§ 44

TJÄNSTESKRIVELSE
2010-03-09
1 (1)

Tyresö kommun

Thomas Halvarsson, Peter Holck

Kommunstyrelsen

Informationssäkerhetspolicy

Förslag till beslut

Att kommunstyrelsen antar den föreslagna informationssäkerhetspolicyn.

Dan Näsman
Tf Kommundirektör

Beskrivning av ärendet

Thomas Halvarsson och Peter Holck fick i uppdrag av kommunchef Staffan Isling att utforma ett förslag till Informationssäkerhetspolicy.
I av kommunstyrelsen antagen It-strategi anger ett av inriktningsmålen att en It-säkerhetspolicy ska tas fram.
Uppdraget blev att ta fram en informationssäkerhetspolicy för att uppfylla dagens krav på informationshantering.

§ 441

Datum
2010-03-24

Informationssäkerhetspolicy

Beslutad av kommunstyrelsen 2010-03-30, xx §

Alla verksamheter inom Tyresö kommun är bundna till denna policy, som är en integrerad del av kommunens säkerhetsarbete. Lokala avvikelser får inte förekomma.

Var och en ska vara uppmärksam på och rapportera händelser som kan misstänkas påverka informationssäkerheten.

Policy

Information är en av kommunens viktigaste tillgångar och hanteringen av den är en viktig del i arbetet med Tyresö kommuns risk- och sårbarhetsanalys

Denna policy ska säkerställa

- En säker och effektiv informationsförsörjning som bidrar till ökat skydd av informationen och stöd för medarbetare, samverkande partners och tredje man
- Att informationen är korrekt och tillgänglig samt att sekretess bibehålls och säkerställs.
- Att kommunens samtliga informationssystem är identifierade och förtecknade. Av förteckningen ska framgå vilken information som lagras i systemen och vem som är systemägare.
- Att kommunens mest kritiska verksamhetssystem är klassificerade enligt Myndigheten för samhällsskydd och beredskaps klassningsmodell BITS.
- Att kommunens informationssystem och utrustning inte utnyttjas för ändamål som är oförenliga med kommunens värderingar och förhållningssätt och därigenom kan skada kommunens anseende
- Att det finns en handlingsplan, användarinstruktioner och riskanalyser som årligen ses över och vid behov revideras.

Bakgrund

Med information avses all information oavsett hur den behandlas eller lagras och oberoende av i vilken form eller miljö den förekommer.
Informationssäkerheten omfattar utan undantag all Tyresö kommuns information.

Utgångspunkter i arbetet med denna policy har varit:

- Lagar, förordningar och föreskrifter
- Avtal
- Tyresö kommuns krav

tyresö kommun

Åtgärder för efterlevnad av policyn

Efterlevnad av denna policy kräver

- att all personal ska ha kunskap om regler och rutiner kring informationssäkerhet
- att Tyresö kommuns personal, elever och förtroendevalda inte besöker sidor med exempelvis rasistiskt, våldsinriktat eller pornografiskt innehåll, såtillvida det inte är direkt relaterat till arbetsuppgifter eller studier
- att avtal är kända och följs
- att alla investeringar både i form av information och teknisk utrustning har tillräcklig skydd
- att det finns en gemensam, säker och väl definierad infrastruktur för datakommunikation
- att hotbilden för varje enskilt informationssystem analyseras fortlöpande
- att händelser som kan leda till negativa konsekvenser i informationssystemen förebyggs

Ledning och ansvar

Ansvaret för informationssäkerheten ligger i kommunens linjeorganisation, det innebär att:

- Kommundirektören har det yttersta ansvaret för informationssäkerheten och att det finns en tydlig ansvarsfördelning för att upprätthålla denna
- Den som är ansvarig för verksamheten som aktuellt informationssystem stödjer ska vara systemägare. I normalfallet är detta förvaltningschef. I de fall ett system endast används inom en verksamhet kan förvaltningschef delegera systemägarskapet till annan verksamhetschef.
- Systemägaren ansvarar för att systemförvaltare utses.
- Systemförvaltaren ansvarar för den dagliga driften av systemen.
- Chefer ansvarar för att personal och elever följer policyn och ska aktivt verka för en positiv attityd till säkerhetsarbetet.
- Alla som hanterar information ansvarar för att informationssäkerheten upprätthålls.

Den som agerar på ett sätt som strider mot denna policy kan bli föremål för disciplinära åtgärder.

Revidering och uppföljning

Årlig uppföljning av informationssäkerhetsarbetet ska genomföras.

Uppföljning är en viktig del för att bevaka att:

- beslut är genomförda
- mål är uppfyllda
- regler följs
- policy, handlingsplan, instruktioner och riskanalyser revideras.