HÖGSBY
KOMMUN

Informationssäkerhetsinstruktion Förvaltning (Infosäk F)

Dokumenttyp	**Dokumentnamn** Infosök F Högsby.doc	**Beslutad/Antaget** 2010-09-06 KF §130	**Version** 1.0
Dokumentägare Kommunstyrelsen	**Dokumentansvarig** IT-strateg	**Reviderad**	**Giltighetstid** 2010-

Informationssäkerhetsinstruktion: Förvaltning

1 Inledning

Informationssäkerhetsinstruktion Förvaltnings roll i Informationssäkerhetsarbetet

Informationssäkerhet är en del i kommunens lednings- och kvalitetsprocess som ska bidra till att ett informationssystem kan användas på avsett sätt och med avsedd funktionalitet.

Styrande dokument för Informationssäkerhetsarbetet är:

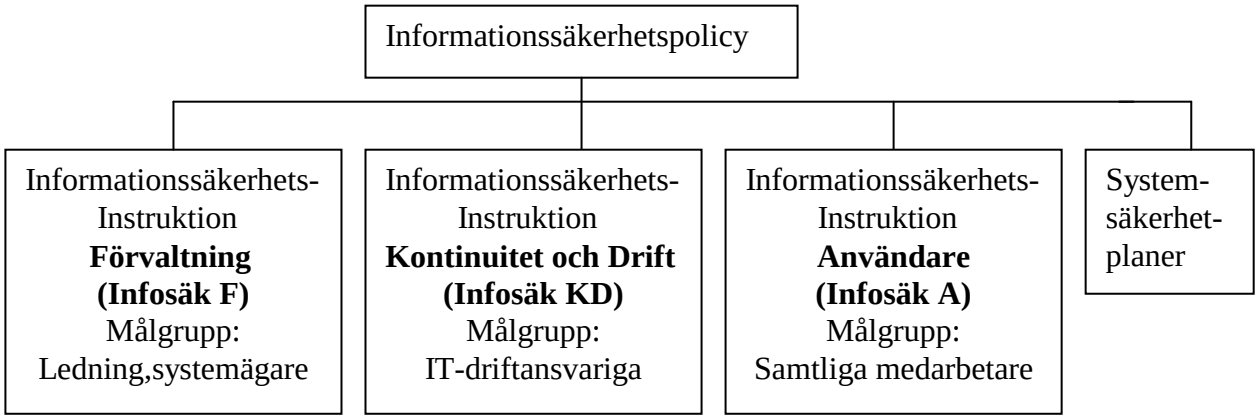

Bild 1 Styrande dokument

Informationssäkerhetspolicyn redovisar ledningens viljeinriktning och mål för Informationssäkerhetsarbetet. Detta dokument, Informationssäkerhetsinstruktion Förvaltning, utgår från Informationssäkerhetspolicyn och syftar till att redovisa:

- organisation och ansvar för Informationssäkerhetsarbetet
- beskriva omfattningen av det ansvar för Informationssäkerhetsarbetet som vilar på de roller som ingår i kommunen
- beskriva hur Informationssäkerhetsarbetet ska bedrivas
- regler för systemunderhåll och incidenthantering

2 Organisation och ansvar

Ansvaret för informationssäkerheten följer linjeorganisationen för varje enskilt informationssystem. Förvaltningschef/verksamhetschef/vd är i regel systemägare och ansvarig för informationssystem som stödjer den egna verksamheten. IT-strategen är systemägare för kommunens tekniska infrastruktur-IT.

Ett informationssystem, med alla dess delar, är en resurs i en verksamhet på samma sätt som personal, lokaler, kontorsmaterial m.m. Ansvarsfördelning och roller ska säkerställa att ett informationssystem kan administreras och hanteras på ett sådant sätt att det under hela sin livstid bidrar till att stödja avsedd verksamhet och uppfylla Informationssäkerhetspolicyns mål.

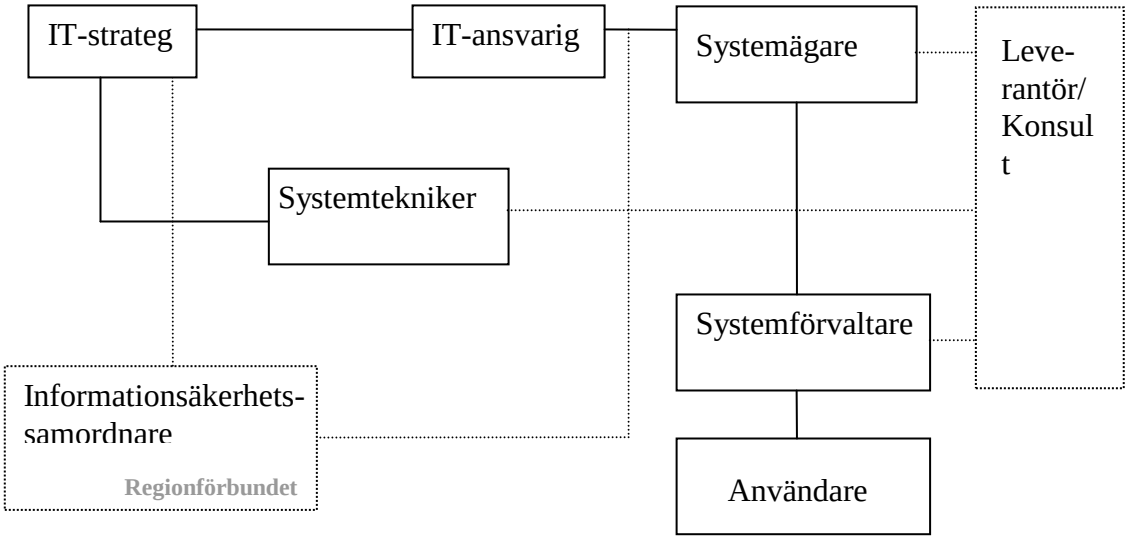

Bild 2 Roller i säkerhetsarbetet

2.1 Övergripande ansvar

Det övergripande ansvaret för kommunens informationssystem vilar på kommunstyrelsen. Ansvaret för informationssäkerheten följer linjeorganisationen för varje enskilt informationssystem. Kommunchefen utser systemägare/informationsägare HSA för samtliga informationssystem. Ledningen identifierar och kommunstyrelsen beslutar om vilka informationssystem som är samhällsviktiga/verksamhetskritiska enligt bilaga Systemförteckning. Systemägare för dessa samhällsviktiga system ansvarar för att en *systemsäkerhetsplan* (risk- och sårbarhetsanalys) upprättas.

2.2 IT-rådet

För att uppnå samsyn i IT-frågor har ett IT-råd inrättats. Gruppen ska, på uppdrag av ledningen, hantera och utreda IT-frågor och förbereda dessa för beslut. IT-strategen leder IT-beredningsgruppen. Gruppen består utöver IT-strateg av IT-ansvarig, ansvarig för outsorcad IT-drift, utvecklingsansvariga inom skola, Vård och omsorg och geografiska informationssystem GIS.

Inför den *årliga verksamhetsplaneringen* ska gruppen i samverkan med verksamhets/ områdescheferna inventera verksamheternas behov av IT-stöd kommande verksamhetsår (kortsiktigt mål) inom områdena:

- Införande. (Med införande avses alla frågor om nyanskaffning av system).
- Systemförvaltning. (Med systemförvaltning avses samtliga aktiviteter som görs för att verkställa alla typer av förändringar av redan existerande system)
- Driftfrågor.
- Systemavveckling. (Med systemavveckling avses samtliga aktiviteter som görs för att ett system tas ur drift)

När inventeringen gjorts analyserar och sammanställer gruppen behoven i form av förslag till årliga mål för kommande verksamhetsår i budget som överlämnas för beslut.

Gruppens uppgifter i övrigt är bl a att:

- medverka vid utformning av förslag på *långsiktiga mål* för IT-verksamheten inom ovanstående områden
- under pågående verksamhetsår samverka med verksamhets/områdescheferna omkring frågor och uppdrag som uppstår inom ovanstående områden (t ex akuta behov, inkomna förslag mm)
- delta i utformningen av kommunens kontinuitetsplan
- planera för hur informationssäkerhetsfrågor från genomförda risk- och sårbarhetsanalyser ska hanteras
- samordna systemägarnas krav på den tekniska infrastrukturen (krav från systemsäkerhetsplaner)
- ansvara för utformning av sekretessförbindelser för konsulter och serviceföretag
- samordna att avtal med annan part som utför tjänst eller uppdrag åt kommunen innehåller en informationssäkerhet som motsvarar kommunens krav
- samordna kompetensutveckling hos verksamhetsansvariga inom områdena IT, juridik och kvalitet
- ansvara för underhåll av kommunens Informationssäkerhetspolicy och Informationssäkerhetsinstruktioner
- ansvara för upprättande och underhåll av kommunens systemförteckning

2.3 Systemägare

Systemägaren ansvarar inför ledningen för att egna system förvaltas på för verksamheten bästa sätt. Vid nyutveckling eller större förändringar av datasystem ska systemägaren alltid samråda med IT-strateg på ett tidigt stadium. Systemägaren fattar de avgörande besluten om systemets införande, förvaltning, drift och avveckling.

Systemägaren har ansvar för bl a följande inom ramen för ledningens resurstilldelning:

- att inför den årliga verksamhetsplaneringen, initiera och föreslå den egna verksamhetens behov av IT-stöd till IT-rådet (i form av kortfattade och översiktliga mål och krav)
- att löpande följa upp att egna system stödjer verksamheten
- att delta i och stödja Informationssäkerhetsarbetet
- att en systemsäkerhetsplan upprättas
- att i systemsäkerhetsplanen fastställa eventuella tilläggskrav utöver basnivån för systemet utgående från
    - den information systemet hanterar
    - lagar, förordningar och författningar
    - verksamhetens krav på säkerhet vad avser sekretess, riktighet och tillgänglighet
    - hotbilden mot informationen
    - vilka olika behörighetsprofiler som ska gälla
    - omfattning av loggning (trans- och säkerhetsloggar)
    - hur loggar ska följas upp, arkiveras, förvaras och sparas
    - längsta acceptabla tid för driftavbrott och/eller informationsbortfall
    - tid för hur snabbt återläsning av säkerhetskopierat material ska kunna ske
- att fastställa systemets dokumentation och användarhandledning
- utbildning som rör systemet
- att, i samråd med IT-strateg, säkerställa att systemet fungerar ihop med samverkande system
- att fatta beslut om förvaltning av systemet och samverka med IT-rådet då systemförändringar aktualiseras
- att lämna förslag på att system som inte i tillräcklig grad är till gagn för verksamheten avvecklas
- att behövliga licenser respektive tillstånd finns
- att i samverkan med IT-strateg fastställa avbrottsplan för systemet
- att driftgodkänna systemet
- att besluta om vilka delar i informationen som är sekretessbelagda

2.4 Systemförvaltare

Systemförvaltare utses av systemägaren och är den person i berörd verksamhet som har ansvaret för den dagliga användningen av systemet.
I detta ingår

- att delta i och stödja Informationssäkerhetsarbetet
- att verkställa systemägarens beslut
- att sköta användar- och behörighetsadministration
- att behörighetstilldelningen till systemet sker på avsett sätt
- att hålla sig informerad om utvecklingen av systemet och påtala behov av förändringar till systemägaren för vidare befordran till IT-rådet
- att dokumentera uppkomna fel, brister och incidenter i systemet och rapportera dessa till systemägaren och IT-strategen
- att ansvara för att koordinera planering av datum för produktionssättning inför nya releaser/versioner
- att medverka i tester vid uppdateringar och felrättningar
- att bevaka att systemet hålls uppdaterat med buggfixar och säkerhetsuppdateringar
- att upprätta förteckning över förslag till förändringar från användare till systemägaren
- att ansvara för användarstöd beträffande verksamhetsrelaterade frågor i systemet
- att samverka med IT-avdelningen och delta i arbetet med säkerhetsfrågor som rör systemet
- att vara kontaktperson gentemot IT-avdelningen
- att vara kontaktperson gentemot leverantören i frågor om systemets funktion
- att i samverkan med IT-avdelningen ta fram installationshandvisning för systemet
- att reservrutiner enligt kontinuitetsplaneringen är kända
- att driften och utvecklingen av systemet följer fastställd säkerhetsnivå
- att användarna av systemet får erforderlig utbildning och information om användarinstruktioner
- att samverka med systemtekniker för att säkerställa driften av systemet

2.5 IT-ansvarig

IT-ansvarig, för närvarande kommunchef, är övergripande ansvarig för hela IT-verksamheten inkl IT-säkerhet samt för IT-verksamhetens budget och ekonomisk uppföljning. IT-ansvarig understödjer arbetet med att uppnå målen i Informationssäkerhetspolicyn.

IT-Ansvarig har ansvar för:

- att delta i och stödja Informationssäkerhetsarbetet
- delta i utformning av förslag på den strategiskt långsiktiga och övergripande IT-utvecklingen och förankra förslagen i ledningen inför politiskt beslut
- att rutiner för säkerhetskopiering uppfyller systemägarnas krav
- att reservrutiner, serviceavtal mm finns så att systemägarnas krav på längsta tillåtna avbrottstid kan tillgodoses
- att arbetsstationer (PC), nätverk och gemensamma resurser har tillräcklig kapacitet
- rapportera Informationssäkerhetsincidenter för ledningen

2.6 IT-strateg

IT-strateg är systemägare inom området teknisk infrastruktur och har det övergripande ansvaret för att ett systems tekniska delar fungerar. IT-strateg samverkar med systemägare vad avser drift och resurstilldelning för ett system. IT-strateg understödjer arbetet med att uppnå målen i Informationssäkerhetspolicyn.

IT-strateg har ansvar för:

- att systemsäkerhetsplan för teknisk infrastruktur –IT upprättas och hålls aktuell
- att samordna IT-säkerhetsarbetet inom kommunen

- att efter beställning tilldela och administrera behörigheter till den gemensamma infrastrukturen
- delta i utformning av förslag på den strategiskt långsiktiga och övergripande IT-utvecklingen
- att omvärldsbevakning sker och avrapporteras regelbundet till IT-rådet
- att systemägares krav enligt systemsäkerhetsplaner omsätts i den tekniska infrastrukturen
- att ett system håller den tekniska och funktionella kvalitet som överenskommits med systemägaren
- att i samråd med systemägare se till att systemet fungerar ihop med samverkande system
- att testmiljö finns tillgänglig vid behov
- att samordna så att rutiner för säkerhetskopiering uppfyller systemägarnas krav
- att biträda systemägarna i avbrottsplaneringen
- att samordna så att reservrutiner, serviceavtal mm finns så att systemägarnas krav på längsta tillåtna avbrottstid kan tillgodoses
- att samordna teknisk rådgivning till systemägarna då förändringar i systemen är aktuella
- att samordna så att arbetsstationer (PC), nätverk och gemensamma resurser har tillräcklig kapacitet
- att Informationssäkerhetsinstruktion: Drift och Kontinuitet är aktuell
- sammanställa och rapportera Informationssäkerhetsincidenter till IT-ansvarig
- att stödja systemägarna i informationssäkerhetsarbetet

2.7 Systemtekniker

Systemteknikern tillhör egen alt outsourcingpartners IT-avdelning, innehar den tekniska kompetensen och ansvarar tillsammans med systemägare och systemförvaltare för att den dagliga driften upprätthålls enligt överenskommelse mellan systemägaren och IT-strateg. Systemtekniker utför på uppdrag av systemägare och systemförvaltare överenskomna tekniska drift- och servicerutiner och har tillgång till installationshandvisningar från respektive systemförvaltare.

Systemteknikern har bl a följande uppgifter:

- registrera/avregistrera användare i systemet (infrastrukturen) med den behörighetsprofil som systemägaren har beslutat
- tillhandahålla teknisk support för användare (helpdesk)
- delta i och stödja Informationssäkerhetsarbetet
- att ett system håller den tekniska och funktionella kvalitet som överenskommits med systemägaren
- initiera felsökning vid driftsstörningar och vidta nödvändiga åtgärder och dokumentera dessa
- ansvara för att rutiner för säkerhetskopiering och förvaring av säkerhetskopierat material följs
- att teknisk infrastruktur - IT hålls uppdaterad med buggfixar och säkerhetsuppdateringar.
- att säkerhetskopierat material förvaras på ett betryggande sätt och att det regelbundet kontrolleras att återläsningsrutiner fungerar
- ansvarar för administration av kommunens brandväggar och skydd mot skadlig kod
- ansvarar för dokumentation av rutiner, utformning och konfiguration av den tekniska infrastrukturen

2.8 Användare

Varje användare ska följa gällande regler för Informationssäkerhet. I detta ansvar ingår att

- delta i och stödja informationssäkerhetsarbetet
- noga ta del av och följa aktuella säkerhetsinstruktioner för användare, Infosäk A
- rapportera olika former fel, brister och incidenter, t ex misstänkt virusangrepp enligt fastställda rutiner

- föreslå förändringar till systemägare/systemförvaltare
- påtala egna behov av utbildning

2.9 Informationssäkerhetssamordnare

Informationssäkerhetssamordnaren stödjer arbetet med att uppnå Informationssäkerhetspolicyns mål. Detta kan innebära aktivt deltagande i projekt, etablerande av interna och externa kontaktnät, utvärdering och deltagande i diskussioner kring metoder, plattformar eller system. Informationssäkerhetssamordnaren kan sägas arbeta som konsult åt verksamheten och står i direkt kontakt med IT-strateg. Informationssäkerhetssamordnaren stödjer Informationssäkerhetsarbetet inom kommunen och har till uppgift att:

- följa upp att Informationssäkerhetspolicy och Informationssäkerhetsinstruktionerna revideras och hålls aktuella
- vara rådgivande i Informationssäkerhetsfrågor
- stödja IT-rådet vid upprättande av Informationssäkerhetsinstruktioner
- stödja IT-strateg vid upprättande av systemsäkerhetsplan samt kontinuitetsplanering för teknisk infrastruktur- IT
- stödja systemägarna vid:
    - upprättande av systemsäkerhetsplan för respektive system
    - upprättande av kontinuitetsplanering för verksamheten
    - säkerhetsgranskning inför driftgodkännande
    - utbildning i Informationssäkerhetsfrågor
- följa upp hur Informationssäkerhetspolicyn efterlevs och delta i Informationssäkerhetsrevisioner

Detaljerad beskrivning av Informationssäkerhetssamordnarens uppdrag finns beskrivet i Avtal mot Regionförbundet, se bilaga Avtal om Informationssäkerhetssamordnare.

3 Informationssäkerhetsutbildning

Information och utbildning inom Informationssäkerhetsområdet ska ges alla medarbetare och omfatta:

- Informationssäkerhetens betydelse för verksamheten
- Innehållet i kommunens Informationssäkerhetspolicy
- Innehållet i Infosäk A och tillämpliga delar av innehållet i Infosäk F och Infosäk KD

Nya medarbetare ska ges information om säkerhetsfrågor före tilldelning av behörighet i nätverket. Närmaste chef ansvarar för att informera om Informationssäkerhetspolicyn, Infosäk A och att medarbetaren har tagit del av broschyren ”Viktig info om känslig info” samt kvitterat detta med skriftlig underskrift.

Systemägare ansvarar för

- att egna medarbetarna erhåller information och utbildning om innehållet i de systemsäkerhetsplaner de är berörda av
- att medarbetare, före tilldelning av behörighet, har tillräckliga kunskaper om säkerhetsreglerna för de system de behöver för de egna arbetsuppgifterna.

Varje enskild medarbetare har ett ansvar att påtala det egna behovet av utbildning.

4 Särskilda rutiner

4.1 Åtkomst till IT-resurser

För att säkerställa att endast behöriga användare förekommer i systemen ska följande rutiner gälla:

4.1.1 Behörighetsadministration

Beställning av åtkomst till IT-infrastrukturen (fileserver, e-post, m m) ska ske på blankett som finns på Intranätet. Verksamhetsansvarig chef är behörig beställare. IT-strateg är mottagare av beställningen och administrerar behörigheter.

Om medarbetare ska ha behörighet till ett verksamhetssystem ska verksamhetsansvarig chef beställa behörighet hos respektive systemförvaltare.

Verksamhetsansvarig chef ska snarast se till att behörigheter återkallas eller ändras om medarbetare slutar eller byter arbetsuppgifter.

4.1.2 Behörighetskontroll

Leverantörslösenord och behörigheter ska förvaras inlåsta, lämpligen både på IT-avdelningen och hos systemförvaltare. Leverantörslösenord är ofta standardiserade och ska därför ändras i anslutning till installationsfasen. Konsulter/leverantörer som vill koppla upp sig via distans måste kontakta IT-avdelningen för instruktioner.

4.1.3 Loggning och spårbarhet

Systemägarnas krav på säkerhets- och transaktionsloggar ska framgå av de systemsäkerhetsplaner som respektive systemägare upprättar.

4.1.4 Informationsklassning

Regler för klassning av information ska framgå av Infosäk A.

4.1.5 Distansarbete, extern anslutning och mobil datoranvändning (bärbar dator)

Systemägare beslutar om ett systems information ska få hanteras på distans med stationär eller mobil utrustning. Organiserat distansarbete ska vara reglerat i kollektivavtal mellan arbetsgivare och den anställde. För extern anslutning och mobil datoranvändning ska särskilda riktlinjer finnas. (Se Infosäk A).

Avtalet och säkerhetsinstruktionen ska minst reglera

- fysiskt skydd i eller utanför hemmet (stöldrisk)
- logiskt skydd (otillbörlig användning) dvs om kryptering krävs vid överföring i vissa fall (obehörig tillgång och förändring) och nivå på autenticering vid uppkoppling mot arbetsgivarens nätverk (obehörig tillgång och förändring).
- om utrustningen endast får användas för arbetsgivarens arbete (virussmitta o.dyl.)
- hantering av utskrifter (obehörig tillgång)
- om lagring och säkerhetskopiering av information ska ske i egen dator eller hos arbetsgivaren (stöldrisk, obehörig tillgång och förstörelse m.m.)
- rutiner för kontroll av skydd mot skadlig programkod (virussmitta o.dyl.)
- hantering av information på mobila enheter såsom CD/DVD-skivor, USB-minne, bärbar dator m.m.

Kommunen ska tillhandahålla utrustningen. Enbart kommunens utrustning får anslutas mot kommunens nätverk.

4.2 Drift och förvaltning av system

Inför den årliga verksamhetsplaneringen inventerar IT-rådet verksamheternas behov av IT-stöd, Gruppen analyserar och klassificerar behoven inom något av områdena (införande, förvaltning, drift eller avveckling) och lämnar förslag på årliga mål kommande verksamhetsår (om möjligt i prioritetsordning) för beslut. Förslag kan också avse långsiktiga mål beroende på ärendets karaktär.

När beslut har fattats förtydligar IT-rådet dessa i form av riktlinjer och anvisningar för hur de ska förverkligas. Utifrån klassificering utformas dessa i projektplaner enligt nedan.

4.2.1 Införande av system

För att klara en lokal anpassning vid införande av ett system ska verksamhetsansvarig chef i samråd med IT-rådet utforma en projektplan för införandet. Denna plan ska omfatta följande (i tillämpliga delar):

- Verksamhetens beskrivning av behov och mål med anskaffningen
- En risk- och sårbarhetsbedömning

  Risk- och sårbarhetsbedömningen är ett viktigt underlag för den kravspecifikation som ska upprättas och syftar bl. a. till att klarlägga de säkerhetskrav som verksamhetens ställer i form av:
  - krav på säkerhet avseende sekretess, riktighet och tillgänglighet
  - rättsliga, -verksamhets-, och hotrelaterade krav
  - kommunikationsberoende (internt och externt)
  - reservrutiner mm.
- Kravspecifikation

  Kraven från risk- och sårbarhetsbedömningen utökas med bl a:
  - Integrationskrav med andra system
  - Krav vid införande
  - Krav på test och acceptans
  - Om systemet anses som samhällsviktigt
  - ytterligare krav som ska gälla fram till den tidpunkt då den tilltänkte systemägaren övertar ansvaret och att systemet övergår till normal systemförvaltning mm i den kravspecifikation som ska utgöra grunden för upphandlingen
  - tidplan
  - resurser (personella och ekonomiska)
  - när och hur uppföljning, utvärdering och avrapportering ska ske
  - när och hur medarbetarna ska informeras och utbildas

4.2.2 Avveckling av system

System som inte längre behövs för verksamheten ska avvecklas snarast. Systemägare ska efter samråd med IT-rådet besluta om och när ett system ska avvecklas.. Vid avveckling ska särskilt uppmärksammas:

- Rättsliga regler såsom Arkivlagen, PUL
- Vad ska tas ut ur systemet före avveckling (på papper eller media)
- Innehåller systemet ärenden vilka behöver avslutas i diariet
- Behöver återläsning av innehåll kunna ske längre fram
- Behöver uppgifter flyttas över till annat system
- Destruktion av media som innehållit information
- Regler för destruktion av media som innehållit sekretessbelagd information

4.2.3 Drift

Kommunens regler för systemdrift ska vara samlade i Infosäk KD som ska innehålla:

- Systemdokumentationer
- Driftdokumentationer
- Bemanningsplan (nyckelpersonberoende)
- Tillträdes- och brandskydd
- Elförsörjning
- Regler för säkerhetskopiering
- Regler för förvaring av datamedia
- Regler för avveckling av datamedia

Den tekniska IT-infrastrukturen ska vara dokumenterad i särskild systemsäkerhetsplan.

4.2.4 IT-incidenthantering

Att återkoppla erfarenheter från incidenter av olika slag är ett viktigt moment när det gäller att spåra brister och svagheter i IT-verksamheten. Riktlinjer för hur incidenter följs upp är därför angelägna. Följande gäller:

- vid misstanke om intrång eller andra incidenter ska användare agera enligt Infosäk A

IT-strateg och IT-systemtekniker ska sammanställa och rapportera till IT-ansvarig:

- intrång och försök till intrång
- brott mot lagstiftning och internt regelverk
- incidenter som orsakar eller skulle kunna orsaka betydande avbrott och störningar.

4.2.5 Tillträdesskydd

IT-ansvarig ska besluta om vilka som ska ha tillträde till datorrum. För att kunna följa upp detta ska besök vara registrerade.

4.2.6 Säkerhetskopiering och lagring

Systemägarnas krav på säkerhetskopiering och lagring för de egna systemen ska framgå av de systemsäkerhetsplaner som respektive systemägare upprättar. Kraven i dessa planer ska vara koordinerade i systemsäkerhetsplan för IT-infrastrukturen.

Upprättade dokument och handlingar ska lagras i kommunens arkivstruktur. Handlingar som innehåller sekretess ska lagras enligt Infosäk A.

4.2.6.1 Avveckling av datamedia

Datamedia med sekretessbelagd information som ska avvecklas i enlighet med systemägarens instruktioner.

4.3 Datakommunikation

4.3.1 Interna kommunikation

Kommunens nät ska vara väl dokumenterat.

4.3.2 Externa anslutningar

Kommunen är för sin verksamhet beroende av datakommunikation med andra kommuner och centrala myndigheter främst via Internet.

Följande riktlinjer gäller:

- För att försvåra för obehöriga att göra intrång kommunens datasystem via externa anslutningar ska det finnas en s k brandvägg installerad
- Kontroller ska ske av vem som får komma ut och vem som får släppas in
- En kontrollista på vilka nätverksadresser och IP-portar som är tillåtna ska användas för att filtrera bort onödig trafik
- Användningen av tjänster ska fastställas och dokumenteras vad gäller kommunikationsriktning, vilka protokoll som ska stödjas samt vilka applikationer som använder protokollen

4.3.3 Brandväggar

IT-strateg ska efter samråd med IT-rådet och systemtekniker besluta om:

- Vad som ska loggas i brandväggen
- Vem som ansvarar för uppföljning av loggar
- Hur ofta uppföljning ska ske
- Hur länge loggarna ska sparas

4.3.4 Användningen av e-post och Internet

Riktlinjer för användningen av Internet och e-post ska framgå av Infosäk A.

I e-postsystemet ska finnas en loggningsfunktion där inkommande och utgående e-post registreras så att alla meddelanden kan spåras. Loggning ska ske av Internettrafiken för att möjliggöra spårning av intrång och missbruk.

5 Kontinuitetsplanering

Av systemsäkerhetsplanerna ska framgå de enskilda systemens krav på avbrotts- och katastrofplanering. Kraven ska vara sammanställda i systemsäkerhetsplanen för den tekniska infrastrukturen.

6 Driftgodkännande

Driftgodkännande avser den process som syftar till att fastställa om ett system uppfyller ställda säkerhetskrav.

I samband med att en systemsäkerhetsplan upprättas granskas om systemet uppfyller
- basnivå
- de tilläggskrav som ställs utifrån rättsliga, verksamhetsspecifika och hotrelaterade krav

Systemägaren beslutar om driftgodkännande. Beslutet baseras på en granskning och säkerhetsutvärdering som bygger på jämförelse mellan verksamheternas krav och vidtagna säkerhetsåtgärder. Driftgodkännandeprocessen relateras till aktuell systemsäkerhetsplan och ska omfatta:
- granskning av säkerhetsåtgärder i systemet
- utvärdering av granskningen i förhållande till systemsäkerhetsplanens krav
- redovisning av beslutsunderlag samt
- beslut

Beslutsunderlaget ska innehålla en sammanfattning av förslag till beslut som kan vara att:
- driftgodkänna systemet
- driftgodkänna systemet efter beslut om när kompletterande säkerhetsåtgärder ska vara genomförda
- inte driftgodkänna systemet.