvaret för informationssäkerheten. Informationssäkerhetsarbetet ska samordnas av IS/IT-avdelningen.

Ansvaret för informationssäkerheten ska 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.

Informationssäkerheten är en integrerad del av vår verksamhet. 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 säkerhetsarbetet.

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

Alla delar inom kommunen är bundna av denna informationssäkerhetspolicy vilket medför att det inte finns utrymme att besluta om lokala regler som avviker från denna.

Den som använder våra informationstillgångar på ett sätt som strider mot denna policy kan bli föremål för disciplinära åtgärder

6 Revidering och uppföljning

Denna policy, samt tillhörande riktlinjer och instruktioner, ska löpande följas upp och vid behov revideras.

7 Referenser

- Rekommendationer och anvisningar från Krisberedskapsmyndigheten, KBM (BITS, Basnivå för IT-säkerhet)
- Standarderna i ISO 27000-serien, Ledningssystem för informationssäkerhet (särskilt SS-ISO/IEC 27001:2006 och SS-ISO/IEC 27002:2005)

§ 366

Kompletterande riktlinjer till policyn om informationssäkerhet för nämndernas hantering av personuppgifter

Ks/2008:490 005

Sammanfattning

I samband med kommunfullmäktiges behandling av förslag till IS/IT-strategi och policy avseende informationssäkerhet 2008-10-02 gavs kommunstyrelsen i uppdrag att utarbeta kompletterande riktlinjer till policyn om informationssäkerhet för nämndernas hantering av personuppgifter. Ärendet har remitterats till stadskontoret som inkommit med förslag till komplettering.

Beslutsunderlag

Policy avseende informationssäkerhet 2008-10-02

Stadskontorets tjänsteskrivelse 2011-09-30

Kommunalrådsyttranden enligt nedan

Stadskontorets förslag

Stadskontorets tjänsteskrivelse 2011-09-30 med förslag till kommunstyrelsens beslut:

- Nuvarande informationssäkerhetspolicy beslutad av kommunfullmäktige 2008-10-02 kompletteras med följande:
  - Punkt 4.4 blir punkt 4.5
  - Ny punkt 4.4 Personuppgifter
  - Vid nämndernas hantering av personuppgifter ska personuppgiftslagstiftningen samt regler och anvisningar från Datainspektionen beaktas.

Majoritetsrådets förslag

Kommunalrådet Mats Greens (M) förslag till kommunstyrelsens beslut:
Med anledning av kommunfullmäktiges beslut 2011-06-22 § 217 att fastställa en nomenklatur för kommunens styrdokument föreslås följande:

- Stadskontorets förslag tillstyrks med ändringen att nuvarande policy avseende informationssäkerhet byter benämning till "Program avseende informationssäkerhet" i linje med antagen nomenklatur för kommunens styrdokument.

Oppositionsrådets förslag

Kommunalrådet Elin Lagerqvist (S) instämmer.

KOMMUNSTYRELSENS BEHANDLING 2011-11-02

Kommunstyrelsens beslut

- Nuvarande informationssäkerhetspolicy beslutad av kommunfullmäktige 2008-10-02 kompletteras med följande:
  - Punkt 4.4 blir punkt 4.5
  - Ny punkt 4.4 Personuppgifter

- Vid nämndernas hantering av personuppgifter ska personuppgiftslagstiftningen samt regler och anvisningar från Datainspektionen beaktas.

– Nuvarande policy avseende informationssäkerhet byter benämning till ”Program avseende informationssäkerhet” i linje med antagen nomenklatur för kommunens styrdokument.

Beslutet expedieras till:
Nämnderna
IS/IT-chefen