Informationssäkerhetsinstruktion
Användare: Övriga
(3:0:2)

Kommunalförbundet ITSAM

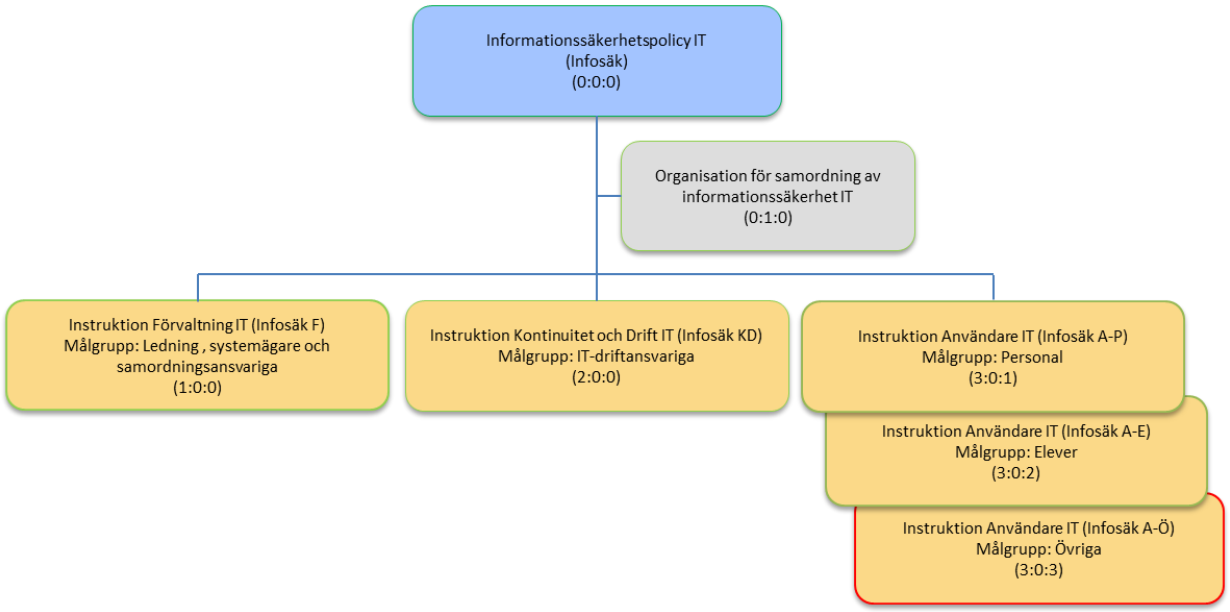
Revision: 20160516
Ersätter: 20130317
Dnr: 2016/00024

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

Innehåll

Instruktionens roll i informationssäkerhetsarbetet inom IT

Informationssäkerhetspolicyn och särskilda informationssäkerhetsinstruktioner med tillhörande dokument styr arbetet kring informationssäkerhet. Tillhörande dokument består av - Organisation för samordning av informationssäkerhet IT samt informationssäkerhetsinstruktionerna,Förvaltning IT (Infosäk F), Kontinuitet och Drift IT (Infosäk KD) och Användare IT (Infosäk A), fördelad på grupperna Personal, Elever och Övriga.



Informationssäkerhetspolicyn redovisar ledningens viljeinriktning och mål för informationssäkerhetsarbetet och syftar till att förtydliga:

- organisation och roller för informationssäkerhetsarbetet
- krav på riktlinjer för områden av särskild betydelse

Informationssäkerhetsinstruktion Förvaltning (Infosäk F) redovisar:

- det ansvar som ingår i de olika rollerna
- de riktlinjer som gäller för områden av särskild betydelse
- regler för systemutveckling, systemunderhåll, incidenthantering

Informationssäkerhetsinstruktion Kontinuitet och drift (Infosäk KD) redovisar:

- organisation och ansvar för drift av informationssystemen
- regler för säkerhetskopiering, lagring, driftadministration och kontinuitetsplanering

Informationssäkerhetsinstruktion Användare (Infosäk A-P, A-E, A-Ö) syftar till att klarlägga:

- hur personal, elever och övriga användare ska verka för att upprätthålla en god säkerhet

Som övriga användare räknas alla som utför uppdrag beställda och kontrollerade av systemförvaltare i samråd med Kommunalförbundet ITSAM.

1. Användarens ansvar

Information är en viktig tillgång för organisationen. För att skydda denna krävs ett säkerhetsmedvetande hos alla användare som delar på ansvaret för säkerheten i informationshanteringen.

För användningen av enskilda program och för att få stöd och hjälp kontaktar användaren ansvarig systemadministratör. Vid problem med dator, nätverksåtkomst, programåtkomst eller telefoni kontaktar användaren ansvarig systemadministratör 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 information. Vilka behörigheter man blir tilldelad avgörs av närmaste inom Kommunalförbundet ITSAM utsedd ansvarig systemadministratör och beror på vilka tjänster användaren ska utföra.

2.2 Identifiering och autentisering

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

2.2.1 Datorinloggning

För internt arbete gäller identifiering och autentisering med användarnamn och lösenord. Innan man loggar in första gången erhålls ett lösenord av Kommunalförbundet ITSAM utsedd ansvarig systemadministratör för åtkomst till tjänster och resurser.

2.2.2 Inloggning till förvaltningsspecifika system

Lösenord till specifika informationssystem erhålls av, Kommunalförbundet ITSAM utsedd, ansvarig systemadministratör.

2.2.3 Distansarbete

Användare som arbetar på distans identifierar sig med användarnamn samt autentiserar sig med lösenord och med erhållen kod till egen, personlig enhet (2-faktors autentisering) alternativt med hjälp av e-legitimation. Åtkomst till interna system på distans möjliggörs genom, av Kommunalförbundet ITSAM angiven och administrerad, portal.
Kravnivåer på identifiering och autentisering för distansarbete regleras av Kommunalförbundet ITSAMs policy för åtkomstkontroll.

2.2.4 Datorinloggning med hjälp av kort

Vid de arbetsplatser där smartkort används, identifierar och autentiserar sig användaren via ett smart kort istället för användarnamn och lösenord. I en del fall krävs det både tillfälligt utgivet smart kort tillsammans med övriga inloggningsuppgifter. Användare som då erhållit smart kort sätter in dessa i datorns kortläsare samt matar in den tilldelade personliga PIN-kod. När kortet dras ut ska datorn låsas automatiskt.
Förlust av smart kort ska omedelbart anmälas till servicedesk för spärr och återkallande av tillhörande certifikat. Begäran om nytt kort görs via av Kommunalförbundet ITSAM utsedd ansvarig systemadministratör.

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 informationen och för att undvika att man som användare blir oskyldigt misstänkt om oegentligheter skulle inträffa. Efter tre misslyckade försök att logga in spärras kontot vilket innebär kontakt med Kommunalförbundet ITSAMs servicedesk eller ansvarig systemadministratör för att få ett nytt lösenord. Har man glömt sitt lösenord eller förlorat möjligheten att få åtkomst till interna resurser via portal, ska ansvarig systemadministratör eller Kommunalförbundet ITSAMs servicedesk meddelas.

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:

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

3. Arbetsplatsen

3.1 Utrustning

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

- Fysiska ingrepp endast får göras av kommunalförbundet ITSAM eller av leverantörens utsända servicetekniker.
- Fel på utrustningen omgående ska anmälas till systemadministratör.
- Alla installationer och konfigurationer enbart får utföras enligt gällande serviceplan och i samråd med ansvarig systemadministratör.

3.2 Programvaror

- Programvaror får installeras i samråd med ansvarig systemadministratör eller av annan godkänd person med delegation.
- Egna program utanför ramen i uppdraget får inte installeras i verksamhetens utrustning.
- Det är inte tillåtet att kopiera eller installera organisationens programvara utanför den ordinarie verksamheten.
- Om behov finns av ytterligare program- eller hårdvara ska begäran om detta göras till ansvarig systemadministratör.

3.3 Service på utrustning

Inför service på erhållen utrustning som innebär att utrustningen lämnas till extern part ska eventuell känslig information tas bort..

3.4 Uttjänt utrustning
Kassering av utrustning görs av utsedd personal från ITSAM.

3.5 När man lämnar datorarbetsplatsen
Vid tillfällen då man inte har uppsikt över datorarbetsplatsen ska användaren alltid låsa arbetsstationen med CTRL+ALT+DEL och Enter. I förekommande fall räcker det med att avlägsna smartkort ur kortläsaren för att uppnå samma resultat.
När användaren arbetar på distans, ska förutom utloggning alternativt låsning av arbetsstation även vpn-förbindelsenavslutas.

4. Klassning och hantering av information

4.1 Klassning av information
Informationssystem inom organisationerna klassas utifrån den information som dessa system hanterar. Klassning görs utifrån aspekterna

- **Sekretess**: Att informationen skyddas från obehörig insyn eller nyttjande
- **Riktighet**: Att informationen inte ändras på obehörigt sätt
- **Tillgänglighe**t: 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.
Verksamhetsrelaterad information samt tillgängliggjord information genom verksamhetssystem får inte föras vidare till tredje part efter uppdragsslut eller då anställning upphör och inte heller användas utanför ramen för ordinarie arbetsuppgifter.

4.2 Lagring
Den information som lagras på anvisade utrymmen säkerhetskopieras dagligen. Man kan välja att lagra filer i egna-, organisationens- 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 såsom USB-minnen mm 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 leasingperiodens utgång eller vid service. ITSAM har inget ansvar för lokalt lagrad information.

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.
För att minska risken avseende identitetsstöld, röjning av lösenord eller PIN-koder eller att dator, surfplatta eller telefon smittas av skadlig kod bör man vara restriktiv och vaksam vid användning av för användaren okända tjänster på Internet.

6. E-post

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. E-postsystemet ska inte användas som ett arkivsystem. Meddelanden, bifogade filer mm som ska sparas, sparas på samma sätt som annan information. Organisationerna lyder under offentlighetslagen och all e-post 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.
- Systemet för E-post 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 skickade länken inte leder till något som är en virusrisk.
- Om man misstänker att virus kommit in via systemet för e-post 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 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 användaren inte skicka känslig information med hjälp av dessa sändlistor.
- Använd ”läskvittens” för interna meddelanden endast då behov för detta föreligger.
- Skicka inte eller vidarebefordra kedjebrev.
- Tänk på hur e-postadress exponeras.
- Om man får hotbrev eller brev innehållande stötande eller kränkande material ska dessa sparas och närmaste chef informeras.
- Sekretessbelagd information får inte distribueras via e-post utan rätt nivå av transportkryptering.

7. Incidenter, virus mm

7.1 Allmänt

Om misstanke finns att någon använt ens användaridentitet eller att man har 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 ansvarig systemadministratör.

- Dokumentera alla iakttagelser i samband med upptäckten och försöka fastställa om kvaliteten på information har påverkats.

Om användaren upptäcker fel och brister i de system som används ska detta rapporteras till ansvarig systemadministratör.

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:

- Om arbete sker internt dra ur nätverkskabeln och/eller avaktivera det trådlösa nätverkskortet, men låta datorn vara igång.
- Omedelbart anmäla förhållandet till ansvarig systemadministratör.
  Observera: Anmälan ska göras per telefon eller besök, inte via epost.

Läs-/surfplattor, smarta telefoner, digitalkameror, USB-minnen mm kan lätt bli virusbärare eftersom användaren där kan mellanlagra information mellan olika datorer. Det är viktigt att den dator användaren ansluter sådan kringutrustning till har ett uppdaterat virusskydd enligt gällande krav.

8. Avslutning av uppdrag

När man avslutar sitt uppdrag ansvarar man för att:

- I samråd med ansvarig systemadministratör rådgöra om vilket av sitt arbetsmaterial som är uppdragsrelaterat och som ska sparas.
- Material av privat natur tas bort.
- Behörigheter man erhållit för åtkomst till informationssystem avbeställs via ansvarig systemadministratör.

9. Gällande regler och föreskrifter

Informationssäkerhetsinstruktionen Användare A-Ö (användarpolicyn) med tillhörande kvittens ska skrivas under av uppdragshållare. Underskriven kvittens ska lämnas till närmaste ansvarig systemadministratör. Uppdragshållare 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.