Informationssäkerhetspolicy IT

(0:0:0)

Antagen av kommunfullmäktige
2014-02-24, KF § 29

Vimmerby
kommun

Informationssäkerhetspolicy IT (0:0:0)

Kommunalförbundet ITSAM och dess medlemskommuner

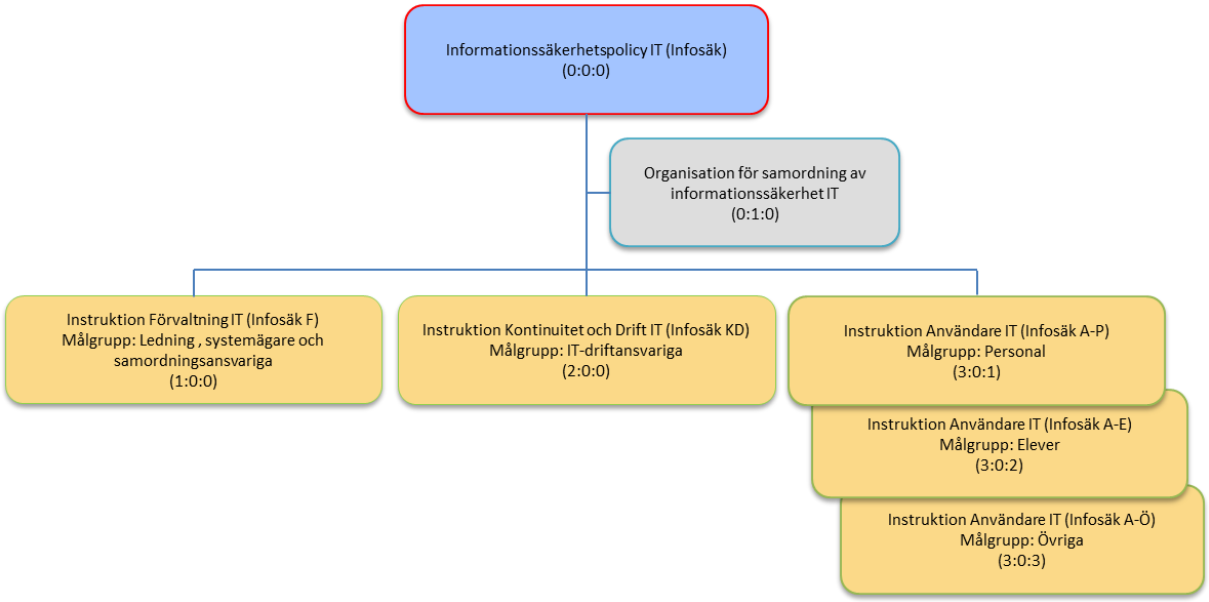
Revision: 2013031201
Fastställd: Direktionen 20130926
Dnr:0036/13

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

Innehåll

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 enlig 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.

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

Antagen av kommunfullmäktige

2014-02-24, KF § 29

Vimmerby kommun

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

Kommunalförbundet ITSAM och dess medlemskommuner

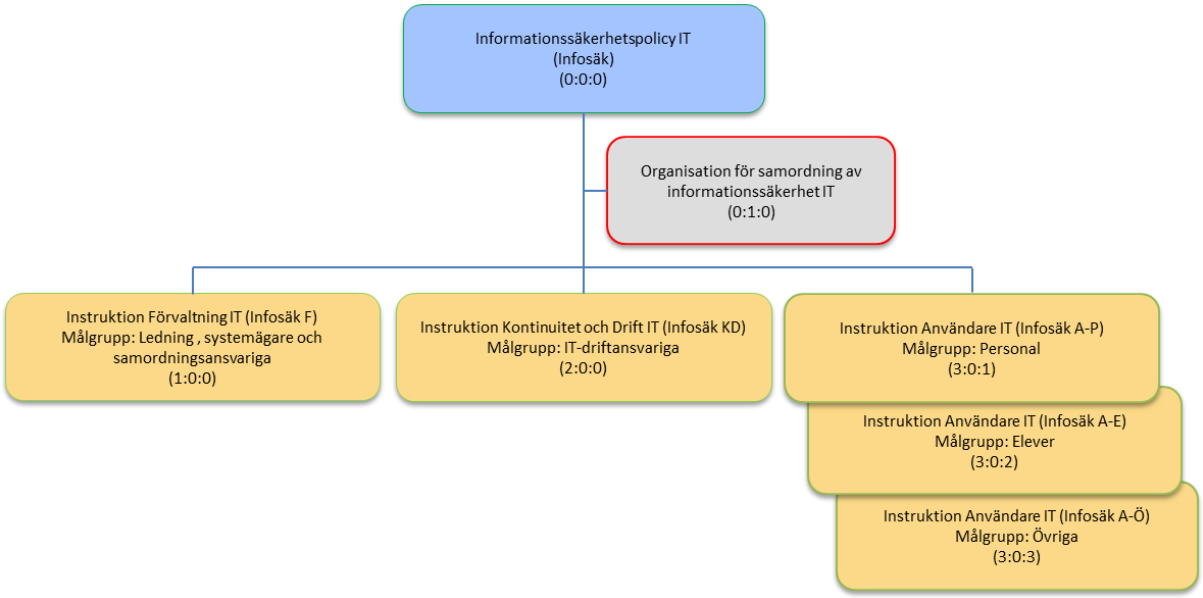
Revision: 2013031201
Fastställd: Direktionen 20130926
Dnr: 0036/13

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