Organisation för samordning av informationssäkerhet IT (0:1:0)

Kommunalförbundet ITSAM och dess medlemskommuner

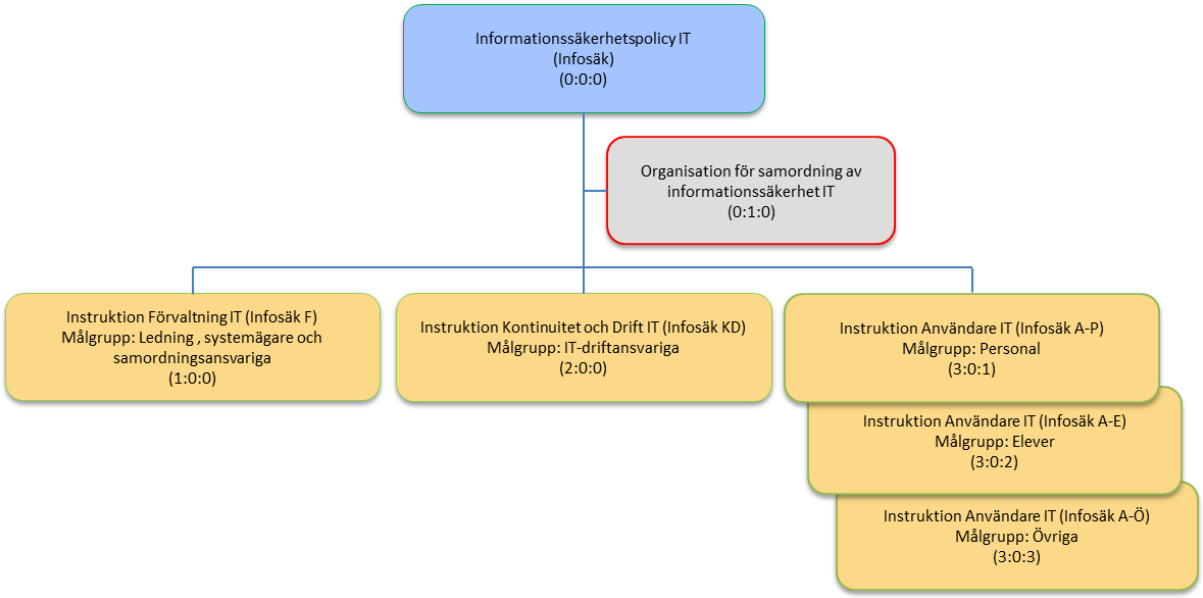
Revision: 2013031201
Fastställd: Direktionen 20130926
Dnr: 0036/13

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

Innehåll

Dokumentets roll i informationssäkerhetsarbetet inom IT

Styrande policy för detta dokument är övergripande informationssäkerhetspolicy IT med tillhörande underliggande policys samt dokumenten - informationssäkerhetsinstruktionerna Förvaltning IT (Infosäk F), Kontinuitet och Drift IT (Infosäk KD) och Användare IT (Infosäk A), fördelad på grupperna Personal, Elever och Övriga.



Informationssäkerhetspolicy IT 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-organisationen och dess roller i informationssäkerhetsarbetet inom IT

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

- Hur förvaltningen 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

Central funktion för samordning av informationssäkerhet IT

Den centrala funktionen har ett särskilt ansvar för informationssäkerhet IT samt ett uppdrag att samordna och revidera arbetet med informationssäkerhet IT i organisationerna. I Kommunalförbundet ITSAMs centrala administration finns en informationssäkerhetsfunktion. Funktionen har till uppdrag att kontinuerligt följa upp informationssäkerhet IT i organisationerna och verka för att denna upprätthålls i enlighet med fastställda lagar, policys, instruktioner, riktlinjer och övriga regelverk.

Informationssäkerhetsfunktionen har även till uppdrag att föreslå informationssäkerhetsåtgärder, följa upp fastställda åtgärder samt att initiera utvecklingsprojekt inom informationssäkerhetsområdet. Informationssäkerhetsfunktionen rapporterar löpande direkt till Kommunalförbundet ITSAMs ledning. Informationssäkerhetsansvarig svarar för samordning, stöd och information gällande IT-säkerhet inom organisationerna. Informationssäkerhetsansvarig initierar därtill utvecklingsprojekt inom informationssäkerhet IT och skall ingå som expertfunktion i alla större IT-projekt.

Arbetet med informationssäkerhet IT ska alltid ges en central betydelse.

Informationssäkerhetsansvarig och informationssäkerhetsgrupp

Ansvarig för Informationssäkerhetsfunktionen är en av Kommunalförbundet ITSAM utsedd och namngiven person. I informationssäkerhetsfunktionen kan förutom ytterst ansvarig en adjungerad grupp bestående av personer med särskilda kompetenser inom informationssäkerhetsområdet ingå. I informationssäkerhetsfunktionen skall informationssäkerhetsfrågor initieras och förankras till stöd för verksamheten.

Informationssäkerhetsansvarig har ett dokumenterat uppdrag och ansvar samt egen budget. I uppdraget ingår inte ansvar för löpande drift eller motsvarande uppgifter.

Uppgifter

Informationssäkerhetsfunktionens huvuduppgift är att skapa förutsättningar för och att verka för att informationssäkerhet IT i organisationerna är tillräcklig för att skapa trovärdighet för hantering av organisationernas informationstillgångar. Informationssäkerhetsfunktionen bereder frågor till ledningsgrupp, ställer krav på informationssäkerhet IT i organisationerna, ger stöd samt följer upp arbetet genom kontinuerlig granskning.

Arbetsformer

Informationssäkerhetsfunktionen består av informationssäkerhetsansvarig och en vid behov adjungerad informationssäkerhetsgrupp som bistår informationssäkerhetsansvarig med utredningar, granskningar mm.

Informationssäkerhetsfunktionen skall från Kommunalförbundet ITSAMs ledning erhålla kontinuerlig rapportering om verksamhet, förslag till verksamhetsplanering och budget. Informationssäkerhetsansvarig och driftfunktioner skall samverka i gemensamma frågor. Informationssäkerhetsfunktionen ställer krav på säker drift medan driftfunktionerna ansvarar för att driften är säker i enlighet med lagar samt informationssäkerhetspolicys, underliggande policys, Informationssäkerhetsinstruktioner, riktlinjer och övriga regelverk.

Informationssäkerhetsansvarig samverkar med ansvariga för arbetsmiljö, fysisk säkerhet, systemägare och projektledare.

Inplacering

Informationssäkerhetsfunktionen är fristående och ingår inte i IT-driftorganisationen. I sakfrågor är informationssäkerhetsansvarig underställd och rapporterar direkt till Kommunalförbundet ITSAMs ledning.

Roller och ansvar

- Kommunalförbundet ITSAMs direktion har det övergripande ansvaret för informationssäkerheten gällande IT och utser själva eller via delegation systemägare för respektive informationssystem.

- Ansvaret för informationssäkerheten gällande IT ska följa den i Kommunalförbundet ITSAM gällande delegationsordningen.

- Informationssäkerhetsansvarig hos Kommunalförbundet ITSAM utses av och är direkt underställd verkställande tjänsteman. Informationssäkerhetsansvarig agerar oberoende direkt under verkställande tjänsteman och har vid incidenter mandat att sätta samman ev. grupper av personer som denne anser sig behöva. Informationssäkerhetsansvarig har det operativa ansvaret för informationssäkerhetsarbetet inom IT där driftasvaret ligger på Kommunalförbundet ITSAM.

- Systemägaren är den som har ansvaret för den verksamhet som aktuellt informationssystem stödjer.

- Systemförvaltarna utses av respektive systemägare och ansvarar för den dagliga användningen av informationssystemen.

- Verkställande tjänsteman ansvarar för att uppfylla organisationens kontinuitetsplan för IT (se Informationssäkerhetsinstruktion Kontinuitet och Drift IT).

- Beskrivning av roller och ansvar framgår av Informationssäkerhetsinstruktion Förvaltning IT-system.

Incidenthanteringsgrupp, IRT (Incident Response Team)

I Kommunalförbundet ITSAM ska det finnas en Incidenthanteringsgrupp (IRT). Den ska bestå av personer med adekvat kunskap om informationssäkerhet inom IT-området. Den ska även arbeta proaktivt och utredande gentemot IT-relaterade angrepp, fysiska såväl som digitala. Inom gruppen ska det finnas personer (IRT-operatörer) med särskild delegation att undersöka och eventuellt stoppa drift vid akuta situationer. Ansvarig för incidenthanteringen samarbetar med samt rapporterar alltid till informationssäkerhetsansvarig inom Kommunalförbundet ITSAM.

Ansvar för informationssäkerhet IT

Varje systemägare ansvarar för informationssäkerhet IT inom sin verksamhet i enlighet med lagar samt fastställda informationssäkerhetspolicys, informationssäkerhetsinstruktioner, riktlinjer och övriga regelverk. Varje medarbetare, förtroendevald, student (elev) och övrig personal ansvarar också för tillämpningen av gällande lagar, informationssäkerhetspolicys, informationssäkerhetsinstruktioner, riktlinjer och övriga regelverk inom det egna området.

Delegationer

Kommunfullmäktige inom respektive medlemskommun inom Kommunalförbundet ITSAM fastställer en gemensam och övergripande informationssäkerhetspolicy IT inom medlemskommunerna. Ansvaret för revidering och uppdatering av samtliga policys inom informationssäkerhets IT överlåts till kommunalförbundet ITSAM. I enlighet med denna ska informationssäkerheten avseende IT-säkerhet organiseras enligt följande:

- Det ska centralt inom Kommunalförbundet ITSAM finnas en informationssäkerhetsfunktion för samordning av informationssäkerhetsarbetet inom IT-området.

- Informationssäkerhetsfunktionen ska bestå av minst en Informationssäkerhetsansvarig som rapporterar löpande till ledningen.

- Systemägaren är ansvarig för informationssäkerheten inom sitt verksamhetsområde och i verksamhetens IT-system i enlighet med organisationens informationssäkerhetspolicy, informationssäkerhetsinstruktioner, riktlinjer och övriga regelverk.

- Systemägaren ska i samråd med Kommunalförbundet ITSAM utse en systemförvaltare för varje IT-system. Systemägaren kan delegera ansvaret för upprätthållandet av informationssäkerheten till t ex systemförvaltaren.

- Systemägare utser behörighetsansvarig enligt beskrivning för Behörighetsansvarig.

- Systemägare utser behörighetsadministratör enligt beskrivning för Behörighetsadministratör.

- Systemägare utser en arkivansvarig vid enheten med ansvar enligt beskrivning för Arkivansvarig.

- Kommunalförbundet ITSAM ska utse en särskild person att bevaka informationssäkerheten gällande IT i systemet samt vara kontaktperson gentemot informationssäkerhetsfunktionen. Den utpekade personen ansvarar för incidentbevakning och incidenthantering med befogenheter enligt dokumentet: Ansvar, befogenheter och skyldigheter för systemadministratör i incidentgrupp (IRT-operatör).

- Kommunalförbundet ITSAM ska utse en IT-ansvarig/tekniskt ansvarig för drift och underhåll av IT-systemet.

- Kommunalförbundet ITSAM ska utse en IT-teknisk förvaltare med ansvar enligt beskrivning för IT-teknisk förvaltare.

- Aktuell delegation ska vara diarieförd vid förvaltningen.

Informationssäkerhetsfunktionens huvudsakliga uppgifter

Informationssäkerhetsfunktionens huvudsakliga arbetsuppgifter består av att:

Bereda och kontrollera

- bereda informationssäkerhetsfrågor avseende IT-säkerhet för beslut av Kommunalförbundet ITSAMs ledning
- ta fram kontinuerlig lägesrapportering av informationssäkerheten gällande IT till Kommunalförbundet ITSAMs ledning
- ta fram en årlig handlingsplan och budget samt uppföljning till Kommunalförbundet ITSAMs ledning
- utforma policys, instruktioner, riktlinjer, regler mm
- ta fram löpande uppföljning av beslutade åtgärder
- initiera en årlig granskning av Kommunalförbundet ITSAM ur ett informationssäkerhetsperspektiv avseende IT-säkerhet
- ansvara för metoder och mallar för kontroll och granskning av informationssäkerheten gällande IT
- ta fram kontrollplan för gemensamma IT-system
- sammanställa granskningsresultat och rapportera till Kommunalförbundet ITSAMs ledning

Ställa krav och bevaka

- formulera säkerhetskrav vid upphandling och införande av nya IT-system
- verka för att säkerhetskrav vid drift av IT-system och tillhörande enheter uppfylls
- verka för att säkerhetskrav på kommunikation uppfylls
- hantera uppföljning av incidenter (se dokumentet IRT-operatör)
- sköta bevakning av informationssäkerhet IT i förekommande IT-projekt
- följa upp beslut inom ansvarsområdet

Stödja verksamheten

- precisera och definiera lämpliga säkerhetsnivåer för aktuella IT-system och tillhörande enheter
- precisera och definiera lämpliga säkerhetsnivåer för IT-infrastruktur

- definiera standarder för säkerhetslösningar

- ta fram åtgärdsförslag och handlingsplaner
- ge stöd vid verksamhetens egen granskning och kontroll av informationssäkerhet IT

- vid behov medverka vid ledningsgrupps- och informationsmöten

- förmedla expertstöd

- internt utbilda och delge information om informationssäkerhetet IT