

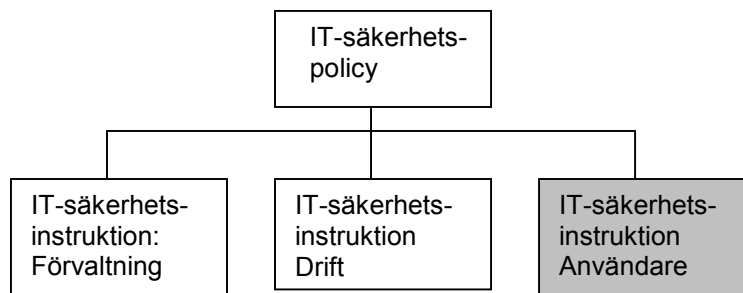
## IT- säkerhetsintstruktion för användare

Innehåll: .....	2
<b>1. INLEDNING</b>	
Mål.....	3
Systeminstruktur och rollfördelning .....	3
<b>2. INFORMATION OCH LAGRING</b>	
<b>4</b>	
Handling som är hemlig .....	5
Lagring av information .....	5
Behörighet.....	7
Lösenord .....	7
<b>3. IT-SÄKERHET OCH KRINGUTRUSTNING</b>	<b>7</b>
Bärbara- och hemdatorer.....	8
Kringutrustning med mellanlagringsmöjligheter .....	8
Vårt lokala nätverk (LAN) .....	8
<b>4. INTERNET OCH E-POST</b>	
<b>9</b>	
E-post .....	9
<b>5. INCIDENTER, VIRUS, STÖLD M M</b>	
<b>10</b>	
Obehörigt intrång .....	10
Virus mm.....	10
<b>6. ÖVRIGT</b>	
<b>11</b>	
Stöd och hjälp .....	11
När du slutar din anställning .....	11

## 1. Inledning

IT-säkerhet är en del i organisationens lednings- och kvalitetsprocess som ska bidra till att ett IT-system kan användas på avsett sätt och med avsedd funktionalitet. KBM:s rekommendationer\*) om basnivå för IT-säkerhet (BITS) ska gälla som ramverk för IT-säkerhetsarbetet

Styrande dokument för IT-säkerhetsarbetet är:



Användningen av IT-stöd i vårt dagliga arbete ökar och införandet av fler strategiska IT-tillämpningar sker kontinuerligt. För att alla dessa system ska vara säkra, tillgängliga och fungera som det effektiva verktyg vi önskar, är det viktigt att användningen sker på ett kontrollerat sätt. En förutsättning för detta är att känna till de krav som ställs på dig som IT-användare inom kommunen.

Du måste veta:

- vilket ansvar du har
- vad du kan göra vid olika incidenter
- var du kan få stöd och hjälp
- de allmänna säkerhetsbestämmelserna
- hur du får nyttja e-post och Internet

Denna instruktion syftar till att ge dig kunskaper och riktlinjer om hur du på ett säkert sätt använder IT-stöden inom kommunen. Se gärna dokumentet som ett uppslagsverk och viktig källa för kunskap om hur IT-systemen och informationen får användas. Saknar du någon information eller vill du veta mera så tvekan inte att kontakta Dataenheten.

### Mål

Målet är att alla användare skall:

- ansvara för informationens riktighet och att den skyddas mot behörig insyn
- vid såväl inmatning, uttag och bearbetning av information.
- rapportera fel och brister
- framföra vid behov av information och utbildning till systemägare
- föreslå utvecklande förändringar av IT-systemen
- meddela systemadministratör behöver av skydd för känslig information
- förstå IT-systemet struktur och rollfördelning inom kommunen
- förstå begränsningar och risker i användandet av e-post och Internet.

\*) KBM; Krisberedskapsmyndigheten

### **Systemstruktur och rollfördelning**

Det övergripande ansvaret för kommunens IT-system vilar på kommunchefen som också utser systemägare för kommunens gemensamma IT-system.

Kommunen eftersträvar att systemägaransvaret för IT-systemen skall följa linjeorganisationen för varje enskild IT-system.

**Systemägaren** (i regel förvaltningschef) initierar den egna verksamhetens behov av IT-stöd. Systemägaren har det övergripande ansvaret inför ledningen att ett IT-system förvaltas på för verksamhetens bästa sätt. Systemägaren beslutar om nyanskaffning, vidareutveckling eller avveckling av IT-system inom ramen för resurstilldelningen för sin verksamhet.

**Systemförvaltare** – ansvarar för förvaltningen av ett IT-system, utarbetar regler för behörighet till systemet, utarbetar kompetenskrav för systemets användare samt ansvarar för utbildningsplanering i samråd med systemägaren.

**Datachef** är systemägare inom området teknisk infrastruktur och har det övergripande ansvaret för att ett systems tekniska delar fungerar. Datachef samverkar med resp. systemägare avseende drift och resurstilldelning för ett IT-system.

**Systemadministratören** tillhör Dataenheten. Systemadministratören ansvarar tillsammans med systemägare och systemförvaltare för att den dagliga driften upprätthålls enligt överenskommelse mellan systemägare och Datachef.

**Användaren** skall följa gällande regler och riktlinjer för IT-säkerhet. I detta ingår att noga ta del av och följa säkerhetsregler som finns för de IT-system som den enskilda använder.

**IT-säkerhetsledning** – Vid större oplanerade IT-relaterade händelser tillämpas kommunens beredskapsplan.

**Referensgrupper** – Systemägaren utser vid behov en referensgrupp för sitt IT-system. Referensgruppen fungerar som en rådgivande och stödjande funktion till systemägaren i diverse frågor som rör systemförvaltningen.

## **2. Information och lagring**

I ditt dagliga arbete kommer du i kontakt med information som kommer levererad till dig många olika former. Det kan vara muntligt, på papper, lagrad i dator via e-post m m. För att du ska få den information som du behöver, vid rätt tidpunkt och med korrekt innehåll har kommunen satt upp som övergripande mål för informationssäkerhetsarbetet att vi skall:

- behandla information på ett tydligt, korrekt, säkert och relevant sätt
- kunna leverera och hämta information vid rätt tidpunkt
- uppnå och upprätthålla en god informationssäkerhet.

Med dessa mål som bakgrund utgår kommunen från synsättet att våra medarbetare ska ha tillgång endast till den information och de system de behöver för sitt arbete.

En stor mängd handlingar (uppgifter) kan vara sekretesskyddade. Det är viktigt att du är förtrogen med karaktären på de handlingar/uppgifter som du hanterar. Följande riktlinjer för klassning av information gäller:

<b>Säkerhetsaspekt</b>	<b>Sekretess</b>	<b>Riktighet</b>	<b>Tillgänglighet</b>
<b>Mycket hög</b>	Data som inte får röjas	Data som: -enligt lagkrav ska säkras mot förändring eller förstöring -av andra skäl än lagkrav få inte vara felaktiga	Data som kan var åtkomlig inom högst en dag
<b>Hög</b>	Data som kan ge väsentliga negativa konsekvenser om de röjs	Data som kan ge väsentliga negativa konsekvenser om de är felaktiga	Data som inte behöver vara åtkomlig inom en dag vecka men inom en vecka
<b>Normal</b>	Data som kan ge negativa konsekvenser om de röjs	Data som kan ge negativa konsekvenser om de är felaktiga	Data om inte behöver vara åtkomlig förrän efter en vecka eller längre

### **Handling som är hemlig**

Handlingar kan vara allmänna eller icke allmänna handlingar. Allmänna handlingar kan sedan vara offentliga eller hemliga. Alla allmänna handlingar måste registreras, arkiveras och diareiföras. Det gäller även handlingar som inkommer via telefax eller e-post m m. En myndighet som vägrar lämna ut en allmän handling kan endast göra så med stöd av lagrum i sekretesslagen. Om du ärtveksam skall du kontakta din chef.

I personuppgiftslagen regleras rätten att behandla personuppgifter. Syftet med personuppgiftslagen är att skydda människor mot att deras personliga integritet kränks genom behandling av personuppgifter.

Om du som medarbetare behöver upprätta särskilda register för uppföljning, kvalitetskontroll och forskning bör du samråda med förvaltningens personuppgiftsombud på ett tidigt stadium i planering av registret

### **Lagring av information**

Allt arbetsmaterial skall lagras. För IT-stödet kan vi övergripande se det som två olika typer av lagringsmöjligheter.

- Information i våra stödsystem

som stöd i det dagliga arbetet har kommunen och dess verksamhet olika IT-baserade stödsystem bl. a. ekonomi och personalsystem. I dessa system är informationen ofta redan "klassad" och inbyggda regelverk ger rättigheter eller sätter begränsningar för dig att hantera informationen.

För vart och ett av stödsystemen skall det finnas en handbok eller en användarinstruktion, som beskriver vilken information systemet innehåller, vad du skall och får tillföra, ändra och eventuellt ta bort. Om reglerna följs har vid goda möjligheter att klara kraven på en god informationssäkerhet i systemen.

- Egna register/dokument

Utöver att arbeta i våra stödsystem kan du komma att upprätta egna register, handlingar och dokument, exempelvis med Word eller Exel. Stödsystemens "inbyggda skydd" användas inte då. Detta kräver särskild uppmärksamhet. Det är viktigt att du tänker över säkerheten och hur du klassar, hanterar och lagrar informationen.

Oavsett om du använder stödsystemet eller har skapat egna dokument så har du ett personligt ansvar för säkerheten i din hantering av information i alla dess former. I detta ansvar ingår bl.a att du själv måste känna till de regler som gäller när du hanterar information. När du hanterar information är du ansvarigt för informationens riktighet och att informationen skyddas mot obehörig insyn. Tveka inte att samråda med din närmaste chef om du känner dig osäker i dessa sammanhang.

När du skapar information är det viktigt att veta var den bör lagras. Den information du lagrar på våra gemensamma utrymmen, som kan nås via det lokala nätverket, säkerhetskopieras automatiskt. Du kan välja att lagra på de enheter du tilldelats beroende av dina arbetsuppgifter.

Alla användare har tillgång till en:

- (Personlig hemkatalog) en enhet där du lagrar personligt arbetsmateriel och som endast du har tillgång till.

Eventuellt har du beroende av arbetsuppgift tillgång till:

- (Gruppenhet) som är en enhet för lagring av information som du och medarbetarna på din enhet har tillgång till.
- (Funktionsenhet) som är en enhet för lagring av information som du och dina medarbetare på din funktion har tillgång till.

Om du lagrar på din lokala hårddisk (C:) är du personligen ansvarig för att säkerhetskopiering sker, t ex på diskett. När du lagrar information på din lokala hårddisk (C:) riskerar du att förlora information som inte kan återskapas till rimliga kostnader, vid t ex en diskrasch, undvik därför lagring på C:.

## **Behörighet**

Våra IT-system är utrustade med behörighetskontrollsystem för att säkerställa att endast behöriga användare kommer åt information. De behörigheter du blir tilldelad beror på dina arbetsuppgifter och avgörs av din chef.

## **Lösenord**

Första gången du loggar in i nätverket får du ett initialt lösenord av Dataenheten. Detta lösenord kan du bara använda en gång för att komma in i nätverket. När du har loggats in, uppmanas du att byta det initiala lösenordet till ett personligt lösenord. Även för övriga system som du fått behörighet till, måste du byta det initiala lösenordet mot ett eget. Lösenordet är strängt personligt och skall hanteras därefter. Tänk på att du själv kan bli misstänkt om någon använder ditt lösenord för olämpliga ändamål. Du skall därför:

- inte avslöja ditt lösenord för andra eller låna ut din behörighet
- skydda lösenordet väl
- omedelbart byta lösenord om du misstänker att någon känner till det
- byta lösenordet med de intervaller som gäller för resp. system. Du får en uppmaning av systemet när det är dags att byta.

Lösenordet ska bestå av de minst det antal tecken, som varje systemägare kräver, och skall konstrueras så att det inte lätt kan kopplas till dig som person. Enkla repetitiva mönster såsom t ex AAAA1111 får inte användas, inte heller andra lättforcerade lösenord, såsom eget eller familjemedlems namn eller enkla tangentkombinationer av typen QWERTY. För att väsentligt försvåra lösenordsknäckning bör bokstäver, siffror och specialtecken blandas i lösenordet.

Om du glömmer ditt lösenord och försöker logga in tillsystemet med ett felaktigt sådant, kommer systemet att låsas efter tre felaktiga försök. Om detta inträffar vänder du dig till din systemadministratör. Du kommer då att få ett nytt initialt lösenord.

## **3. IT-säkerhet och kringutrustning**

För att uppnå nödvändig IT-säkerhet finns regler och rekommendationer för användning av IT-systemen inom kommunen:

- Mjukvara (program) som inte godkänts av Dataenheten får ej installeras eller användas på arbetsstationer eller nätverk som administreras av kommunen. Det är inte heller tillåtet att kopiera eller använda kommunens program utanför kommunens verksamhet. Om du är i behov av ytterliga programvaror eller hårdvara t ex handdator, digitala kameror m m ska du anmäla det till din chef.
- All installation och konfiguration av hårdvara och arbetsstationer ska ske av Dataenheten så att kommunens standard följs.
- Vid tillfällen när du inte har uppsikt över arbetsstationen skall du tillfälligt låsa arbetsstationen. Vid längre frånvaro skall arbetsstationen loggas ur.
- Vid fel på arbetsstationen med tillhörande hårdvara skall du omgående anmäla detta till Dataenheten.

- Din arbetsstation med tillhörande hårdvara är kommunens egendom och får ej bytas, förändras eller medtagas utan Dataenhetens medgivande.
- Inför service på din utrustning som innebär att din persondator lämnas bort eller kasseras måste all information på din hårddisk tas bort. Rådgör då med Dataenheten.

### **Bärbara- och hemdatorer**

Av kommunens IT-säkerhetspolicy framgår att arbete utanför kommunens lokaler som kräver uppkoppling mot det interna nätverket kräver medgivande av systemägaren som samråder med Dataenheten. Om du har en egen bärbar- eller hemdator som du använder för hemarbete bör du tänka på att dessa kan utgöra en säkerhetsrisk. Tänk på att:

- inte kopiera känslig information till diskett som du sedan tar med hem. Risk finns att obehöriga kan ta del av den
- att du inte får lagra sekretessbelagd eller för verksamheten känslig information på den egna datorn
- lagringsmedia som du använder/skapar i hemdatormiljö på disketter, brända skivor, zip-disk m m få inte användas i kommunens nätverk förrän viruskontroll av lagringsmediet har skett. Kontrollen sker mot ett uppdaterat program i av Dataenheten anvisad utrustning.

### **Kringutrustning med mellanlagringsmöjlighet**

Handdatorer, digitala kameror, mobiltelefoner m.m kan lätt bli virusbärare då du kan mellanlagra information mellan olika datorer i dessa. Därför skall du inte ansluta denna typ av kringutrustning mot en dator som du inte med säkerhet vet har ett uppdaterat virusprogram. All kringutrustning skall vara godkänd och installerad av Dataenheten.

### **Vårt lokala nätverk (LAN)**

Nätverket är en mycket viktig gemensam resurs som ger oss alla möjligheter att lagra information, dela på skrivare och program, upprätta kommunikation m m. Följande regler gäller för nätverket:

- Utskrifter av dokument på gemensam skrivare skall snarast hämtas.
- Inloggning i kommunens nätverk skall ske med ditt personliga lösenord.
- All inloggning eller försök till inloggning under annan, eller med annans identitet är absolut förbjuden.
- När du arbetar i kommunens nätverk loggas och registreras i allmänhet dina aktiviteter. Loggningsfunktionerna används för att spåra obehörig verksamhet och intrång. Detta görs för att skydda informationen samt för att undvika att oskyldiga misstänkts om oegentligheter inträffar.
- Information som ska sparas på gemensamma utrymmen i det lokala nätverket, skall lagras på anvisad plats (se kap 2).
- Det är absolut förbjudet att ansluta sig externt via egen icke godkänd uppkoppling t ex modem.
- Det är förbjudet att skaffa sig systemrättigheter än det som tilldelats.

Om vi alla följer dessa regler så kan obehöriga inte komma åt informationen. Kom ihåg att du ansvarar för allt som registreras med din användaridentitet.

#### **4. Internet och e-post**

När du använder Internet kan säkerheten i kommunens lokala nätverk påverkas i mycket hög grad beroende på ditt beteende.

Kommunen förutsätter att den som laddar ner filer från Internet har gott omdöme och endast hämtar in sådant som är relevant för arbetet och kommer från välrenommerade webbplatser.

Ingen programvara får laddas ner. Utöver säkerhetsrisken kan en felaktig hantering innebära skadeståndskrav vid t ex brott mot upphovsrätten.

Det är inte tillåtet att via Internet titta eller lyssna på material av pornografisk eller rasistisk karaktär. Förbudet gäller också material som är diskriminerande (religion, kön, sexuell läggning, etc.) eller har anknytning till kriminell verksamhet. I specifika fall kan det dock vara motiverat för arbetet t ex vid utredningar, omvärldsanalyser m m, att besöka sidor som normalt är förbjudna. På begäran av huvudman för verksamhet kan systemägaren för infrastruktur besluta att stänga av åtkomst till webbplatser som inte bedöms vara nödvändiga för tjänsteutövning eller lärande.

När du använder Internet i tjänsten representerar du kommunen. Gör det med ett gott omdöme så att ditt eget agerande på nätet i skadar oss. Agera i enlighet med våra värderingar så att det du förmedlar på nätet inte skadar oss. Du bör tänka på att du lämnar spår i en fil som loggar Internettrafiken på kommunen. Denna loggfil är offentlig handling och visar vilka webbplatser du har besökt.

#### **E-post**

E-post är ett rationellt hjälpmedel i arbetet, men minneskapaciteten för det är begränsad. Tänk därför på att regelbundet radera i mapparna "Inkorgen", "Skickat" och "Borttaget" för att frigöra utrymme så att inte din e-post spärras. E-postsystemet skall inte användas som ett arkivsystem, meddelanden, bifogade filer m m som du vill spara, sparar du på samma sätt som du lagrar annan information.

Om du under en längre period inte har möjlighet att kontrollera din e-post skall du sätta frånvarobesked med uppgift om vem som hanterar "dina ärenden". Var extra uppmärksam då du använder e-post. E-post med bilagor utgör ett stort hot när det gäller spridning av virus.

#### **Allmänt**

- e-postsystemet är ett arbetsverktyg och bör inte användas för privat bruk
- det är samma regler för diarieföring av e-post som för vanliga brev
- om du misstänker att det kommit in virus via e-postsystemet ska du agera som beskrivits i avsnittet om Incidenter.

#### **Utformning**

- det är inte tillåtet med automatisk vidarekoppling till annan e-postadress.

- ange alltid för meddelandet för att klargöra för mottagaren vad denne kan förvänta sig för innehåll i e-brevet.
- skriv inte någon känslig information i ämnesraden
- skriv korta brev. Tänk på att mottagaren kanske får stora volymer e-post
- använd läskvittens endast för interna meddelanden när du har behov av detta
- du bör vara selektiv med att använda stora gruppadresser (massutskick) och med att skicka eller vidarebefordra meddelanden som innehåller stora filer
- skicka inte vidarebefordra kedjebrev av någon sort
- sprid inte din e-postadress till mindre seriösa ställen
- stryk dig från e-postlistor om du inte vill få fler brev via dem eller är frånvarande en längre tid
- använd inte heller din vanliga användaridentitet och ditt lösenord när du registrerar dig i konferenser eller publika e-postservrar
- om du får hotelsebrev eller liknande, kontakta din chef. Ta inte bort brevet.

#### Bilagor

Som mottagare av en bilaga har du ett ansvar att signalera om det är något problem. Det finns begränsningar vad avser bilagestorlekar och filtyper.

Se vidare i kommunens "Policy/ritlinjer elektronisk post" (e-post) beslutat av kommunstyrelsen den 20 november 2000, § 227.

### **5. Incidenter, virus, stöld m m**

#### **Obehörigt intrång**

Om du misstänker att någon obehörig använt din användaridentitet och varit inne i IT-systemet skall du:

- notera när du senast var inne i IT-systemet
- notera när du upptäckte intrånget
- omedelbart anmäla till Dataenheten alternativt till systemansvarig, eller din chef
- dokumentera alla iakttagelser i samband med upptäckten och försöka att fastställa om kvaliteten på din information har påverkats.

#### **Virus m m**

Virus m m är ofta ytterst smittsamma och "smittkällan" kan vara svår att identifiera. Gratisprogram, spelprogram och de filer som laddas ner från Internet eller medföljande filer till e-post är de vanligaste smittbärarna. Kommunen har bra programvaror för viruskontroll och det görs kontinuerlig kontroll i nätverket. Även disketter och filer som du hämtar från Internet kontrolleras av virusprogram i nätverket. Men eftersom det hela tiden tillverkas nya datavirus så gäller följande:

Tecken på datavirus i systemet kan vara att:

- datorn utför operationer/arbete utan att du själv initierar det, t ex förändringar sker på skärmen (tecken flyttas, försvinner etc.).
- pip eller hälsningar på skärmen
- datorn uppträder på ett onormalt sätt, t ex arbetar mycket långsamt

Om du misstänker att systemet innehåller virus eller liknande ska du:

- INTE stänga din dator genom att slå av strömmen utan istället dra ut nätverkskabeln
- omedelbart anmäla förhållandet till Dataenheten eller till närmaste chef. OBS! Anmälan ska ske per telefon eller besök, EJ per e-post.

Om du får brev med virusvarning där man talar om att ett virus är på gång skall du inte skicka meddelande om detta till alla på kommunen, ta i stället kontakt med Dataenheten som kan avgöra om det är en seriös varning eller kanske bara ett skämt. Skicka inte heller någon varning externt. Dataenheten har informationsansvar vid ev. incidenter.

## **6. Övrigt**

Om du misstänker stöld, brand, sabotage och dylikt, kontakta din närmaste chef eller Dataenheten.

Om du upptäcker eller misstänker att någon bryter mot regler gällande Internet- och eller e-postanvändning skall närmaste chef och Dataenheten kontaktas.

Om du upptäcker fel och brister i de system du använder skall du rapportera dessa till systemägaren.

Kommunen bidrar till att öka IT-säkerheten i landet genom att löpande rapportera alla typer av IT-incidenter till PTS (Sitic). Genom att rapportera händelser hjälper du till att förebygga.

## **Stöd och hjälp**

För att få kunskap om vilka enheter vi använder, hur man lägger in skärmläckare med lösenord etc, kan du få stöd och hjälp av Dataenheten som hjälper dig med nätverks- och inloggningsproblem.

## **När du slutar din anställning**

Ansvarar du för att:

- rådgöra med din chef om vilket av ditt arbetsmaterial som skall sparas. Notera att allt arbetsmaterial du framställt anses vara kommunen egendom och får inte tas med utan chefs godkännande.
- privat material rensas och tas bort.

De behörigheter du fått i våra IT-system avbeställs genom din chefs försorg.