



Informationssäkerhetspolicy IT (0:0:0)

Kommunalförbundet ITSAM och dess medlemskommuner

Revision: 2013031201
Fastställt: Direktionen 20130926
Dnr:0036/13

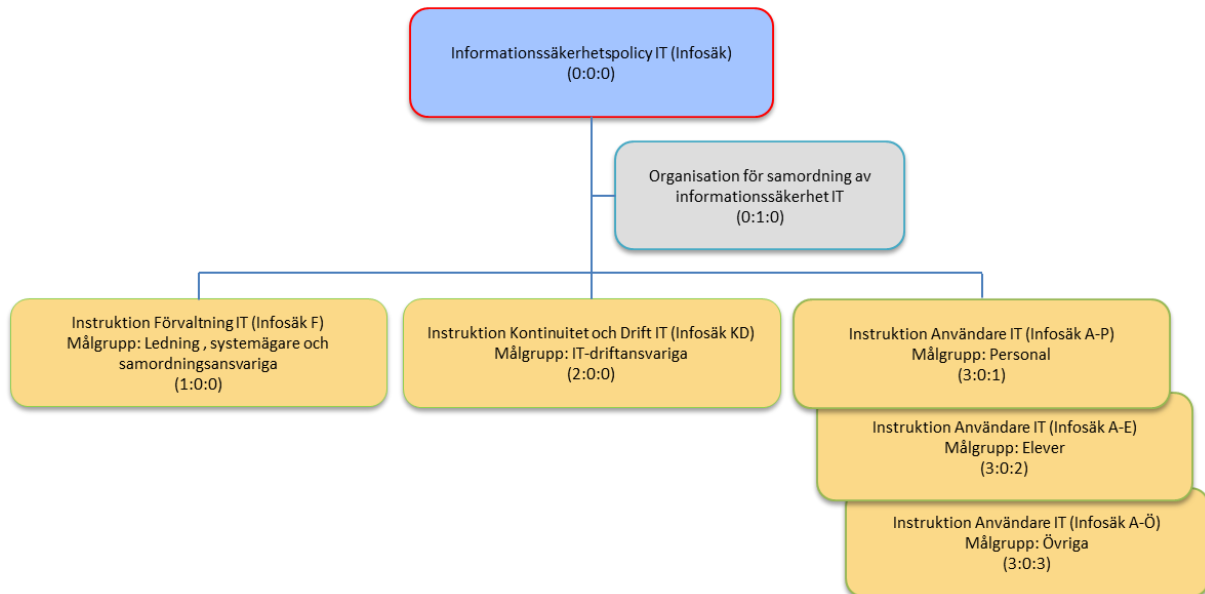
Kommunalförbundet ITSAM, Storgatan 36A, 590 36 Kisa
Tel: 0494 – 197 00, Fax: 0494 – 197 99, Org nr: 222000-2584

Innehåll

Policyns roll i informationssäkerhetsarbetet inom IT	3
Definitioner	4
Lagar, förordningar och externa regelverk.....	4
Informationstillgångar.....	4
Mål.....	5
Generella krav	5
Revidering och uppföljning.....	6

Policyns roll i informationssäkerhetsarbetet inom IT

Styrande dokument är denna policy med tillhörande underliggande policys samt dokumenten – Organisation för samordning av informationssäkerhet IT, informationssäkerhetsinstruktionerna Förvaltning IT (Infosäk F), Kontinuitet och Drift IT (Infosäk KD) och Användare IT (Infosäk A), fördelad på grupperna Personal, Elever och Övriga.



Denna policy syftar till att klarlägga:

- övergripande viljeinriktning och mål för informationssäkerhetsarbetet inom IT
- krav på riktlinjer för områden av särskild betydelse

Organisation för samordning av informationssäkerhet IT syftar till att klarlägga:

- IT-driftorganisationen och dess roll i informationssäkerhetsarbetet inom IT

Informationssäkerhetsinstruktion Förvaltning IT (Infosäk F) syftar till att klarlägga:

- Hur förvaltning av IT-system ska organiseras och struktureras
- IT-organisationen och det ansvar som ingår i de olika rollerna
- regler för systemutveckling, systemunderhåll och incidenthantering

Informationssäkerhetsinstruktion Kontinuitet och Drift IT (Infosäk KD) syftar till att klarlägga:

- IT-organisationen och det ansvar som finns för drift av informationssystemen
- regler för säkerhetskopiering, lagring, driftadministration och kontinuitetsplanering

Informationssäkerhetsinstruktion Användare IT (Infosäk A-P, A-E, A-Ö) syftar till att klarlägga:

- hur användare ska verka för att upprätthålla en god säkerhet

Definitioner

Datasäkerhet

Datasäkerhet är säkerhet beträffande skydd av datorsystem och dess data syftande till att förhindra obehörig åtkomst och obehörig eller oavsiktlig förändring eller störning vid databehandling.

IT-säkerhet

IT-säkerhet beträffande skydd av IT-system och dess data syftande till att förhindra obehörig åtkomst och obehörig eller oavsiktlig förändring eller störning vid databehandling samt dator- och telekommunikation.

Informationssäkerhet

Informationssäkerhet är säkerhet beträffande skydd av informationstillgångar syftande till att upprätthålla önskad sekretess, riktighet och tillgänglighet (även spårbarhet och oavvislighet) för desamma.

Informationssäkerhet IT

Med Informationssäkerhet IT angivet i denna policy och i tillhörande underliggande dokument avses datasäkerhet och IT-säkerhet för att upprätthålla minsta nivå av informationssäkerheten.

Lagar, förordningar och externa regelverk

Syftet med informationssäkerhetspolicy IT och dess förvaltning är att hanteringen av organisationernas informationstillgångar med tillhörande bärande system och infrastruktur ska ske inom ramen för svenska lagar och förordningar och för uppsatta regelverk från stat och myndighet.

Personuppgifter

Hantering av personuppgifter regleras av Personuppgiftslagen, PUL (1998:204). En organisation kan vara personuppgiftsansvarig och/eller personuppgiftsombud för en personuppgiftsansvarig. Mellan IT-driftorganisationen och den personuppgiftsansvariga ska det upprättas PUL-avtal där detta regleras.

Lagar som hänsyn ska tas till vid drift av informationsbärande system är bl. a Tryckfrihetsordningen SFS 1976:954, Offentlighets- och sekretesslagen (2009:400), Arkivlagen (1990:782), Kommunala redovisningslagen (1997:614), Förvaltningslagen (1986:223), Patientdatalagen (2008:355), Säkerhetsskyddslagen (1996:627), Säkerhetsskyddsförordningen (1996:633), Lagen om behandling av personuppgifter inom socialtjänsten (2001:454), Socialtjänstlagen (2001:453), Lagen om offentlig upphandling (2007:1091), Lagen om skydd för företagshemligheter (1990:409), Personuppgiftslag, PUL (1998:204).

Informationstillgångar

Information är en mycket viktig tillgång och hanteringen av den är en del i arbetet med IT-organisationens risk- och sårbarhetsanalys.

Utgångspunkter i arbetet med informationssäkerhet IT är:

- lagar, förordningar och föreskrifter
- avtal

- interna krav

Med informationstillgångar avses all information oavsett om den behandlas manuellt eller automatiserat och oberoende av i vilken form eller miljö den förekommer. Informationssäkerhet IT omfattar organisationernas alla informationstillgångar utan undantag som med IT anskaffas, lagras, behandlas, transporteras eller publiceras.

Syftet med informationssäkerhet IT är

- att rätt information är tillgänglig för rätt person när den behövs och på ett spårbart sätt
- att informationen är och förblir korrekt och oförvanskad

Informationssäkerhet IT är en integrerad del av verksamheten. Alla som hanterar informationstillgångar ansvarar för att upprätthålla säkerheten för dessa. Det är också ett ansvar för alla på alla nivåer att aktivt verka för en positiv attityd till informationssäkerhet IT. Var och en ska vara uppmärksam på och rapportera händelser som kan påverka säkerheten för organisationernas informationstillgångar.

Alla delar inom organisationerna är bundna av denna policy vilket medför att det inte finns utrymme att ensidigt besluta om lokala regler som avviker från den. Den som använder informationstillgångarna på ett sätt som strider mot denna policy kan bli föremål för disciplinära åtgärder.

Mål

För organisationernas informationssäkerhetsarbete inom IT gäller att:

- all personal har kunskap om gällande informationssäkerhetsregler
- informationsförsörjningen är säker, effektiv och bidrar till ökat skydd och stöd för alla, även samverkande parter och tredje man
- ingångna avtal är kända och följs
- krishanteringsförmågan upprätthålls
- 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 verksamheten analyseras fortlöpande
- händelser i informationssystem som kan leda till oönskade konsekvenser förebyggs

Årliga mål för arbetet beslutas i, och framgår av, verksamhetsplaneringen. För att uppnå de årliga målen anges:

- vad som ska göras under året och hur
- en tidplan
- behov av personella och ekonomiska resurser
- när och hur uppföljning, utvärdering och avrapportering ska ske
- när och hur medarbetare ska informeras och utbildas

Generella krav

IT-system

IT-systemen ska vara identifierade och förtecknade. Av förteckningen ska framgå vem som är systemägare. Alla IT-system ska minst klara den basnivå för informationssäkerhet IT som IT-organisationen

rekommenderar (ex. BITS). Vissa IT-system är en förutsättning för att kunna bedriva verksamheten. För dessa ska en riskanalys upprättas med stöd av IT-organisationens verktyg för analys av informationssäkerhet IT (ex. BITS Plus eller likvärdigt). Analysen ska utgöra underlag för driftgodkännande.

Information om informationssäkerhet IT

All personal ska regelbundet ta del av den dokumentation som behövs för att informationssäkerheten inom IT ska upprätthållas.

Informationsklassificering

Informationstillgångar inom organisationerna och som hanteras av Kommunalförbundet ITSAM ska klassificeras med avseende på sekretess, riktighet och tillgänglighet enligt organisationernas gemensamma klassningsmodell.

Distansarbete

För att användare ska kunna arbeta effektivt kan arbetsgivaren erbjuda möjlighet att arbeta mobilt på distans. Rutiner, instruktioner och underliggande policys för detta ska finnas.

Användning av Internet och elektronisk post

Vid användning av Internet kan organisationernas namn mm exponeras. Bland annat av detta skäl kan det därför vara av vikt att lägga restriktioner på vilka hemsidor som får besökas (ex. hemsidor med rasistiskt, våldsinriktat eller sexuellt innehåll). Undantag från detta kan beviljas av chef om informationen på sådana sidor kan ha relevans för arbetsuppgifterna.

Sekretessbelagd information får inte skickas utan kryptering med e-post eller hanteras via sociala medier eller andra externa tjänster som ligger utanför organisationernas administrativa kontroll.

Risk- och sårbarhetsanalys

En risk- och sårbarhetsanalys ska genomföras på befintliga system en gång varje år. Vid nyanskaffning av system ska en analys göras enligt Informationssäkerhetsinstruktion Förvaltning IT, InfoSäk F.

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 för IT-driften baserad på de olika informationssystemens samlade krav.

Revidering och uppföljning

Uppföljning är en viktig del i informationssäkerhetsarbetet avseende IT-säkerhet för att bevaka att

- beslutade åtgärder är genomförda
- årliga mål är uppfyllda
- regler efterföljs
- att policys, säkerhetsinstruktioner och risk- och sårbarhetsanalyser regelbundet och vid behov revideras

Kommunalförbundet ITSAM har enligt ITSAM-avtalet ansvaret för Informationssäkerhetspolicy IT med tillhörande underliggande policys, instruktioner, rutiner och riktlinjer samt rätten att förändra, ta bort, eller lägga till i den samma och i dess underliggande dokumentstruktur.

Informationssäkerhetspolicy IT med tillhörande underliggande policys, instruktioner, rutiner och riktlinjer publiceras löpande på <http://www.itsam.se>.