FALKENBERG

Kommunledningskontoret
Patrik Annervi
0346-88 60 14
patrik.annervi@falkenberg.se

Datum
2012-07-05

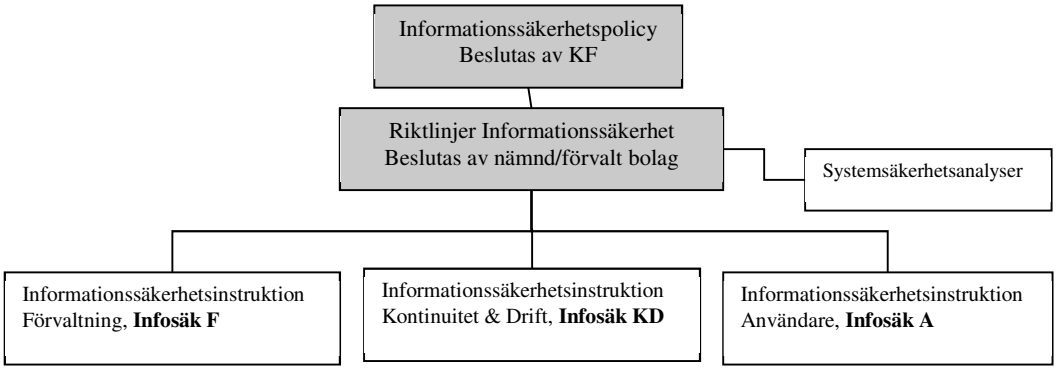
Informationssäkerhetsinstruktion Användare (Infosäk A)

Innehållsförteckning

Chefen ansvarar för

1. Instruktionens roll i informationssäkerhetsarbetet

Informationssäkerhetspolicy, riktlinjer för informationssäkerhet, informationssäkerhetsinstruktioner samt systemsäkerhetsanalyser styr kommunens informationssäkerhetsarbete.



Informationssäkerhetsinstruktion Användare (**Infosäk A**) redovisar hur en användare ska verka för att upprätthålla en god säkerhet.

Informationssäkerhetspolicyn med tillhörande riktlinjer redovisar ledningens viljeinriktning och mål för informationssäkerhetsarbetet och syftar till att klarlägga:

- 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

2. Användarens ansvar

Information är en viktig tillgång för Falkenbergs kommun. För att skydda denna krävs ett säkerhetsmedvetande hos alla medarbetare. Du som användare får tillgång till systemet för att underlätta ditt arbete och måste då ta en del i ansvaret för säkerheten i informationshanteringen.

Det är alla användares skyldighet att använda IT-miljön på ett ansvarsfullt sätt. Samhällets lagar gäller som norm. Detta innebär att alla ska respektera alla människors lika värde, använda ett vårdat språk samt värna om såväl sin egen som andras integritet.

Datorerna är öppna för egna programinstallationer. Det är dock inte tillåtet att installera något annat operativsystem än det som tillhandahålls av kommunen.

För att kunna leva upp till de säkerhetskrav som ställs på dig måste du känna till:

- Vilket ansvar du har för ditt arbete och dina lösenord
- Vad du skall göra vid olika incidenter
- Var du kan få stöd och hjälp

För stöd och hjälp när det gäller användningen av enskilda program kontaktar du aktuell systemförvaltare eller systemansvarig.

Har du problem med din dator ska du kontakta kommunens IT-service.

3. Åtkomst till information

3.1 Behörighet

Falkenbergs kommuns informationssystem är utrustade med behörighetskontrollsystem för att säkerställa att det endast är behöriga användare som kommer åt informationen.

De behörigheter du blir tilldelad beror på dina arbetsuppgifter och avgörs av din chef. Sedan **ansvarar du** för att följa de regler och riktlinjer som kopplas till behörigheten.

3.2 Inloggning

Innan du loggar in, i kommunens nätverk, första gången får du ett lösenord av IT-service för åtkomst till vårt interna IT-nätverk. Lösenordet ska du byta till ett personligt lösenord efter första inloggningen. Samma förfarande gäller för enskilda informationssystem som kräver lösenord för åtkomst.

Lösenord är strängt personliga och ska hanteras därefter. 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.
- Lösenordet ska bytas minst var 90:e dag om inget annat anges. I vissa system får du en automatisk påminnelse om detta.

Ditt konto är personligt och får endast användas av dig. Det innebär att du inte får lämna (låna) ut det till någon annan. Du får inte heller utnyttja någon annans konto.

Du är ansvarig för den trafik som härrör kontot och skall alltså bevara lösenordet för dig själv (jfr PIN kod till bankkort etc.).

Du lämnar spår efter dig när du 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 oskyldiga misstänks om oegentligheter inträffar.

Om ditt lösenord kommer på avvägar skall du utan dröjsmål anmäla detta till IT-service eller till behörighetshandläggaren på din förvaltning/bolag, så att lösenordet kan ändras.

Efter tre misslyckade försök att logga in, i kommunens nätverk, spärras ditt konto. Ta då kontakt med IT-service för att få ett nytt engångslösenord.

Har du glömt ditt lösenord får du ett nytt engångslösenord av IT-service

3.3 Val av lösenord

Lösenord måste vara uppbyggda så att de inte går att gissa sig till. Samtidigt får inte lösenordet vara så komplicerat och svårt att komma ihåg att det måste skrivas upp på en lapp, som obehöriga kan komma över.
Lösenordet ska konstrueras så att det inte lätt går att koppla till dig som person och minst innehålla 8 tecken. Enkla repetitiva mönster t.ex. ”ABCD1234” eller ”AAAAA222” skall undvikas, liksom alla andra lättforcerade lösenord, såsom eget eller familjemedlems namn eller lösenord av typen ”QWERTYUI”, dvs. enkla tangentbordskombinationer. De flesta system tillåter inte denna typ av lösenord utan kräver komplexa lösenord. I nätverket krävs att 3 av 4 olika typer av tecken används, versaler, gemener, specialtecken och siffror.

För att skapa ett bra lösenord kan du:

- Välj en uttalbar, men meningslös sekvens, till exempel ”BAMROKAD”, kombinera gärna med siffror eller tecken till exempel ”bam3rokad”
- ovanstående exempel kan också konstrueras genom att blanda små och stora bokstäver, till exempel ”hHsfOmGt” eller ”liT#oTesJh”.

Tidigare använda lösenord
Du kan inte återanvända tidigare använda lösenord. När du byter lösenord till nätverket kontrollerar systemet att du inte använder något av de 8 senast använda lösenorden.

Bortglömda lösenord
Om du försöker logga in till nätverket med ett felaktigt lösenord kommer systemet efter tre felaktiga försök att låsas. Om detta inträffar vänder du dig till IT-supporten eller behörighetshandläggaren på din förvaltning/bolag. Du kommer då att få ett nytt initialt lösenord.

3.4 Byte av lösenord

Byte av lösenord är aktuellt

- var 90:e dag när det gäller interna nätverket. En dialogruta visas på skärmen när det är dags.
- för enskilda system efter ett visst tidsintervall som bestäms av respektive systemägare
- omedelbart om du misstänker att någon annan känner till det

4. Din arbetsplats

Ordning och reda på arbetsplatsen är viktigt för säkerheten.
Kom ihåg att du ansvarar för allt som registreras med din användaridentitet.

Utskrifter på gemensamma skrivare ska hämtas så snart som möjligt. Tänk på att kvarglömda dokument kan komma i orätta händer.

Hög säkerhet är inte enbart kopplad till tekniska lösningar. Även med enkla förändringar av rutiner kan man uppnå detta t.ex. ”städat skrivbord”.

Se till att datorer som innehåller känslig information inte står placerade så att obehöriga kan läsa från skärmen (exempelvis i receptioner). Skärmsläckare ska alltid användas i denna typ av miljöer.

4.1 Utrustning

Den utrustning som du förfogar över, d v s stationär, dockningsbar PC (Viatores) och/eller bärbar PC med tillhörande utrustning gäller:

- Fysiska ingrepp får endast utföras av IT-Service
- Fel ska omgående anmälas till IT-service
- All installation och konfiguration får endast utföras av IT-service4.2 Programvaror
- Programvaror ska godkännas och installeras av IT-service eller av IT-service anvisad/godkänd person.
- Egna program kan, och får inte, installeras i myndighetens datorer.
- Om man har administratörsrättigheter kan man installera specialprogram på datorn men då på eget ansvar
- Det är inte tillåtet att kopiera eller använda myndighetens program utanför vår verksamhet.
- Om du är i behov av ytterligare programvaror eller hårdvara ska du anmäla det till din chef.

4.2 Mobil datoranvändning/distansarbete

Användning av bärbar IT-utrustning (bärbar pc, handdator, mobiltelefon etc.) innebär särskilda risker, i synnerhet om de används på oskyddade platser som konferenslokal, flygplats och hotellrum.

Därför bör du:

- Alltid hålla utrustningen och datamedia ständigt under uppsikt, och om du inte kan det ska du låsa in den.
- Tänka på att inte lagra verksamhetskritisk information på den bärbara utrustningen.
- Inte exponera känslig information vid arbete på t.ex. tåg.
- Tänka på vad du säger och var, i din mobiltelefon.
- Förvara utrustning och känslig information på ett säkert sätt, lämna aldrig datorn i bilen, tag datorn som handbagage vid flygresor och behandla den alltid som din egna.
- Använda lösenord vid uppstart av mobiltelefon och/eller handdator samt om möjligt lägga in ägarinformation.
- Inte låta anhöriga eller vänner nyttja den bärbara utrustningen.
- Helst alltid använda programportalen (program.falkenberg.se) vid externt arbete då allt lagras på kommunens servrar

4.3 Service på utrustning

Skall din arbetsstation på service skall du se till att eventuell känslig information avlägsnas. Om den går sönder måste du rådgöra med IT-service innan den sänds iväg på service eller kasseras.

4.4 Kassering av utrustning

Kontakta IT-service för destruktion.

4.5 Om du lämnar arbetsplatsen

Vid tillfällen när du inte har uppsikt över arbetsstationen kan du tillfälligt låsa arbetsstationen med kortkommandot: **CTRL+ALT+DEL och LÅS DATORN alt Windows flagga +L.**

För medarbetare med SHITS - kort skall kortet alltid tas med då du lämnar din arbetsplats

5. Klassning och hantering av information

5.1 Allmänhandling

För att allmänheten skall kunna utnyttja sin rätt att ta del av allmänna handlingar är det viktigt att man kan få veta vilka handlingar som finns hos myndigheterna.

En allmän handling som kommer in till myndigheten eller upprättas där skall därför registreras (diarieföras). Tre viktiga undantagsfall finns från denna regel. Följande handlingar behöver inte diarieföras:

- Handlingar som uppenbarligen har liten betydelse för myndighetens verksamhet (t.ex. pressklipp, cirkulär och reklamtryck).
- Handlingar som inte är säkerhetsskyddade och som hålls ordnade så att det utan svårighet kan fastställas, om de har kommit in till myndigheten eller upprättats där
- Handlingar som förekommer hos myndigheten i stor omfattning och som har undantagits från registreringsskyldigheten i sekretessförordningen (gäller för kommunens del endast för vissa handlingar hos socialnämnd och inrättningar för vård av patienter).

I tryckfrihetsförordningens 2 kap anges vad som menas med allmän handling.

En *handling* är en framställning i skrift eller bild men också en upptagning som man kan läsa, avlyssna eller uppfatta på annat sätt endast med hjälp av något tekniskt hjälpmedel. Man kan uttrycka det så att en handling är ett föremål som innehåller information av något slag.

En *elektronisk handling* är en bestämd mängd data som kan läsas, avlyssnas eller på annat sätt uppfattas endast med hjälp med tekniskt hjälpmedel.

En handling är allmän om den förvaras hos en myndighet och enligt särskilda regler anses *inkommen* dit eller upprättad där.

En handling som överförs elektroniskt anses enligt huvudregeln ha kommit in till myndigheten när data som representerar handlingen har nått myndighetens tekniska funktion för att ta emot e-post eller med andra ord, har anlänt till myndighetens elektroniska adress.

En elektronisk handling som har överförts till en e-postadress som tjänstemannen innehar privat eller som arbetsgivaren tillhandahåller, utan att den utgör en officiell adress för myndigheten, anses inkommen när handlingen har tagits emot av behörig tjänsteman.

5.2 Klassning av information

Utgångspunkten för all informationsklassning är att den ska utgå ifrån Falkenbergskommuns behov av skyddsåtgärder för den specifika informationen.
All information kommer inte att behöva samma skydd. Viss information kanske inte behöver skyddas alls. Annan information kan behöva avsevärda skyddsåtgärder.

När man klassificerar Falkenbergskommuns informationstillgångar ska man utgå ifrån informationens vikt utifrån informationssäkerhetskraven på sekretess, riktighet och tillgänglighet.

- **Sekretess:** Här klassas information efter vem eller vilka som får ta del av den
- **Riktighet:** Här klassas information efter hur viktig det är att man kan lita på den
- **Tillgänglighet:** Här klassas informationen efter hur viktigt det är att den är tillgänglig

Falkenbergskommuns klassningsmodell framgår av bifogad bilaga 2

I modellen klassificeras information utifrån de konsekvenser som oönskad påverkan på informationens kvalitet bedöms leda till.
Konsekvenserna värderas i termer av oönskad påverkan på verksamheten eller annan part till följd av otillräcklig sekretess, riktighet eller tillgänglighet.
Om exempelvis organisationen lider allvarlig skada av att viktig information för verksamheten blir tillgänglig för obehöriga, ska informationen placeras i en klass med hög konsekvensnivå avseende sekretess.

5.3 Lagring

Den information du lagrar på våra gemensamma utrymmen säkerhetskopieras automatiskt. Du kan välja att lagra på enheterna W, V eller P.

OBS! På ovanstående enheter får inte sekretesskyddade uppgifter lagras, se vidare bilaga

W: (Personlig hemkatalog) är din personliga enhet som endast får användas för dokument/filer som används i ditt arbete. Om du väljer W - enheten kommer dina medarbetare ej åt informationen.

V: (Organisationsenhet) är en enhet för lagring av dokument/filer som alla medarbetare på din enhet bör ha tillgång till.

P: (Kommun gemensam) är en enhet för tillfällig lagring av dokument/filer som alla medarbetare i den kommunala organisationen bör ha tillgång till t ex när man delar stora dokument mellan förvaltningar.

I förekommande fall kan också ytterligare enhetsbeteckningar finnas

6. Internet/Intranät

Organisationens nätverk är anslutet till Internet via en brandvägg som reglerar in- och utgående trafik. Trafik genom brandväggen loggas. Loggen kan användas för granskning om misstanke om brott föreligger.

Intranätet finns tillgängligt för alla som är i kommunens administrativa nätverk övriga når det via inloggning från hemsidan. Här informeras om allt som händer i vår miljö, här finns också möjligheten att lägga felanmälningar till IT-service.

När du använder Internet kan säkerheten i myndighetens lokala nätverk påverkas i mycket hög grad beroende på ditt beteende. Myndigheten förutsätter att den som surfar på Internet endast besöker välrenommerade webbplatser.

Det är inte tillåtet att via Internet ladda ner spelprogram eller poker sajter in i kommunens system. Gratisprogram får inte laddas in i kommunens system utan att de godkänts av IT-servicen och genomgått ett virustest.

Det är inte tillåtet att via Internet titta eller lyssna på material av pornografisk, nazistisk eller rasistisk karaktär. Förbudet gäller också material som är diskriminerande (religion, kön, sexuell läggning, nationalitet, etc.) eller har anknytning till kriminell verksamhet.

I specifika fall kan det dock vara motiverat för arbetet, t ex vid utredningar, omvärldsanalyser mm, att besöka sidor som normalt är förbjudna. Beslut om detta bör fattas av närmaste chef.

Tänk på att när du surfar på Internet representerar du Falkenbergs Kommun och lämnar spår efter dig i form av Falkenbergs Kommuns IP-adress.

För privat användning under arbetstid gäller samma regler som för telefoni, om det inkräktar på arbetets utförande och resultat är det inte acceptabelt

Missbruk av Internet
Exempel på missbruk av Internet finns nedan. Missbruk kan i vissa fall leda till rättslig påföljd

- Spam, massutskick via e-post.
- Dataintrång
- Kedjebrev, pyramidspel via e-post/news
- Att skicka mail bomber, dvs. många mail samtidigt i syfte att skada
- Att sända e-post som är kränkande eller hotfull
- Att trakassera andra via e-post, på chat eller i andras gästböcker/anslagstavlor
- Att dela ut processorkapacitet eller spela spel över Internet

7. 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”, se vidare under 7.1 Gallring. E-postsystemet ska inte användas som ett arkivsystem. Meddelanden, bifogade filer mm som du vill spara, sparar du på samma sätt som du lagrar annan information.

E-post ska i Falkenbergs Kommun användas på ett sådant sätt att hänsyn tas till både säkerhet och offentlighetsprincipen.

Var selektiv med att skicka eller vidarebefordra meddelanden som innehåller stora filer för att undvika onödig belastning av systemresurser. Tänk på att även e-post som skickas från kommunens nätverk via Internet (t.ex. från Windows live, hotmail, osv.) registreras med kommunens IP-adress.

Om du under en längre period inte har möjlighet att kontrollera din e-post skall du sätta frånvarobesked med uppgift om vem som ska hantera dina inkommande ärenden.

E-post med bilagor utgör ett stort hot när det gäller spridning av virus.

- e-postsystemet är ett arbetsverktyg och bör inte användas för privat bruk.
- samma regler gäller 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.
- e-postsystemet får inte användas för kedjebrev, pyramidspel eller annat där man uppmanar andra användare att skicka pengar eller att vidarebefordra texter i all oändlighet
- användaren bör inte skicka e-post filer i stora volymer utan godkännande från systemansvarig för den e-post server som används.
- ange alltid ämne i ämnesraden för meddelandet för att klargöra för mottagaren vad denne kan förvänta sig för innehåll i e-posten.
- skriv inte någon känslig information i ämnesraden
- kontrollera vilka som är medlemmar på sändlistor innan du använder dem, (risk att känslig information når fel mottagare)
- skriv korta brev
- använd ”läskvittens” för interna meddelanden endast när du har behov av detta
- tänk på hur du sprider din e-postadress
- i varje tjänstemans brevlåda är vyerna (översikterna) *Inkorg och Skickat* att betrakta som ett diarium och ska vid förfrågan från medborgare och media visas upp eller kopieras, utlämning av brev sker efter sedvanlig sekretessprövning.
- viktiga handlingar bör inte skickas enbart med e-post utan även med reguljär post.
- om du får hotelsebrev ska du spara brevet och kontakta din chef

Observera. E-postsystemet får inte användas för att skicka sekretessbelagd information

7.1 Gallring

Gallring är en strukturerad utrensning av information som bedöms vara mindre betydelsefull i ett långtidsperspektiv.
Det innebär att gallring alltid ska föregås av en informationsklassning där informationens värde bestäms utifrån krav från lagstiftning och verksamhet. I dag produceras mer information än någonsin på olika medier, därför blir också gallringen allt viktigare eftersom väsentlig information tynger informationssystemen.
I den offentliga verksamheten styrs gallring från tryckfrihetsförordningen och arkivlagen som innebär att en mycket stor del av den information som inkommer till Falkenbergs Kommun är att betrakta som allmänna handlingar. Allmänna handlingar får inte förstöras utan ett gallringsbeslut.

Radera e-post, cookies och temporära Internet filer
I Falkenbergs kommun får du radera

- E-post av mindre betydelse omgående
- Cookiefiler och temporära Internet filer efter inaktualitet

8. Incidenter, virus mm

8.1 Allmänt incidenter

En incident kan vara i stort sett vad som helst: från besökare på villovägar, olåsta dörrar och misslyckad säkerhetskopiering, till driftavbrott, försök till dataintrång och virusangrepp. En incident kan vara en medveten handling eller ske helt oavsiktligt. Någon glömmer t.ex. att låsa en dörr eller att säkerhetskopiera informationen på en server.

Incidenter eller bister som upptäcks skall hanteras enligt **bilaga 3** i denna instruktion. Vilket innebär att alla fall av olovligt dataintrång, eller brott mot tystnadsplikt eller sabotage mot IT-system skall rapporteras som avvikelser.

Myndigheten rapporterar IT – incidenter till PTS. Om du misstänker att någon använt din användaridentitet eller att du varit utsatt för någon annan typ av incident ska du:

- notera när du senast var inne i IT-systemet
- notera när du upptäckte incidenten
- omedelbart anmäla förhållandet till IT-service och/eller din chef.
- dokumentera alla iakttagelser i samband med upptäckten och försöka fastställa om kvaliteten på din information har påverkats

8.2 Virus

Virus eller skadlig kod är oönskade programmerade instruktioner för datorn t.ex. virus, maskar och trojaner. Det är det vanligast förekommande hotet mot IT-system. Det som är gemensamt för de olika typerna av skadlig kod är att de skapar extra kostnader, både genom det förebyggande arbetet, åtgärdsarbete och som krävs om någon incident skulle inträffa. Ytterligare bieffekter som eventuellt kan tillkomma efter en incident är t.ex. kostnader i form av minskad produktivitet, skadad utrustning, skador på nätverket, förlorade affärer, ränteförluster p.g.a. försenade betalningar, intern information som sprids externt och imageförlust. Den skada som sker är beroende av hur den skadliga koden "ser ut" och hur den drabbade datormiljön är utformad.

Skadlig kod benämns ofta som virus, mask eller trojan. Ibland används flera begrepp för att beskriva samma skadliga kod, eftersom det blivit vanligare med kombinerade hot, t.ex. en blandning av mask och trojan. Definitionerna går delvis in i varandra eftersom de är närbesläktade.

Falkenbergs Kommun har programvaror för viruskontroll både i klienterna och i nätverket, men kan ändå drabbas av effekter av s.k. skadlig kod. Om du misstänker att din dator innehåller virus ska du:

- dra ut nätverkskabeln, men låta datorn vara på
- omedelbart anmäla förhållandet till IT-service eller till närmaste chef. OBS! Anmälan ska ske per telefon (0346-88 55 55) eller besök, inte per e-post.

Om du får brev med virusvarning gör inget annat än att kontakta IT-service.

Handdatorer, digitala kameror, USB-minnen, mobiltelefoner mm kan lätt bli virusbärare eftersom du kan mellanlagra information mellan olika datorer i dessa. Var noga med att den dator du ansluter sådan kringutrustning till har ett uppdaterat virusprogram.

9. Avslutning av anställning

När du slutar din anställning ansvarar du för att:

- rådgöra med din chef om vilket av ditt arbetsmaterial som ska sparas, notera att allt arbetsmaterial du framställt anses vara Falkenbergs Kommuns egendom och får inte tas med utan chefs godkännande.
- privat material tas bort
- de behörigheter du fått för åtkomst till våra informationssystem avbeställs av din chef

Bilaga 1 - Användarinstruktion sekretesskyddade uppgifter för Hälso- och Sjukvård och Socialtjänsten.

Denna rutin handlar om hantering av sekretesskyddade uppgifter i elektroniska produkter, datasystem, lagringsmedia samt överföring däremellan inom socialförvaltningen och skolhälsovården och deras entreprenader.

Rutinen behandlar inte förvaring av uppgifterna i pappersform.

Lagring av uppgifter

Var får uppgifterna förvaras
- I journalsystemen för skolhälsovården. I journalsystemen för äldre- och handikappomsorgen och individ- och familjeomsorgen.
- Sekretesskyddade uppgifter som inte kan lagras i berörda journalsystem får skrivas ut på papper och förvaras på det sätt som föreskrivs för fysiska akter

Var får uppgifterna inte förvaras
- I enskilda datorer/handdatorer/mobiltelefoner eller annan enhet på arbetsplatsen eller annan plats. Detta hindrar inte att ha tillgång till berörda journalsystem från bärbar dator på annan plats som loggar in via Citrix. I dessa fall sker ingen lagring i datorn.
- I kommunens nätverk om inte Systemansvarig har gett skriftligt tillstånd. Sådant tillstånd ges normalt inte.
- På server eller nätverk utanför kommunens nätverk
- Diskett, CD, DVD, USB minne, flyttbar hårddisk liknande.

Överföring av sekretesskyddade uppgifter

Hur får sekretesskydda uppgifter överföras
- Genom meddelandesystemet i berörda journalsystem
- Genom telefon
- Genom telefax om faxnumret uppgiften sänds till är fast lagrad i den sändande faxen, har prövats och mottagaren står vid sin fax för att ta emot uppgiften. Mottagaren behöver inte stå vi faxen vid mottagande om uppgiften lagras i mottagande faxen och enbart kan tas ut efter inmatning av säkert lösenord
- Genom brev

Hur får sekretesskyddade uppgifter inte överföras
- Annat mail system (inkl. kommunens mail och externa system som t.ex. hotmail), chat program (t.ex. MSN), Community program (t.ex. facebook) eller liknande tjänster eller på annat jämförbart sätt.
- Om man erhåller sekretesskyddade uppgifter via mail skall mailet skrivas ut och behandlas som en inkommen handling. Mailet får inte besvaras genom svars mail utan enbart på det sätt som beskrivs under punkten ”hur får sekretesskyddade uppgifter överföras”

Åtkomstskydd

Dator som används för åtkomst av uppgifter i berörda journalsystem skall skyddas så att inte obehörig kan få tillgång till sekretesskyddade uppgifter. Detta kan ske genom att
- Datorn står i utrymme som enbart är tillgänglig för behörig personal om så är möjligt, dessutom
- skall utloggning ske från berörda journalsystem så fort den som loggat in inte lägre behöver ha tillgång till systemet eller lämnar datorn

Spårbarhet
Det skall gå att kunna spåra vem som haft tillgång till sekretesskyddat material. Detta sker genom att
inloggning till berörda journalsystem enbart sker genom personal som har enskild behörighet
Gruppbehörigheter får inte användas.

Förhållningssätt vid tillgång till sekretesskyddade uppgifter

Det bör påpekas att den som har tillgång till sekretesskyddade uppgifter enbart får läsa de uppgifter man behöver för att kunna utföra arbetet. Uppgifter därutöver får man inte befatta sig med även om man har tillgång till dem.

Information till personalen
Närmaste chef ansvarar för att:

- Informera nyanställd personal om denna rutin (bilaga 1) i samband med personalintroduktionen. Medarbetaren skall skriva på försäkran om sekretess för informationssäkerhet, (bilaga 2) som bevis för att man erhållit och förstått informationen. Dokumentet förvaras sedan i den anställdes personakt.

- Redan anställd personal informeras om denna rutin i samband med APT eller i annat sammanhang **senast 2012-12-31**. Personalen skall i samband därmed skriva på försäkran om sekretess för informationssäkerhet, (bilaga 2) på samma sätt som vid personalintroduktion.

- Innehållet i denna rutin (bilaga 1) gås igenom med berörd personal i samband med arbetsmiljö/skyddsronden - två gånger om året.

Bilaga 2 – Försäkran om sekretess för Informationssäkerhet

Jag har tagit del av Falkenbergs kommuns ”Informationssäkerhetsinstruktioner för användare” och försäkrar att jag kommer att följa dessa.

Jag är medveten om att dessa instruktioner bland annat handlar om hantering av sekretesskyddade uppgifter i elektroniska produkter, datasystem, lagringsmedia sam överföring däremellan.

Jag försäkrar även att jag kommer att ta del av och följa de förändringar som görs av instruktionerna. Jag är medveten om de åtgärder som kan vidtagas vid brott mott dessa instruktioner.

Arbetstagarens namnteckning	Namn förtydligande

Arbetsgivarens namnteckning	Namn förtydligande

Denna försäkran skrivs ut i två exemplar:

1 exemplar till arbetsgivarens personal akt

1 exemplar till arbetstagaren

Bilaga 3 – Rutin för misstanke av

Dataintrång
Brott mot tystnadsplikt
Sabotage IT-system

Tillämpningsområde: Falkenbergs kommun

Syfte

Klargöra hur arbetsgivaren Falkenbergs kommun agerar när medarbetare:

1.tagit del av patientinformation utan att ha rätt till den. (dataintrång)
2.när medarbetare brutit mot tystnadsplikten och röjt sekretessbelagda uppgifter. (brott mot tystnadsplikt)
3.när medarbetare medvetet orsakat störning/avbrott på it-system (=sabotage). (sabotage/skadegörelse)

1. Patientjournaler

Elektroniska patientjournaler innebär att många personalgrupper har tillgång till information om ett stort antal patienter. Att gå in och läsa och ta del av andra patientjournaler/uppgifter än dem användaren har rätt till kan betraktas som dataintrång och/eller brott mot tystnadsplikt, där arbetstagaren riskerar åtal. Härutöver riskerar arbetstagaren arbetsrättsliga påföljder.

Lagöverträdelser

1. **Dataintrång - 4 kap 9 c § brottsbalken***
   Den som i annat fall än som sägs i 8 och 9 §§ olovligen bereder sig tillgång till en uppgift som är avsedd för automatiserad behandling eller olovligen ändrar, utplånar, blockerar eller i register för in en sådan uppgift döms för *dataintrång* till böter eller fängelse i högst två år. Detsamma gäller den som olovligen genom någon annan liknande åtgärd allvarligt stör eller hindrar användningen av en sådan uppgift.

   Kommentar
   Alla uppgifter, d v s fakta, information eller begrepp, som uttrycks i en för en dator anpassad och läsbar form omfattas av bestämmelsen.

2. **Brott mot tystnadsplikt - 20 kap 3 § brottsbalken**
   När medarbetare brutit mot tystnadsplikten och röjt sekretessbelagda uppgifter.
   Röjer någon uppgift, som han är pliktig att hemlighålla enligt lag eller annan författning eller enligt förordnande eller förbehåll som har meddelats med stöd av lag eller annan författning eller utnyttjar han olovligen sådan hemlighet dömes, om ej gärningen eljest är särskilt belagd med straff, för *brott mot tystnadsplikt* till böter eller fängelse i högst ett år. Den som av oaktsamhet begår gärning som avses i första stycket, dömes till böter. I ringa fall skall dock ej dömas till ansvar.

   Kommentar
   ”Röjer” innebär inte något mera än att uppgiften lämnas ut. Det krävs således inte att utlämnandet medför ett avslöjande. Ett utnyttjande av en hemlig uppgift kan exempelvis bestå i att göra ekonomiska dispositioner i eget intresse eller andra handlingar och åtgärder på grund av uppgiften.

3. Sabotage/Skadegörelse - Regleras i 12-13 kap brottsbalken

Förtroendemissbruk
Förutom att dataintrång och/eller brott mot tystnadsplikt är olagligt är det att betrakta som ett ***förtroendemissbruk*** där arbetstagaren till skada för arbetsgivaren kan utnyttja vårdinformation för egen vinning. Sabotage mot it-system ses också som ett ***förtroendemissbruk***.

Bedömningen av vilka åtgärder som lämpligen bör vidtas vid förtroendemissbruk måste, som inledningsvis påpekats, göras utifrån omständigheterna i varje enskilt fall. Av betydelse är gärningens art och omfattning, arbetstagarens ställning och graden av den skada arbetsgivaren respektive tredje man lidit.

2. Ansvar - chef och medarbetare

Ansvaret för informationssäkerheten följer ytterst verksamhetsansvaret, men *alla har ett egenansvar.* **Falkenbergs kommun accepterar inte att medarbetare otillåtet öppnar patient/skolhälsovårdsjournaler**. Det ska stå klart för alla att ett sådant beteende inte är tillåtet och vilka konsekvenser det kan få.

Chef ansvarar för att informera medarbetare om regler som gäller för vårdinformation och eventuella konsekvenser om man bryter mot dessa. Särskild rutin gäller för information till personal som ska använda tjänstelegitimation/SITHS-kort (se intranätet Nationell eHälsa). Vid informationen ska chefen försäkra sig om att medarbetaren inte bara tagit del av informationen, utan även förstått den. Bilagorna 1-4.

Hälso- och sjukvårdspersonal får ta del av dokumenterade uppgifter om en patient/elev:

- Om han eller hon deltar i vård och behandling eller skolhälsovård av patient/elev, det vill säga har en vårdrelation. Med vårdrelation menas att arbetstagaren deltar i eller ansvarar för vård eller skolhälsovård som är pågående (planeras och genomförs).

- Om uppgifter behövs av andra skäl för arbete inom hälso- och sjukvården ska detta vara på uppdrag av verksamhetschef/motsvarande, till exempel utvärdering, kvalitets-granskning, administration eller för att genomföra en särskild patientstudie på en vårdenhet.

- Om andra behov finns till exempel forskning, där en etikprövningsnämnd ska ha godkänt studien och patienten ska lämna sitt samtycke till att informationen får hämtas.

Socialtjänstpersonal får ta del av dokumenterade uppgifter om en brukare/klient:

- Om han eller hon deltar i planerade eller pågående insatser till/utredning av brukare/klient och behöver uppgifterna för att utföra sina arbetsuppgifter.

- Om uppgifter behövs av andra skäl för arbete inom socialtjänsten ska detta vara på uppdrag av verksamhetschef/motsvarande, till exempel utvärdering, kvalitetsgranskning, administration eller för att genomföra en särskild brukar-/klientstudie på en enhet.

- Om andra behov finns, till exempel forskning, där en etikprövningsnämnd ska ha godkänt studien och brukaren/klienten ska lämna sitt samtycke till att informationen får hämtas.

3. Åtgärder vid misstanke om dataintrång/brott mot tystnadsplikt/sabotage mot it-system

Avvikelse

Alla fall av olovligt dataintrång eller brott mot tystnadsplikt eller sabotage mot it-system ska *rapporteras som avvikelse,* se bilaga 4.

Avvikelserna ska följas upp av närmast ansvarig chef och bedömningen av vilka åtgärder som kan och lämpligen bör vidtas. Detta måste på sedvanligt sätt göras mot bakgrund av omständigheterna i varje enskilt fall. Av betydelse är gärningens art och omfattning, arbetstagarens ställning och graden av den skada arbetsgivaren respektive tredje man lidit. Med skada för arbetsgivaren avses inte enbart ekonomisk skada utan även den skada som tillfogas arbetsgivaren genom ett minskat förtroende från allmänheten.

4. Vid misstanke om dataintrång, brott mot tystnadsplikt eller sabotage mot it-system ska åtgärder vidtas i följande steg:

Steg 1. Förvaltningen

Vid arbetsgivarens misstanke om dataintrång och brott mot tystnadsplikt ska berörd chef med personal- och verksamhetsansvar för den **som** är misstänkt omedelbart kontakta närmast överordnad chef och fakta ska samlas in. Ett underlag är loggkontrolluppgifter.

- Berörd chef för den som är misstänkt, personalchef och facklig representant träffar den person som misstänks.
- Mötet ska klarlägga bilden av misstanken och den misstänkte ska ges möjlighet att yttra sig. Mötet ska dokumenteras. Gruppen gör en bedömning om misstanken kvarstår eller inte.

Sabotage IT-system

När personal på IT Service, chef eller medarbetare misstänker sabotage mot it-system ska förvaltningschefen till den/de som misstänks, och personalchefen informeras och handla enligt ovan. Se *Informationssäkerhetsinstruktion Användare Kap 7. Incidenter, virus mm.*

Steg 2. Om misstanken kvarstår

Berörd chef för den som misstänks, förvaltningschef och personalchef tar ställning till fortsatta åtgärder.

Brottsmisstanke

Som huvudregel ska polisanmälan göras om det kan påvisas att arbetstagaren uppsåtligen har berett sig tillgång till information som arbetstagaren inte har rätt att ta del av och/eller på något sätt brutit mot tystnadsplikten. Arbetsgivaren lämnar då över till annan myndighet att göra bedömning om brott anses ha begåtts. Berörd förvaltningschef beslutar om polisanmälan ska göras. Polisanmälan formuleras alltid av personalchefen. Berörd förvaltningschef skriver under.

Arbetsgivaren kan även efter en anmälan till polis- eller åklagarmyndighet inleda eller fortsätta en utredning för att klarlägga om det finns grund för uppsägning eller avskedande. Om arbetstagaren nekar till brott kan arbetsgivaren varsla och underrätta enligt 30 § LAS men vänta med uppsägning eller avsked till dess brottsligheten har prövats av domstol (se AD 1976 nr 51). Om arbetstagaren däremot erkänner brottet, måste arbetsgivaren inom två månader efter kännedom om erkännandet, åberopa brottet som grund för uppsägning eller avskedande enligt LAS.

Patienten/eleven/brukaren/klienten
Vid lämpligt tillfälle i processen, dock alltid före polisanmälan ska patienten/eleven/brukaren/klienten som har blivit utsatt för dataintrånget/brottet mot tystnadsplikt, informeras av verksamhetschef/ /motsvarande/chef för den som är misstänkt.

Steg 3. Arbetsrättsliga åtgärder
Observera att disciplinförfarande inte får inledas eller fortsätta om arbetsgivaren har anmält förseelsen till polis- eller åklagarmyndighet (AB § 11 mom 2). Först när den processen är avslutad kan den arbetsrättsliga processen påbörjas.

Avstängning
Arbetstagaren kan av arbetsgivaren, vanligtvis genom arbetsledningsbeslut, tillfälligt tas ur arbete (AB § 10). Inför beslut ska arbetsgivaren genomföra överläggning med berörd lokal facklig organisation. Avstängning är en tillfällig åtgärd i avvaktan på att arbetsgivaren tar ställning till ett eventuellt beslut om polisanmälan, disciplinpåföljd, uppsägning, avskedande eller annan åtgärd.

Disciplinpåföljd eller uppsägning/avskedande
Disciplinförfarande (varning) får inte inledas eller fortsätta om arbetsgivaren har anmält förseelsen till polis- eller åklagarmyndighet (AB § 11 mom. 2). Om polis eller åklagare avskriver ärendet eller om arbetstagaren frikänns på grund av att gärningen visserligen har begåtts men inte är brottslig, kan disciplinpåföljd trots detta komma ifråga för samma gärning.

Bilaga 4 – exempel på avvikelser

Kategori	Typ av frågor/avvikelser - exempel
Informationssäkerhet • Försummelse i efterlevnad av policy och instruktioner • IT-funktionsrelaterade problem • Sekretessbrott	**Avvikelsen** **Exempel:** o Felanvändning av Internet, program, nätverk, dator o Olovlig/felaktig installation av program i apparat/nätverk o Avsaknad av licens för programanvändning o Användning av annans inloggning o Loggkontroll i system - ej genomförd o Fax av patientinformation o Brev – fel kuvert, fel adress, ej rek Störning eller avbrott i IT-system som äventyrat informationssäkerheten exempelvis åtkomst av patientuppgifter i journalsystem saknas helt eller delvis **Exempel:** o Fel behörighet o Obehörig tagit del av eller felaktigt förvarad information o Ej upprättat sekretessavtal med person/ företag o Överhörning vid diktering/telefonering/möten
Kategori	**Typ av frågor/avvikelser – exempel**
IT och kommunikationsteknik • Datakommunikation • IT-stöd · Hårdvara · Mjukvara • Telefoni	Fel vid överföring av information mellan olika system eller vid åtkomst av data över nätverket Funktionella brister på utrustningen, exempelvis tangentbord eller skärm på en pc-arbetsplats Funktionella brister i program Fel på telefoni, sökare eller sökning
Kategori	**Typ av frågor/avvikelser – exempel**
Patient/elev/brukare/klient o Lex Sarah o Lex Maria o Synpunktshantering	Inom socialtjänsten och hälso- och sjukvården finns särskilda regelverk som reglerar avvikelser, skador och risk för skador i förhållande till brukare/elev/patient/klient/kund. Uppfylls förutsättningarna enl. dessa regelverk skall ärendet handläggas enl. dessa regelverk oberoende av eventuell annan handläggning.

Bilaga 5 - Ordlista

AD	Active Directory, behörighets databas där alla användare och resurser kopplas ihop.
Användaridentitet	En unik identitet för en person som utnyttjar ett datasystem
Behörighet	Rättighet för en användare att utnyttja olika resurser i ett datasystem. Rättigheterna bör överensstämma med personens uppgifter och ansvar i den verksamhet där personen är aktiv.
Behörighetsansökan	Handling underskriven av ansvarig chef och anställd och som reglerar den anställdes behörighet.
Behörighetshandläggare	En person på förvaltning/bolag som utsetts till att hantera underskrivna behörighetsansökningar.
Behörighetskontroll	Administrativa och tekniska åtgärder för kontroll av användares identitet, styrning av användares behörighet att använda datasystemet och dess resurser samt för registrering av denna användning.
Behörighetskontroll-system	Säkerhetsfunktioner som tillsammans utför behörighetskontroll i ett datasystem.
Bifogade filer	Dokument som skickas som separat fil kopplad till ett e-meddelande (i e-postsammanhang).
Brandvägg	Hinder mot oönskad kommunikation mellan olika datornät, främst mot intrång.
Cookie-filer (kakor)	Liten datamängd med information om tidigare besök som en webbserver skickar till en webbläsare och senare kan hämta information därifrån. Om man flera gånger vid olika tillfällen besöker en viss webbserver eller webbplats, så medför kakan att webbservern kan känna till att man tidigare varit där och också veta vad man gjort vid de tidigare besöken. Exempel: Om man gått in på en viss banks webbplats och sökt sig fram till sitt lokala kontors webbsida, kan informationen i kakan styra så att man vid nästa besök på bankens webbplats kommer direkt till det lokala kontorets webbsida.
Data	Uppgifter om olika företeelser, t ex anställda.
Dataintrång	Obehörig tillgång till information i IT-system. Datalagen anger i 21 § straff för dataintrång för den som olovligen bereder sig tillgång till datauppgift eller olovligen ändrar eller utplånar eller gör tillägg.
Datasystem	Innefattar datorer, program, servrar mm., den tekniska lösningen och utformningen.
Diskutrymme	Utrymme data tar på en hårddisk.
E-post	Överföring av meddelande med hjälp av datorer där meddelandet kan läsas vid valfri tidpunkt.

Filserver	En server där man lagrar filer (data) och som kan nås av flera användare. På denna finns ofta användarnas ”hemkataloger”.
Gratisprogram	Program du kan använda utan att betala licenskostnad.
Hemkatalog	Den plats på en filservers lagringsutrymme där du kan lagra dina filer.
Hårddisk	Enhet i server eller klient som fysiskt lagrar data.
Incident	Oönskad händelse, t ex datavirusattack.
Intranät	Ett internt ”Internet” för kommunens användare.
Internet	Det internationella datornätet som har största utbredningen och som bygger på TCP/IP, en standard för datakommunikation.
IT-system	Hur datakomponenter som datorer, program, och kablar samarbetar.
IT-säkerhetsfunktion	IT-säkerhetsfunktionen finns centralt på stadskontoret och understödjer arbetet med att uppnå IT-säkerhetspolicyns mål.
Kedjebrev	Brev som det är tänkt skall föröka sig genom att brevskrivarna skickar samma brev till flera personer.
Klient	Den anställdes dator.
Logg	Kontinuerligt insamlad information om de operationer som utförs i ett datasystem. Registrerade uppgifter kan utnyttjas till att i efterhand analysera vilka operationer som utförts och vilka användare som initierat dessa.
Loggning	Förande av logg.
Lösenord	Används i samband med inloggning. Lösenordet kan vara genererat av systemet eller (till skilda delar) av bägge.
Mailbomber	När man skickar en stor mängd e-postmeddelanden samtidigt till en e-postserver för att den skall sluta att fungera.
Modemuppkoppling	Då man använder en vanlig telefonledning för datakommunikation.
Nätverk	Ett system av datorer, som på något sätt är förbundna med varandra, t ex via kablar eller trådlöst.
Program	Instruktioner lagrade i datorn, som styr hur den fungerar.
Server	Vanligtvis mer kraftfull dator som används av flera klienter.
Shareware (spridprogram)	Program som får spridas fritt men som användaren förväntas betala en avgift för vid upprepad användning

Snabel-a	Tecknet @ (ett ringomgärdat a)
Spam	Man skickar skräppost.

Surfa	Besöka olika webbplatser genom att använda de länkar som finns på webbsidorna, möjligen utan att ha ett på förhand definierat mål.
System	Består av komponenter som på något sätt är förbundna med varandra.
Systemansvarig	Utses av nämnd/styrelse och företräder den i hanteringen av ett system.
Systemförvaltare	Har det övergripande ansvaret för att de olika datasystemens tekniska delar fungerar.
Systemadministratör	Ansvarar tillsammans med systemförvaltaren för att den dagliga driften upprätthålls enligt överenskommelse med systemansvarig.
Säkerhetskopia	Kopia av fil eller andra data som sparas för att användas om originalet blir förstört.
Temporära Internet-filer	Används för att spara webbsidor och filer (till exempel bilder) medan du tittar på dem. Detta gör att det går snabbare att visa webbsidor som du ofta besöker eller redan har sett.
Verksamhetssystem	System som används för att effektivisera eller på annat sätt förbättra en verksamhet.
Vidarekoppling	Automatisk vidaresändning av e-post till ett annat e-postsystem.
Webbaserad e-post	En form av e-post är s.k. webbaserad e-post. Det är en e-posttjänst som användaren får tillgång till genom att logga in på en viss webbsida och som inte kräver något e-postprogram eller eget abonnemang hos en Internetleverantör.
Webben	Funktion på Internet eller på ett intranät som medger att man enkelt kan hämta sammanlänkad information i form av text, bild och ljud.
Webbläsare	Datorprogram för hämtning och visning av information.
Webbsida	Den mängd information på en webbplats som man kan nå utan att behöva gå vidare via en länk; motsvarar ofta så mycket man kan se på skärmen samtidigt eller genom att rulla bilden.