



**Hässelholms
kommun**

KOMMUNAL
FÖRFATTNINGSSAMLING G 31

1(1)

Gäller från
2011-03-02

Diarienummer
2010/1037

Antagen: kommunstyrelsen 2007-02-28 § 24 och ändrad senast 2011-03-02 § 78

Informationssäkerhetsinstruktion - Förvaltning

Se bilaga

Informationssäkerhetsinstruktion

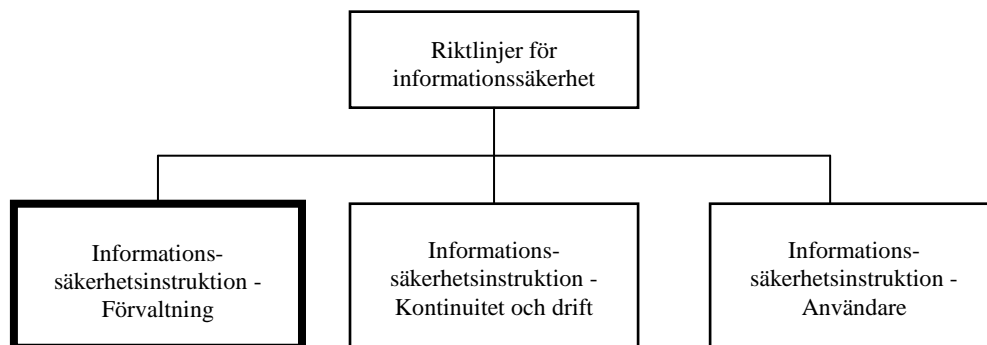
Förvaltning

INNEHÅLL

1	INLEDNING	3
2	ORGANISATION OCH ANSVAR.....	3
2.1	Övergripande ansvar	4
2.2	IT-styrgrupp	4
2.3	IT-säkerhetschef.....	4
2.4	Systemägare	4
2.5	Referensgrupper.....	5
2.6	Systemförvaltare	5
2.7	Användare.....	6
2.8	IT-driftchef.....	6
2.9	Driftansvariga	6
2.10	Informationssäkerhetsledning.....	6
3	SYSTEMANSKAFFNING, -FÖRVALTNING OCH -AVVECKLING.....	6
3.1	Systemanskaffning.....	6
3.2	Systemförvaltning	7
3.3	Systemdrift.....	8
3.4	Systemavveckling	8
4	GRANSKNING OCH DRIFTGODKÄNNANDE	8
5	UTBILDNING OCH INFORMATION	9
6	BEHÖRIGHETSADMINISTRATION.....	9
7	SÄKERHET I NÄTVERK OCH GEMENSAMMA SYSTEM	9
8	DISTANSARBETE OCH MOBIL DATORANVÄNDNING	9
9	IT-INCIDENTHANTERING	9
10	KONTINUITETSPLANERING	9

1 INLEDNING

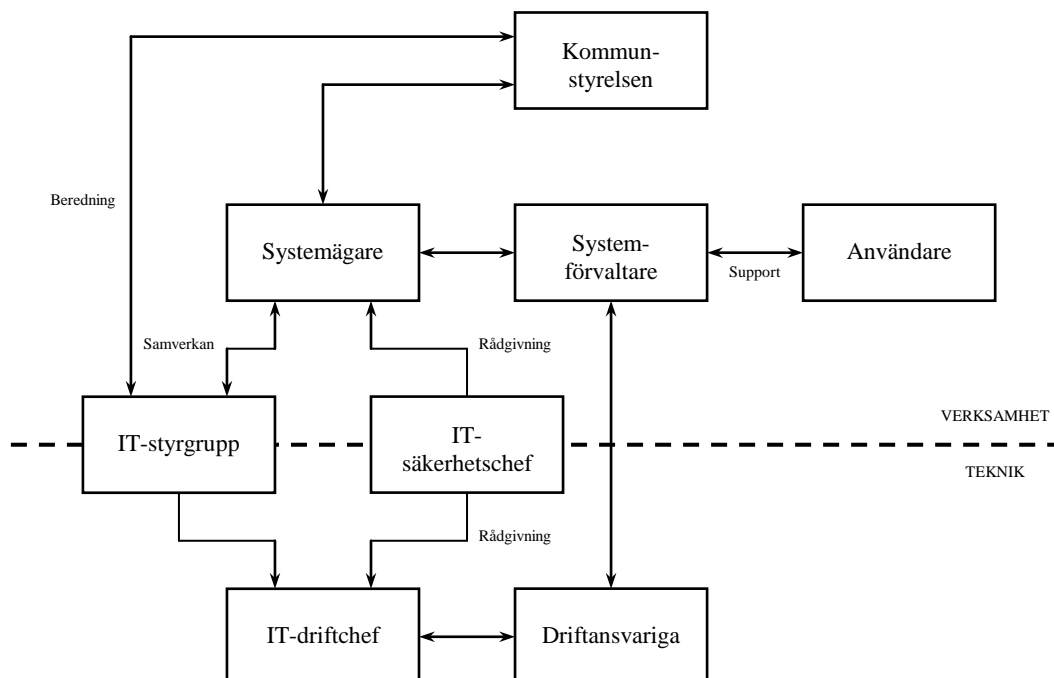
Denna informationssäkerhetsinstruktion är en konkretisering av Hässleholms kommuns riktlinjer för informationssäkerhet. Instruktionen beskriver omfattningen av det ansvar för informationssäkerheten som vilar på de roller som beskrivs i riktlinjerna.



Riktlinjer för informationssäkerhet och informationssäkerhetsinstruktioner

2 ORGANISATION OCH ANSVAR

En fastställd ansvarsfördelning är en avgörande förutsättning för att Hässleholms kommun ska kunna uppfylla informationssäkerhetsmålen. Kommunen eftersträvar att ansvaret ska följa linjeorganisationen för varje enskilt IT-system. Följaktligen är respektive förvaltningschef i regel systemägare och ansvarig för IT-system som stöder den egna verksamheten.



Roller inom informationssäkerhetsområdet

2.1 Övergripande ansvar

Det övergripande ansvaret för kommunens informationssäkerhet vilar på kommunstyrelsen.

2.2 IT-styrgrupp

IT-styrgruppen ska, på uppdrag av kommunstyrelsen, hantera och utreda generella frågor avseende anskaffning, drift, förvaltning och avveckling av informationshanteringsresurser. Inom ramen för detta ingår frågor som avser informationssäkerhet.

2.3 IT-säkerhetschef

IT-säkerhetschefen stöder arbetet med att uppnå informationssäkerhetsmålen och har till uppgift att

- ansvara för att *Riktlinjer för informationssäkerhet* samt *Informationssäkerhetsinstruktion - Förvaltning* och *Informationssäkerhetsinstruktion - Användare* hålls aktuella,
- fastställa vilka system som ska betraktas som samhällsviktiga,
- vara rådgivande till systemägarna i informationssäkerhetsfrågor och
- biträda systemägarna med att
 - upprätta en systemsäkerhetsplan,
 - upprätta en kontinuitetsplan för verksamheten,
 - genomföra säkerhetsgranskning inför driftgodkännande,
 - medverka vid utbildning i informationssäkerhetsfrågor,
 - samordna uppföljning och incidentrapportering och
 - följa upp hur *Riktlinjer för informationssäkerhet* efterlevs.

2.4 Systemägare

Systemägaren ansvarar för att egna IT-system förvaltas på för verksamheten bästa sätt och fattar de avgörande besluten om IT-systemets anskaffning, drift, förvaltning och avveckling.

Systemägaren har ansvar för att

- initiera och föreslå den egna verksamhetens behov av IT-stöd till IT-styrgruppen (i form av kortfattade och översiktliga mål och krav),
- i en systemsäkerhetsplan fastställa tilläggskrav utöver basnivån (gäller i första hand samhällsviktiga IT-system) utifrån
 - det informationsinnehåll IT-systemet ska ha,
 - de lagar och förordningar som gäller för systemet,
 - krav på säkerhet avseende sekretess, riktighet och tillgänglighet,
 - hotbilden för IT-systemet,
 - vilka olika behörighetsprofiler som ska gälla,
 - omfattning av loggning (transaktions- och säkerhetsloggar),
 - krav på hur loggar ska följas upp, arkiveras och förvaras,
 - längsta acceptabla tid för driftavbrott,
 - krav på säkerhetskopiering och på hur snabbt återläsning av säkerhetskopierat material ska kunna ske,

- driftgodkänna systemet (gäller i första hand samhällsviktiga IT-system),
- fastställa organisation och befattningar som rör systemet,
- utse systemförvaltare för systemet,
- vid behov utse en referensgrupp för systemet,
- fastställa IT-systemets dokumentation och användarhandledning,
- planera och genomföra utbildning i systemet,
- säkerställa att erforderliga licenser och tillstånd finns,
- besluta om förvaltning av IT-systemet och samverka med IT-styrgruppen då systemförändringar aktualiseras,
- löpande följa upp att systemet stöder verksamheten,
- i samverkan med driftansvarig fastställa en kontinuitetsplan för IT-systemet,
- i samråd med driftansvarig säkerställa att systemet fungerar ihop med samverkande IT-system,
- följa upp systemets ekonomi avseende utveckling och användning samt tillsammans med driftansvarig avseende teknisk drift och
- föreslå avveckling av system som inte i tillräcklig grad gagnar verksamheten.

2.5 Referensgrupper

För system som berör flera verksamheter och därmed också flera verksamhetschefer ansvarar systemägaren för att vid behov utse en lämpligt sammansatt referensgrupp för systemet. Referensgruppens uppgift är bland annat att fortlöpande lämna synpunkter till systemägaren på IT-systemet och hur detta kan utvecklas.

2.6 Systemförvaltare

Systemförvaltaren utses av systemägaren och ansvarar för IT-systemets systemsäkerhetsplan och förvaltning samt för den dagliga användningen av systemet. Systemförvaltaren samverkar med driftansvarig för att säkerställa en säker och rationell drift av systemet.

Systemförvaltaren har ansvar för att

- verkställa beslut som systemägaren fattar,
- hålla sig informerad om utvecklingen av systemet och påtala behov av förändringar för systemägaren,
- dokumentera uppkomna fel, brister och incidenter och rapportera dessa till den centrala IT-supporten,
- initiera och planera för driftsättning av nya versioner,
- initiera och medverka i tester i samband med felrättningar och uppgraderingar,
- registrera/avregistrera användare med den behörighetsprofil som systemägaren har beslutat,
- ge support i verksamhetsrelaterade frågor,
- upprätta förteckning över förslag till förändringar,
- delta i arbetet med säkerhetsfrågor och
- informera om reservrutiner.

2.7 Användare

Varje användare ska följa gällande informationssäkerhetsregler. I detta ansvar ingår att

- noga ta del av och följa regler och anvisningar i *Informationssäkerhetsinstruktion - Användare*,
- rapportera om fel, brister och incidenter, till exempel virusangrepp, till den centrala IT-supporten samt
- framföra förslag till förändringar i systemet till systemförvaltaren.

2.8 IT-driftchef

IT-driftchefen är systemägare för kommunens tekniska IT-infrastruktur och ansvarar för att

- IT-infrastrukturen uppfyller de samlade kraven från samtliga systemsäkerhetsplaner,
- upprätta *Informationssäkerhetsinstruktion - Kontinuitet och drift*, och hålla denna aktuell,
- ta fram och underhålla en systemsäkerhetsplan för den tekniska IT-infrastrukturen samt
- utse en driftansvarig för respektive IT-system.

2.9 Driftansvariga

Driftansvarig utses av IT-driftchefen och ansvarar för att

- systemet fungerar ihop med samverkande IT-system,
- en lämplig testmiljö finns tillgänglig vid behov,
- rutinerna för säkerhetskopiering uppfyller systemägarens krav,
- säkerhetskopierat material förvaras på ett betryggande sätt och att regelbundet kontrollera att återläsningsrutinerna fungerar,
- reservrutiner, serviceavtal med mera finns, så att systemägarens krav på längsta tillåtna avbrottstid kan tillgodoses,
- biträda systemägaren i kontinuitetsplaneringen,
- vara teknisk rådgivare till systemägaren då förändringar i systemet är aktuella,
- gemensamma resurser har tillräcklig kapacitet,
- initiera felsökning vid driftstörningar och vidta nödvändiga åtgärder samt
- dokumentera uppkomna fel, brister och incidenter och rapportera dessa till den centrala IT-supporten.

2.10 Informationssäkerhetsledning

Vid större oplanerade IT-relaterade händelser tillämpas *Krisledningsplan för Hässleholms kommun*.

3 SYSTEMANSKAFNING, -FÖRVALTNING OCH -AVVECKLING

3.1 Systemanskaffning

När behov uppstår av större förändringar av befintligt IT-stöd eller av ett helt nytt IT-stöd ska samråd ske med övriga kommuner inom Skåne Nordost. En analys av förutsättningarna för samverkan kring IT-stödet ska genomföras. Resultatet överlämnas till kommunchefsgruppen för beslut om eventuell samverkan.

I de fall samverkan kan ske utser kommunchefsgruppen en projektledare och en projektgrupp bestående av verksamhetsföreträdare, en tekniskt ansvarig och en upphandlingsansvarig. Vid behov utses även en styrgrupp, till vilken projektledaren rapporterar.

Om samverkan med en eller flera andra kommuner inte är möjlig, ansvarar den verksamhetsansvarige chefen för systemanskaffningsprojektet.

Projektledaren/verksamhetsansvarig chef utformar en projektplan för nyanskaffningen. Denna ska omfatta

- en beskrivning av verksamhetens behov,
- mål med nyanskaffningen,
- en tidplan,
- resursbehov (personella och ekonomiska),
- en plan för när och hur uppföljning, utvärdering och avrapportering ska ske och
- en plan för när och hur medarbetarna ska informeras och utbildas.

Projektledaren/verksamhetsansvarig chef sammanställer också en kravspecifikation. Denna ska innehålla

- en risk- och sårbarhetsbedömning som klarlägger
 - verksamhetens krav på säkerhet avseende sekretess, riktighet och tillgänglighet,
 - tilläggskrav i form av rättsliga, verksamhets- och hotrelaterade krav,
 - krav på och beroende av kommunikation (internt och externt) och
 - reservrutiner samt
- krav på integration med andra system.

Projektplan och kravspecifikation överlämnas till kommunchefsgruppen/IT-styrgruppen för godkännande.

Nyanskaffning kan ske genom avrop från tillämpligt ramavtal eller genom upphandling i enlighet med lagen om offentlig upphandling. Om möjligt ska standardprodukter användas.

3.2 Systemförvaltning

Med systemförvaltning avses samtliga aktiviteter som görs för att styra, administrera och utveckla existerande system och stöda användandet (rätta, uppdatera, ändra, komplettera, utveckla med mera).

Vid samverkan kring förvaltning och drift av ett IT-system utser kommunchefsgruppen en central systemägare, en central systemförvaltare och en central driftansvarig hos värdkommunen. Övriga kommuner utser en lokal systemägare, en lokal systemförvaltare och en lokal driftansvarig.

För samhällsviktiga och/eller gemensamma system ska en systemsäkerhetsplan upprättas enligt BITS Plus, MSB:s (Myndigheten för samhällsskydd och beredskap) verktyg för informationssäkerhetsanalys. Av denna ska framgå

- om systemet uppfyller kraven enligt MSB:s råd om basnivå,
- om systemet omfattas av tilläggskrav i form av rättsliga krav, specifika verksamhetskrav och hotrelaterade krav samt
- systemägarens krav på kontinuitetsplan.

Om de förutsättningar som legat till grund för systemsäkerhetsplanen förändras ska planen revideras.

3.3 Systemdrift

Regler för systemdrift ska samlas i *Informationssäkerhetsinstruktion - Drift* och omfatta bland annat

- systemdokumentationer,
- driftdokumentationer,
- bemanningsplan (nyckelpersonberoende),
- tillträdes- och brandskydd,
- elförsörjning,
- regler för säkerhetskopiering och
- regler för förvaring av datamedia.

Kommunens interna nätverk ska vara dokumenterat i en särskild systemsäkerhetsplan.

3.4 Systemavveckling

Systemägaren beslutar om när ett IT-system ska avvecklas. Vid avveckling ska särskilt uppmärksammas

- arkivlagens regler,
- vad som ska tas ut ur systemet före avveckling (på papper eller datamedia),
- om systemet innehåller ärenden vilka behöver avslutas,
- om återläsning av innehållet måste kunna ske längre fram och
- om uppgifter behöver flyttas över till ett annat IT-system.

4 GRANSKNING OCH DRIFTGODKÄNNANDE

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

I samband med att en systemsäkerhetsplan upprättas granskas om IT-systemet uppfyller

- basnivå och
- de tilläggskrav som ställs utifrån rättsliga, verksamhetsspecifika och hotrelaterade krav.

Driftgodkännandeprocessen relateras till aktuell systemsäkerhetsplan och ska omfatta

- avgränsningar,
- granskning av säkerhetsåtgärder i IT-systemet,
- utvärdering av granskningen i förhållande till systemsäkerhetsplanens krav,
- redovisning av beslutsunderlag samt
- förslag till beslut.

Beslutsförslaget kan vara en rekommendation att

- driftgodkänna IT-systemet,
- driftgodkänna IT-systemet efter beslut om kompletterande säkerhetsåtgärder och när dessa ska vara genomförda eller
- inte driftgodkänna IT-systemet.

Systemägaren beslutar om driftgodkännande. Beslutet baseras på en granskning och säkerhetsutvärdering, som i sin tur bygger på en jämförelse mellan verksamhetens krav och vidtagna säkerhetsåtgärder.

5 UTBILDNING OCH INFORMATION

Systemägaren är ansvarig för att medarbetare, före tilldelning av behörighet, har tillräckliga kunskaper om säkerhetsreglerna för det IT-system de behöver för de egna arbetsuppgifterna. Utöver regelbundna utbildningar i det specifika systemet ska varje medarbetare ha utbildning om kommunens

- *Riktlinjer för informationssäkerhet och*
- *Informationssäkerhetsinstruktion - Användare.*

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

6 BEHÖRIGHETSADMINISTRATION

Utgångspunkten är att kommunens medarbetare endast ska ha tillgång till den information och de IT-resurser som krävs för att de ska kunna lösa sina arbetsuppgifter. Dessa rutiner reglerar tilldelning, ändring, uppföljning och borttagning av behörigheter.

Verksamhetschef ska, på delegation från systemägaren,

- besluta om användares behörighet till IT-systemen inom sin verksamhet,
- lämna skriftlig beställning till systemansvarig omfattande alla uppgifter som krävs för att lägga upp behörigheter och
- ansvara för den löpande uppföljningen av behörigheter.

Endast behörighetsadministratör ska kunna registrera vilka resurser en användare får utnyttja.

7 SÄKERHET I NÄTVERK OCH GEMENSAMMA SYSTEM

Reglerna för säkerhet i det interna nätverket, gemensamma IT-system och Internet framgår av *Informationssäkerhetsinstruktion - Användare.*

8 DISTANSARBETE OCH MOBIL DATORANVÄNDNING

Regler för arbete utanför kommunens lokaler som kräver uppkoppling mot det interna nätverket framgår av *Informationssäkerhetsinstruktion - Användare.*

9 IT-INCIDENTHANTERING

Incidenter kan vara interna eller externa intrång och intrångsförsök, felaktig användning av IT-system och IT-resurser m m. Hur användare ska agera vid misstanke om intrång framgår av *Informationssäkerhetsinstruktion - Användare.*

10 KONTINUITETSPLANERING

Kontinuitetsplaneringen framgår av *Informationssäkerhetsinstruktion - Kontinuitet och drift* och respektive systemsäkerhetsplan.