# Informationssäkerhetsinstruktion Förvaltning IT (1:0:0)

Kommunalförbundet ITSAM

Revision: 20151130
Ersätter: 20130227
Dnr: 2013/00036

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

# Innehåll

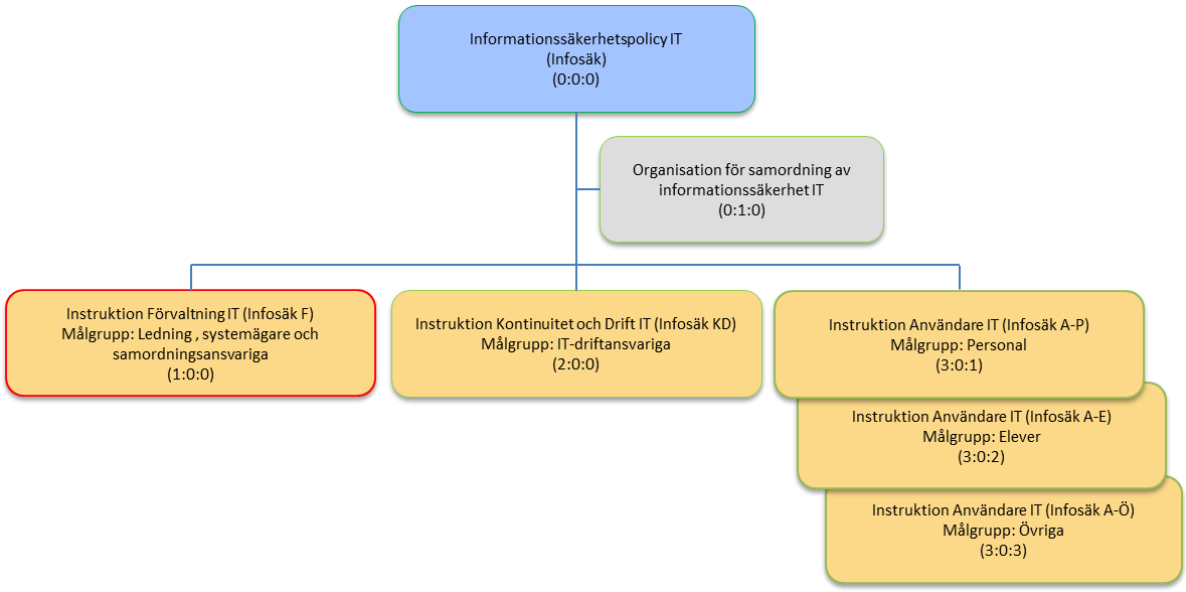
Innehåll ..... 3
Instruktionens roll i informationssäkerhetsarbetet ..... 5
1 Organisation och ansvar ..... 6
1.1 Direktion ..... 6
1.2 Stab (ledning) ..... 6
1.3 Informationssäkerhetsansvarig ..... 6
1.4 Systemägare ..... 6
1.5 Systemförvaltare ..... 6
1.6 Kommunalförbundet ITSAMs verkställande tjänsteman ..... 6
1.7 Systemtekniker ..... 7
1.8 Behörighetsansvarig ..... 7
1.9 Behörighetsadministratör ..... 7
1.10 Arkivansvarig ..... 7
1.11 Användare ..... 7
2 Regler och rutiner ..... 7
2.1 Ansvar för tillgångar ..... 7
2.2 Informationsklassificering ..... 8
2.3 Under anställningen ..... 8
2.4 Säkrade utrymmen ..... 8
2.5 Kontroll av utomstående tjänsteleverantör ..... 8
2.6 Hantering av datamedia ..... 8
2.7 Distribution av media ..... 8
2.8 Övervakning ..... 8
2.9 Styrning av användares åtkomst ..... 8
2.10 Styrning av åtkomst till nätverk ..... 9
2.11 Styrning av åtkomst till operativsystem ..... 9
2.12 Distansarbete ..... 9
2.13 Säkerhetskrav på system ..... 9

2.14 Säkerhet i utvecklings- och underhållsprocesser ..... 10

2.15 Hantering av informationssäkerhetsincidenter och förbättringar ..... 10

## Instruktionens roll i informationssäkerhetsarbetet

Styrande dokument är övergripande informationssäkerhetspolicy 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.




Informationssäkerhetspolicyn 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

# 1 Organisation och ansvar

## 1.1 Direktion

Kommunalförbundet ITSAMs direktion fattar inriktningsbesluten hur informationssäkerhetsarbetet inom IT ska bedrivas.

## 1.2 Stab (ledning)

Verkställande tjänsteman ska i enlighet med direktionens beslut se till att informationssäkerhetsarbetet efterlevs. Detta inkluderar frågor avseende anskaffning, drift, förvaltning och avveckling av informationshanteringsresurser.

## 1.3 Informationssäkerhetsansvarig

Informationssäkerhetsansvarig stödjer arbetet med att uppnå informationssäkerhetspolicyns mål och ansvarar för analyser av de delar av IT-stödet som är gemensamma för hela verksamheten. Informationssäkerhetsansvarig initierar och stödjer systemägarnas arbete med att genomföra enskilda systemsäkerhetsanalyser.

## 1.4 Systemägare

Inom ramen för antagna mål och resurser fattar systemägaren beslut om de egna systemens införande, drift, förvaltning och avveckling. Systemägaren ansvarar för att systemsäkerhetsanalyser för de egna systemen genomförs. Som systemägare ska för varje kommun finnas en utpekad person per system.

## 1.5 Systemförvaltare

Systemförvaltaren utses av systemägaren och är operativt ansvarig för systemet.
Systemförvaltaren

- ansvarar för att verkställa beslut fattade av systemägaren
- ansvarar för systemets funktionalitet och den dagliga användningen
- ansvarar för användar- och behörighetsadministration i systemet
- ansvarar för support i verksamhetsrelaterade frågor
- genomför erforderliga utbildningar
- dokumenterar uppkomna fel, brister och incidenter i systemet och rapporterar dessa till systemägaren och Kommunalförbundet ITSAM
- dokumenterar förslag till ändringar/utveckling av systemet
- är kontaktperson mot systemleverantör och Kommunalförbundet ITSAM
- deltar i arbetet med IT-säkerhetsfrågor
- initierar och medverkar i tester i samband med felrättningar och uppgraderingar

Som systemförvaltare ska för varje kommun finnas en utpekad person per system.

## 1.6 Kommunalförbundet ITSAMs verkställande tjänsteman

Kommunalförbundet ITSAMs verkställande tjänsteman är systemägare för de system som definieras som Core-system och som är vitala och strategiska för en fungerande IT-infrastruktur såsom den inom ITSAM. System som avses är förtecknade i systeminventeringen och exempel på sådana är e-post, fillager, IDM, metakatalog, system för certifikatutgivning etc. Verkställande tjänsteman ansvarar för att de strategiska systemens tekniska delar fungerar och att basnivåerna gällande drift och kontinuitet uppfylls. Verkställande tjänsteman för kommunalförbundet är ytterst:

- driftansvarig för kommunalförbundets olika IT-systems tekniska delar
- remissinstans i IT-frågor
- beställarkompetens inom IT-området
- systemägare för förvaltningsövergripande IT-system
- ansvarig för beslut tillsammans med andra systemägare vid disciplinära åtgärder av användare
- teknisk rådgivare till systemägare av förvaltningsspecifika system
- ansvarar för upphandlingar av hård- och mjukvara tillsammans med systemägare vilka har det fulla ekonomiska ansvaret
- ansvarig för att upprätta IT-systemsäkerhetsplan och medverkar i granskningsarbetet inför driftgodkännande av system
- teknisk rådgivare då förändringar i system är aktuella
- ansvarig för att driften av förvaltningsspecifika system sköts
- ansvarig för att IT-systemen håller den tekniska och funktionella kvalitet som överenskommits med systemägare och att systemen fungerar ihop med samverkande IT-system
- ansvarig för att tillhandahålla IT-utrustning med tillräcklig kapacitet och driftsäkerhet

### 1.7 Systemtekniker
Systemtekniker som tillhör Kommunalförbundet ITSAM, innehar den tekniska kompetensen, och ansvarar tillsammans med systemägare och systemförvaltare för att den dagliga driften upprätthålls enligt överenskommelse mellan systemägaren och verkställande tjänsteman eller av denne delegerad person.

### 1.8 Behörighetsansvarig
Se systemförvaltare.

### 1.9 Behörighetsadministratör
Se systemförvaltare.

### 1.10 Arkivansvarig
Arkivansvarig ansvarar dels för att informationsflöden dokumenteras och uppdateras kontinuerligt, dels ansvarar för att tillgängligheten till informationsmängder finns för rätt subjekt och dels ansvarar för att informationsmängder säkerhetskopieras och återställs vid behov.

### 1.11 Användare
Användare är de som i sitt dagliga arbete använder implementerade system och som har det yttersta ansvaret för att på ett regelmässigt vis hantera den tillgängliga informationen med avseende på integritet, sekretess och tillgänglighet.

## 2 Regler och rutiner

### 2.1 Ansvar för tillgångar
IT-utrustning ska vara förtecknad och inventerad. Av förteckningen ska framgå var tillgångarna är placerade samt vem som ansvarar för tillgången. Omflyttning och överlåtelse av tillgång får inte ske utan samråd med kommunalförbundet ITSAM.

## 2.2 Informationsklassificering
Regler för klassning av information framgår av *Infosäk A*.

## 2.3 Under anställningen
Information och utbildning av anställda omfattar:

- Innehållet i *Informationssäkerhetspolicy IT* och *Infosäk A-P, A-E och A-Ö*

Systemägare/verksamhetsansvarig ansvarar för att:

- nya användare ges grundläggande informationssäkerhetsutbildning före tilldelning av behörighet i systemet.
- användarhandledning för aktuellt system finns.
- medarbetare har tillräckliga kunskaper om säkerhetsreglerna för de system de behöver för de egna arbetsuppgifterna.

## 2.4 Säkrade utrymmen
Känslig information från system ska lagras på resurser i datorhallar som ska vara försedda med kontrollsystem för in- och utpassering. Utrymmen med kopplingspunkter ska vara låsta. Känslig information som inte hanteras i system ska förvaras i brandklassade säkerhetsskåp. Övervakning av servicepersonal, städpersonal m.fl. ska ske och beslut ska tas av VD eller av denne delegerad person om och när tillträde till säkrade utrymmen tillåts. Beslut skall dokumenteras.

## 2.5 Kontroll av utomstående tjänsteleverantör
Beställare av utomstående leverantörers tjänster ska följa upp och granska att överenskommelser gällande informations- och IT-säkerheten följs.

## 2.6 Hantering av datamedia
Datamedia med sekretessbelagd information som ska avvecklas överlämnas till kommunalförbundet som hanterar destruktion av media.

## 2.7 Distribution av media
Om media som innehåller känslig information måste transporteras fysiskt ska systemägaren kontaktas för beslut om tillvägagångssätt.

## 2.8 Övervakning
Systemloggar ska föras och för dessa ska systemägaren besluta:

- vad som ska loggas
- hur ofta loggarna ska analyseras
- vem som ansvarar för analyser av loggarna
- hur länge loggarna ska sparas
- hur loggarna ska förvaras

Detaljerad information samt anvisningar för användning och övervakning av loggfiler framgår av *separat dokument*, upprättat av systemägaren.

## 2.9 Styrning av användares åtkomst
För att säkerställa att endast behöriga användare förekommer i systemen ska beställning, borttagande eller ändring av åtkomst till system ske på föreskrivet sätt och dokumenteras enlig gällande rutiner. Media innehållande lösenord, PIN-koder och certifikatnycklar ska förvaras inlåsta.
Styrande dokument: *Informationssäkerhetsinstruktion A, Policy för åtkomstkontroll.*

## 2.10 Styrning av åtkomst till nätverk

Verkställande tjänsteman ansvarar för att genom anvisningar reglera:

- autentisering vid externa anslutningar
- anslutning av utrustning till interna och externa nätverk
- anslutning av externa nätverk till eget nät med ingående säkerhetsfunktioner, autentisering mm
- anslutning av trådlösa nät
- säkerhet vid Internetanslutning
- att en översikt av säkerhetsarkitekturer för interna nätverket och kommunikationsanslutningar upprättas
- administrationen av brandväggen samt besluta om vad som ska loggas i den, vem som ansvarar för uppföljningen av loggarna, hur ofta uppföljning ska ske och hur länge loggarna ska sparas
- att upprätta underlag för ledningens beslut om kommunikationstjänster

## 2.11 Styrning av åtkomst till operativsystem

Verkställande tjänsteman beslutar i vilken utsträckning användning av administrationsverktyg eller systemhjälpmedel som kan förbigå system- och tillämpningsspärrar ska användas.

## 2.12 Distansarbete

Systemägare beslutar om ett systems information ska få hanteras på distans. Distansarbete ska vara reglerat i avtal mellan arbetsgivaren och den anställde.
Styrande dokument: *Informationssäkerhetsinstruktion A, Policy för åtkomstkontroll*

## 2.13 Säkerhetskrav på system

Inför nyanskaffning och införande av ett system ska systemägare i samråd med kommunalförbundet utforma en projektplan för införandet.

Denna plan ska minst omfatta:

- beskrivning av behov och mål med anskaffningen
- en inledande systemsäkerhetsanalys
  Analysen syftar till att klarlägga säkerhetskraven på det system som planeras införas och den utökas därefter med en kravspecifikation som minst omfattar:
- integrationskrav med andra system
- krav på test
- tidplan
- personella och ekonomiska resurser
- fastställa omfattning av användarutbildning
- krav på acceptans
  Projektledare för nyanskaffningsprojekt förbereder överlämnandet från test och utveckling till drift och förvaltning tillsammans med den blivande systemägaren. Beslut om tidpunkt när systemet övergår från projekt till förvaltning fattas i samråd mellan kommunalförbundet och systemägaren. I och med överlämnandet övergår ansvaret till systemägaren som då också övertar all dokumentation och upprättar en systemsäkerhetsanalys.
- Driftgodkännande avser den process som syftar till att fastställa om ett system uppfyller ställda säkerhetskrav. Denna process omfattar följande steg:
- systemägare driftgodkänner sina system efter genomförd systemsäkerhetsanalys
- systemägaren koordinerar sina krav med informationssäkerhetsansvarig
- informationssäkerhetsansvarig ansvarar för att underlag för driftgodkännande behandlas av systemägaren samt undertecknas och arkiveras

## 2.14 Säkerhet i utvecklings- och underhållsprocesser

Förslag om önskemål på förändringar i systemet lämnas av systemförvaltaren till systemägaren. Arbetet bedrivs enligt organisationens process och rutin för införande och utveckling av systemet.

## 2.15 Hantering av informationssäkerhetsincidenter och förbättringar

Vid misstanke om intrång eller andra incidenter ska användare agera enligt *Informationssäkerhetsinstruktion A-P, A-E och A-Ö*. Informationssäkerhetsansvarig ska till verkställande tjänsteman och systemägare sammanställa och rapportera:

- intrång och försök till intrång
- brott mot lagstiftning och internt regelverk
- incidenter som orsakar eller skulle kunna orsaka betydande avbrott och störningar
- konsekvenser och förslag till åtgärder efter intrång eller funktionsfel