



Informationssäkerhetspolicy

Linköpings kommun

Antaget av: Kommunfullmäktige
Status: Antaget 2016-08-30 § 291
Giltighetstid: Tillsvidare



Sekretess: Öppen
Diarienummer: Ks 2016-481
Dokumentansvarig: Administrativa
direktören
Upprättat av:
Adresserat till: Kommunfullmäktige
Tidpunkt för aktualitetsprövning:
Tidpunkt för senaste revidering:
Relaterade styrdokument: Säkerhetspolicy
Sökord: Informationssäkerhetspolicy,
informationssäkerhet, policy, Info Säk

1 Giltighet

Denna informationssäkerhetspolicy är en tillämpning av säkerhetspolicyn och är fastställd av Linköpings kommunfullmäktige 2016-08-30 enligt § 291 Dnr 2016-481, för att gälla tills vidare. Alla verksamheter samt bolag inom Linköpings kommun omfattas av denna informationssäkerhetspolicy.

2 Inledning och motiv

Linköpings kommun hanterar stora mängder information. Att information som kommunen hanterar i relationer med kommuninvånare, företag och organisationer såväl som inom vår egen organisation är korrekt utgör en grund för tillit och förtroende. Det är även viktigt att information i alla externa och interna relationer är tillgänglig när det behövs och att känslig information skyddas för att vi skall kunna fullgöra vårt uppdrag i samhället. Informationens säkerhet är därför en mycket viktig aspekt för alla verksamheter(informationsägaren) inom Linköpings kommun.

3 Syfte

Linköpings kommuns informationssäkerhetspolicy redovisar kommunfullmäktiges viljeinriktning och mål för informationssäkerhetsarbetet.

Informationssäkerhetspolicyn med kompletterande riktlinjer, regler och tillämpningsanvisningar ger kommunens verksamheter förutsättningar och stöd i informationssäkerhetsarbetet.

4 Målsättning

Informationssäkerhet är kommunens förmåga att hantera informationen så att legala, etiska, och verksamhetsmässiga intentioner upprätthålls. Målsättningen med kommunens informationssäkerhetsarbete är därför att skydda kommunen, dess verksamhet och invånare som annars riskerar att skadas genom bristande informationssäkerhet.

Att genom ett väl förankrat och integrerat ledningssystem för informationssäkerhet möjliggöra bra service och utveckling, samt ett gott samarbete såväl internt som externt för verksamheten generellt.

Linköpings kommun värderar informationstillgångarna, kartlägger informationsrelaterade risker och tilldelar informationen ett relevant skydd för att säkerställa följande kriterier hos informationen:

- Konfidentialitet skydd mot obehörig insyn
- Riktighet skydd mot oönskad förändring
- Tillgänglighet åtkomlighet för behörig person vid rätt tillfälle

- Spårbarhet entydig härledning av utförda aktiviteter till en identifierad användare

5 **Omfattning**

Informationssäkerhetsarbetet innebär ett systematiskt och långsiktigt arbete och omfattar hela kommunens verksamhet och all information oavsett bärare (exempelvis information i datorer, i telefonsamtal eller i skrift på papper). I och med att information till stora delar skapas, bearbetas, lagras och transporteras i elektronisk form, omfattar informationssäkerhetsarbetet även tekniska aspekter såsom exempelvis IT-utrustning, programvaror och nätverk.

6 **Roller och organisation**

Alla ska följa gällande informationssäkerhetsriktlinjer, tillämpningsanvisningar, rapportera svagheter och incidenter som kan påverka informationssäkerheten. Ansvariga för informationstillgångar och för resurser som hanterar information skall utses.

Verksamhetsansvariga/informationsägaren ska planera, genomföra och återrapportera informationssäkerhetsarbetet. Chefer på alla nivåer har ett ansvar att informera sina medarbetare om informationssäkerhetspolicyn och dess tillämpningar.

Följande roller är centrala för det strategiska och operativa informationssäkerhetsarbetet i Linköpings kommun:

Säkerhetschefen	ansvarar strategiskt och operativt för kommunens hela säkerhetsarbete, vilket innefattar informationssäkerhetsarbetet.
Informationssäkerhets- samordnaren	har ansvaret för att utveckla och samordna informationssäkerhetsarbetet.
Informationsägare	informationsägare är tillika verksamhetsansvarig och ansvarar för att värdera informationen och därigenom ställa krav på dess skydd.
Informationsresursägare	ansvarar för att skydda information med relevanta säkerhetsåtgärder utifrån informationens värde.
IT-säkerhetsansvarig	ansvarar för att samordna och stödja informationsresursägare i val av relevanta

säkerhetsåtgärder. Har även ett övergripande ansvar för att säkerställa ett grundskydd för information hanterad i IT-verksamheten.

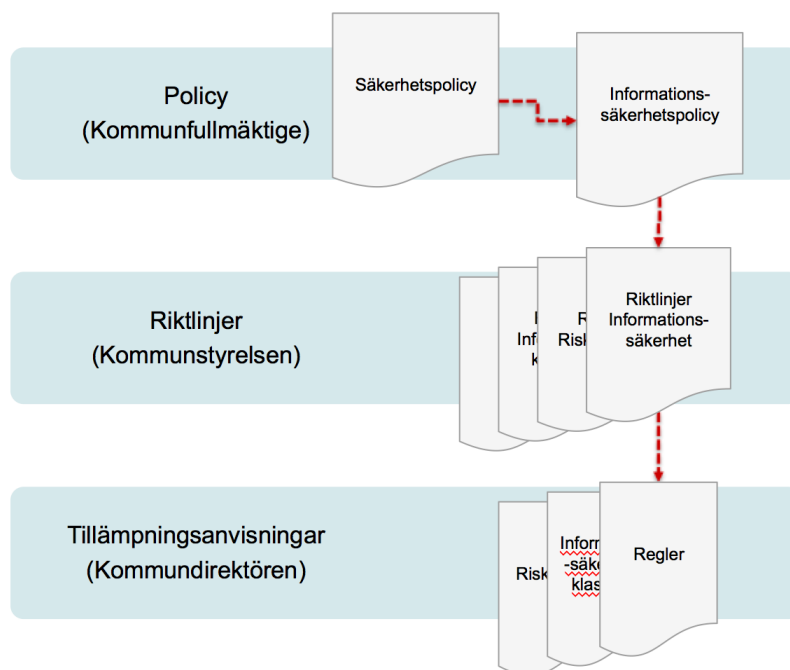
Informationssäkerhetsrådet

i detta forum sker kommunens samordning och uppföljning av informationssäkerhetsarbetet. Informationssäkerhetssamordnaren är sammankallande och leder arbetet för att förverkliga den målsättning som formulerats i denna policy. Representanter för kommunens olika verksamheter samt säkerhetschefen ska ingå. Rådet ska sammanträda regelbundet och rapportera om sin verksamhet till kommunledningen.

7 Tillämpning

För att uppfylla målsättningen med Linköping kommuns informationssäkerhet och för att kunna styra och leda arbetet med informationssäkerhet, har kommunen valt att införa ett systematiskt informationssäkerhetsarbete. Arbetet ska följa MSB: s (Myndigheten för Samhällsskydd och Beredskap) rekommendationer för kommuners informationssäkerhet samt kraven i informationssäkerhetsstandarderna ISO/IEC 27001.

Ramverket ska utformas enligt följande struktur:



Informationssäkerhetspolicyn konkretiseras med riktlinjer som fastställs av kommunstyrelsen. Dessa dokument revideras och förnyas vid behov. I huvudsak behandlas:

- Roller, ansvar och befogenheter
- Identifiering, värdering, klassificering och hantering av våra informationstillgångar
- Riskhantering
- Incidenthantering
- Relevanta skyddsåtgärder, exempelvis
 - säkerhetskopiering,
 - loggning,
 - behörighetshantering,
 - åtkomstkontroll,
- Säkerhetsmedvetande
- Kontinuitetshantering
- Uppföljning och efterlevnad