Informationssäkerhetsinstruktion
Användare: Personal
(3:0:0)

Kommunalförbundet ITSAM

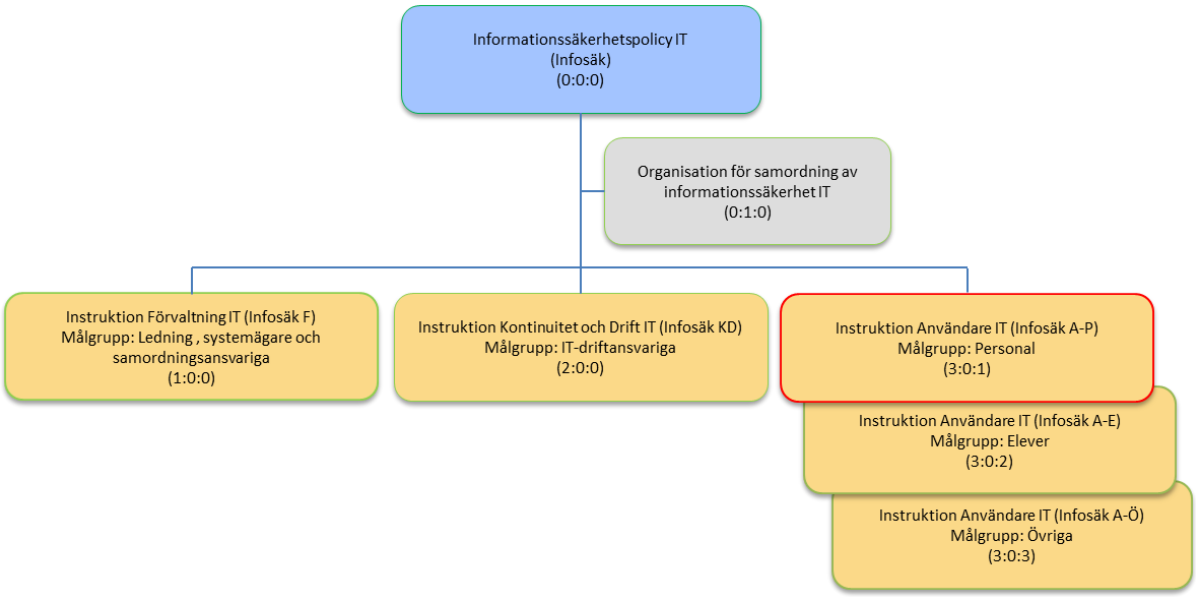
Revision: 20130317
Dnr: 2013/00036

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

Innehåll

Säkerhetsinstruktionens roll i informationssäkerhetsarbetet

Styrande dokument för informationssäkerhetsarbetet är övergripande informationssäkerhetspolicy IT med tillhörande underliggande policys samt dokument - Organisation för samordning av informationssäkerhet IT samt informationssäkerhetsinstruktionerna Förvaltning IT (Infosäk F), Kontinuitet och Drift IT (Infosäk KD) och Användare (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

Som personal räknas alla som har anställning i Kommunalförbundet ITSAM eller inom dess medlemskommuner samt förtroendevalda. Personal ska också räknas de som utför löpande arbete inom ordinarie kommunala funktioner men som tillhör en extern samarbetsorganisation.

1. Användarens ansvar

Information är en viktig tillgång för organisationerna. För att skydda denna krävs ett säkerhetsmedvetande hos alla användare. Som användare har man del i ansvaret för säkerheten i informationshanteringen.

För stöd och hjälp när det gäller användningen av enskilda program kontaktar man aktuell systemägare eller systemförvaltare. Vid problem med dator, nätverksåtkomst, programåtkomst eller telefoni kontaktas systemförvaltaren eller Kommunalförbundet ITSAMs servicedesk.

2. Åtkomst till information

2.1 Behörighet

Verksamhetens informationssystem är utrustade med behörighetskontrollsystem för att säkerställa att endast behöriga användare kommer åt rätt information. Vilka behörigheter man blir tilldelad avgörs av närmaste chef och beror på vilka arbetsuppgifter man är tilldelad.

2.2 Identifiering och autentisering

Varje användare som ska ha åtkomst till IT-resurser, interna datanät och Internet måste ansöka om användarID i form av användarnamn eller certifikat med tillhörande lösenord eller PIN-kod.

2.2.1 Datorinloggning

Innan man loggar in första gången erhålls ett lösenord av Kommunalförbundet ITSAM för åtkomst till tjänster och resurser. Lösenordet ska bytas till ett personligt lösenord efter första inloggningen.

2.2.2 Inloggning förvaltningsspecifika system

Lösenord för åtkomst enskilda informationssystem erhålls av i första hand systemförvaltaren till det specifika systemet och i andra hand av Kommunalförbundet ITSAMs servicedesk.

2.2.3 Distansarbete

Med distansarbete menas att verksamhetssystem görs tillgängliga även utanför ordinarie arbetsplats. Användare som arbetar på distans identifierar sig med dels med användarnamn och tillhörande lösenord och dels, i de fall det krävs, också med att man erhåller en verifieringskod till egen, personlig enhet (2-faktors autentisering) såsom exempelvis mobiltelefon, alternativt med hjälp av eID eller liknande. Åtkomst till interna system på distans görs via angiven av Kommunalförbundet ITSAM administrerad portal.
Kravnivåer på identifiering och autentisering för distansarbete regleras av Kommunalförbundet ITSAMs policy för åtkomstkontroll.

2.2.4 Inloggning med hjälp av kort

Vid de arbetsplatser där smarta kort används, identifierar och autentiserar man sig via ett smartkort istället för användarnamn och lösenord. Användare som använder smarta kort sätter in dessa i datorns kortläsare samt matar in den tilldelade personliga PIN-kod erhållits tillsammans med smartkortet. När kortet dras ut ska datorn låsas automatiskt.
Förlust av smartkort ska omedelbart anmälas till Kommunalförbundet ITSAMs servicedesk för spärr och återkallande av tillhörande certifikat. Begäran om nytt kort görs via närmaste chef.

2.2.5 Spårbarhet

Som användare lämnar man spår efter sig när man är inloggad och arbetar i systemen. De loggningsfunktioner som finns i systemen används för spåra obehörig åtkomst. Detta för att skydda informat-

ionen och för att undvika att man som användare blir oskyldigt misstänkt om oegentligheter skulle inträffa. Efter tre misslyckade försök att logga in spärras kontot. Om det händer måste kontakt tas med Kommunalförbundet ITSAMs servicedesk för att få ett nytt engångslösenord. Har man glömt sitt lösenord får man även där ett nytt engångslösenord via Kommunalförbundet ITSAMs servicedesk.

2.3 Val av lösenord och PIN-koder

För lösenord gäller att de:

- ska vara minst åtta tecken långa
- ska bestå av en blandning av versaler, gemener och andra tecken
- inte kan och ska återanvändas

Beroende på typ av smart kort är längden på PIN-koden 4 tecken eller fler.

- Observera att PIN-koden endast består av siffror

2.4 Byte av lösenord och PIN-kod

Byte av lösenord och PIN-kod ska:

- ske var 90:e dag för det interna nätverket
- för enskilda system ske efter ett visst tidsintervall som bestäms av respektive systemägare
- ske omedelbart om man misstänker att lösenordet eller PIN-koden blivit röjt

3. Arbetsplatsen

3.1 Utrustning

För den utrustning man förfogar över, ex. stationär eller bärbar PC med tillhörande utrustning, smart telefon, surfplatta och liknande gäller att:

- fysiska ingrepp endast får göras av Kommunalförbundet ITSAMS serviceavdelning eller av leverantörens utsända servicetekniker.
- fel på utrustningen omgående ska anmälas till Kommunalförbundet ITSAMs servicedesk.
- alla installationer och konfigurationer endast får utföras av Kommunalförbundet ITSAMs personal. Undantaget är vid godkänd delegation av installation.

3.2 Programvaror

- Programvaror ska godkännas och installeras av Kommunalförbundet ITSAMs utsedda tekniker eller av annan godkänd person med delegation.
- Egna program får inte installeras i utrustning där Kommunalförbundet ITSAM har ett driftansvar.
- Det är inte tillåtet att kopiera eller installera sin arbetsgivares programvara utanför den ordinarie verksamheten.
- Om behov finns av ytterligare program- eller hårdvara ska begäran om detta ske vi angivna kanaler.

3.3 Service på utrustning

Inför service på erhållen utrustning från arbetsgivaren vilket innebär bortlämnande av densamma till extern part ska känslig information avlägsnas om sådan finns.

3.4 Uttjänt utrustning

Kassering av utrustning görs av från Kommunalförbundet ITSAM utsedd personal eller extern part.

3.5 När man lämnar datorarbetsplatsen

Vid tillfällen då man inte har uppsikt över datorarbetsplatsen ska man alltid låsa arbetsstationen med CTRL+ALT+DEL och Enter alternativt logga ut ur systemet. I förekommande fall räcker det med att avlägsna smartkort ur kortläsaren för att uppnå samma resultat.

4. Klassning och hantering av information

4.1 Klassning av information

Informationssystem inom organisationerna klassas utifrån den information som hanteras i systemet. Klassning görs utifrån aspekterna

- **Sekretess**: Att informationen skyddas från obehörig insyn eller nyttjande
- **Riktighe**t: Att informationen inte ändras på obehörigt sätt
- **Tillgänglighet**: Att informationen finns tillgänglig för rätt person vid rätt tillfälle
- **Spårbarhet**: Att händelser går att härleda till användare och/eller system

Tas information ut ur systemet och lagras på andra media eller används i ett annat sammanhang måste den klassas där den används och hanteras därefter. Även information i arbetsmaterial ska klassas.
Allmänt gäller att verksamhetsrelaterad information samt tillgängliggjord information genom verksamhetssystem inte får föras vidare till tredje part efter uppdragsslut eller då anställning upphör eller användas utanför ramen för sina ordinarie arbetsuppgifter.

4.2 Lagring

Den information som lagras på anvisade utrymmen säkerhetskopieras dagligen. Man kan välja att lagra filer i egna-, organisations- eller andra gemensamma utrymmen/resurser.
Hemmakatalogen är en enhet som kan användas för lagring av personligt arbetsmaterial. I förekommande fall kan även andra enhetsbeteckningar finnas.
Organisationskataloger är enheter för lagring av information som berör personal inom den egna organisationen. Organisationskataloger delas av alla som har rättigheter till dessa.
Om man lagrar information på lokala enheter är man personligen ansvarig för säkerhetskopiering. Lagrar man information på lokala enheter riskerar man att förlora information som inte kan återskapas till rimliga kostnader vid t ex en diskkrasch eller om datorn har skickats tillbaka till tillverkaren efter leasingperiods utgång eller vid service. Kommunalförbundet ITSAM tar inget ansvar för information som lagras på arbetsdator såsom stationär dator, bärbar dator, telefon eller platta mm.

5. Internet

Använder man Internet kan säkerheten i organisationens system och datanät äventyras beroende på beteende.
Det är inte tillåtet att via Internet titta eller lyssna på material av pornografisk eller rasistisk karaktär. Förbudet gäller även material som är diskriminerande (religion, kön, sexuell läggning mm) eller som har anknytning till olaglig/kriminell verksamhet.
Undantag från detta kan beviljas av chef om informationen på sådana sidor kan ha relevans för arbetsuppgifterna.
Tänk på att när man surfar på Internet, deltar i diskussioner eller gör inlägg via digitala sociala nätverk fortfarande representerar sin arbetsgivare och dennes värderingar. Detta gäller även utanför arbetstid där man bör klargöra att man uttalar sig som privatperson vid inlägg i kontroversiella ämnen även om de saknar anknytning till sin yrkesroll.
Vid användning av Internet på sin arbetsplats eller inom andra lokaler hos sin arbetsgivare lämnar man alltid spår efter sig i form av IP-adresser mm.

6. Epost

E-post är ett rationellt hjälpmedel i arbetet men lagringskapaciteten för det är begränsad. Tänk därför på att regelbundet radera i mapparna ”Inkorgen”, ”Skickat”, och ”Borttaget” för att frigöra utrymme så att inte epost-kontot spärras. Epostsystemet ska inte användas som ett arkivsystem. Meddelanden, bifogade filer mm som ska sparas, sparas på samma sätt som annan information. Man får inte radera epostmeddelanden som ska klassificeras som tjänstpost. Organisationerna lyder under offentlighetslagen och all epost anses vara allmän handling om den saknar sekretessmarkering. Ovidkommande e-post som saknar koppling till ärenden eller offentlig förvaltning kan gallras.

- Var selektiv med att skicka eller vidarebefordra meddelanden som innehåller stora filer för att undvika onödig belastning av systemresurser.
- Om man under en längre period inte har möjlighet att kontrollera sin e-post bör man sätta frånvarobesked med eventuell uppgift om vem som ska hantera sina inkommande ärenden. Man kan också delegera hanteringen av sin epost till kollega.
- E-postsystemet är ett arbetsverktyg och bör inte användas för privat bruk.
- Samma regler gäller för diarieföring av e-post som för vanliga brev.
- E-post med bilagor utgör ett stort hot när det gäller spridning av virus, trojaner och andra typer av skadlig kod. Klicka inte på länkar i meddelanden utan att först ha kontrollerat med avsändaren att den verkligen skickat en länk till något som inte är en virusrisk.
- Om man misstänker att virus kommit in via e-postsystemet ska man agera i enlighet med vad som beskrivs i avsnittet Incidenter.
- Det är generellt inte tillåtet med automatisk vidarebefordran till annan e-postadress.
- Ange alltid ämne i ämnesraden för meddelandet för att klargöra för vad mottagaren vad för innehåll som kan förväntas.
- Skriv aldrig känslig information i ämnesraden.
- Kontrollera vilka som är medlemmar på sändlistor innan dessa används, risk finns att känslig information når fel mottagare. Kan man inte kontrollera vilka som finns på sändlistan ska man inte skicka känslig information inte skickas till sådan.
- Använd ”läskvittens” för interna meddelanden endast då behov för detta föreligger.
- Skicka inte eller vidarebefordra kedjebrev.
- Tänk på hur epostadress exponeras.
- Om man får hotbrev eller brev innehållande stötande eller kränkande material ska dessa sparas och kontakt ska tas med sin närmaste chef.
- Sekretessbelagd information får inte distribueras via e-post

7. Incidenter, virus mm

7.1 Allmänt

Om misstanke finns att någon använt ens användaridentitet eller att man varit utsatt för annan liknande incident ska man

- notera när man senast var inloggad (datum och tidpunkt).
- notera när incidenten upptäcktes (datum och tidpunkt).
- omedelbart anmäla förhållandet till Kommunalförbundet ITSAMs servicedesk eller till närmaste chef.
- dokumentera alla iakttagelser i samband med upptäckten och försöka fastställa om kvaliteten på information påverkats.

Om man upptäcker fel och brister i de system som används ska detta rapporteras till Kommunalförbundet ITSAMs servicedesk eller till närmaste chef.

7.2 Virus

Inom organisationen ska samtliga uppkopplade enheter ha programvaror för viruskontroll både i klienterna och i nätverket men man kan ändå drabbas av effekter av det som kallas för skadlig kod. Om misstanke finns att dator innehåller virus ska man:

- dra ur nätverkskabeln och/eller avaktivera det trådlösa nätverkskortet, men låta datorn vara igång.
- omedelbart anmäla förhållandet till endera Kommunalförbundet ITSAMs servicedesk eller närmaste chef. Observera: Anmälan ska göras per telefon eller besök, inte via epost.

Om man får e-post med virusvarning ska man enbart kontakta Kommunalförbundet ITSAMs servicedesk.
Läs-/surfplattor, smarta telefoner, digitalkameror, USB-minnen mm kan lätt bli virusbärare eftersom man där kan mellanlagra information mellan olika datorer. Var noga med att den dator man ansluter sådan kringutrustning till har ett uppdaterat virusskydd enligt gällande krav.

8. Avslutning av anställning

När man avslutar sin anställning ansvarar man för att:

- i samråd med närmaste chef rådgöra om vilket av sitt arbetsmaterial som ska sparas. Notera att allt arbetsmaterial som framställt anses vara arbetsgivarens egendom och får inte tas med utan chefs godkännande.
- material av privat natur tas bort.
- behörigheter man erhållit för åtkomst till informationssystem avbeställs av närmaste chef.

9. Gällande regler och föreskrifter

Informationssäkerhetsinstruktionen Användare A-P (användarpolicyn) med tillhörande kvittens ska skrivas under av personal. Underskriven kvittens ska lämnas till närmaste ansvarig chef. Personal ska vid underskrift ha tillgång till ett eget exemplar av denna informationssäkerhetsinstruktion. Observera att den kan komma att uppdateras och att det alltid är den senaste uppdaterade versionen som gäller.