FALKÖPING
KOMMUNEN

Säkerhetsinstruktioner för användare av Falköpings kommuns nätverk

SÄKERHETSINSTRUKTIONER FÖR ANVÄNDARE AV FALKÖPINGS KOMMUNS NÄTVERK

1 BAKGRUND 1

2 INLOGGNING 1

3 HANTERING AV INFORMATION 3

4 INTERNET 4

5 E-POST 5

6 SÄKERHETSINCIDENTER 5

7 BÄRBARA DATORER, MOBILTELEFONER OCH EXTERNA LAGRINGSMEDIA 6

8 ARBETSPLATSEN 6

1 BAKGRUND

Dessa instruktioner avser i första hand de som har en inloggning i kommunens personalnätverken. Instruktion ligger även till grund för och används i tillämpliga delar i de säkerhetsinstruktioner som gäller för skolans elever.

Information är en mycket viktig tillgång för vår kommun. För att skydda de värden informationen representerar krävs ett säkerhetsmedvetande hos alla medarbetare. Du som användare har alltså en stor del av ansvaret för säkerheten i vår informationshantering. Som bilaga till säkerhetsinstruktionen finns kommunens ”Riktlinjer för hantering av e-post och Internetanvändning.” De utgör tillsammans med säkerhetsinstruktionen det ramverk som gäller för användare av Falköpings kommuns nätverk. För att du ska kunna leva upp till de säkerhetskrav som ställs på dig är du skyldig att känna till:

- ***vilka regler som gäller och vilket ansvar du har***
- ***vad du ska göra vid olika incidenter***
- ***var du kan få stöd och hjälp***

Det mesta du behöver veta finns i detta dokument. Ta dig därför tid och läs igenom dessa sidor. Är det något du inte förstår eller som du tycker verkar oklart får du gärna kontakta IT-avdelningens. Du vänder dig då till IT-support som du når på **tel. 88 53 00** under kontorstid. Det gäller även i alla andra frågor som rör IT-avdelningens verksamhet. Vill du ha en mer heltäckande beskrivning av kommunens alla IT-säkerhetsregler ska du läsa den Generella säkerhetsinstruktionen

Särskilda regler för vissa system

Observera att vissa system, som hanterar särskilt känsliga uppgifter, kan ha striktare säkerhetsregler än de som beskrivs här. Om något av de system du använder innehåller särskilt känsliga uppgifter bör du därför kontrollera med din systemanförvaltare om det finns kompletterande säkerhetsinstruktion för det systemet.

2 INLOGGNING

Nätverket är utrustat med ett inloggningssystem (BKS) för att garantera att det bara är behöriga användare som kommer åt information och att en användare enbart kan komma åt den information som den behöver för att utföra sina arbetsuppgifter.

För alla anställda innebär anställningsavtalet att man automatiskt får behörighet till kommunens nätverk. Det innebär att du, förutom möjlighet att logga in i nätverket, också får tillgång till e-post, kontorsprogram, Internet, intranät och öppna interna webb-tjänster. (För icke anställa finns en manuell rutin.) Behöver du dessutom använda något verksamhetssystem (t.ex. Procapita) är det systemägaren (vanligtvis din förvaltningschef) som beslutar om detta. Därefter ansvarar Du för att följa de regler som kopplas till behörigheten.

För att få behörighet krävs därför att:

1. Din chef har skrivit under ditt anställningsavtal
2. Din förvaltningschef beslutar om vilka verksamhetssystem du ska ha.
3. IT-avdelningen ser till att du får tillgång till de tjänster som du har behörighet till.
4. Därefter får du:

- **EN ANVÄNDARIDENTITET** Användaridentiteten är ditt ”namn” i nätverket och konstrueras efter principen: de tre första bokstäverna i ditt förnamn samt en unik tresiffrig kod.
- **ETT LÖSENORD** – Som alltid är din egen hemlighet!

Initialt lösenord

Första gången loggar du in med ett initialt lösenord som du får av IT-avdelningen. Det lösenordet ska du bara använda en gång för att komma in i systemet och därefter byta det till ditt personliga lösenord. På detta sätt säkerställs att det bara är du själv som känner till ditt lösenord.

Lösenordet är strängt personligt!

och ska hanteras därefter. Du ska därför:

- inte avslöja ditt lösenord för andra eller låna ut din behörighet.
- skydda lösenordet väl. (Vilket bl.a. innebär att du absolut inte får ha lösenordet uppskrivet på en lapp som du förvarar under tangentbordet, skrivbordsunderlägget eller i skrivbordslådan!)
- omedelbart byta lösenordet om du misstänker att någon känner till det.
- byta lösenordet var 90:e dag. (Du får en uppmaning när det är dags att byta.)

Lösenordet ska bestå av minst 6 tecken

och ska helst vara en blandning av bokstäver och siffror. Det får inte konstrueras så att det lätt kan kopplas till dig som person. Enkla upprepade mönster såsom t ex ”ABC123”, ”AAAAA2” får inte användas. Inte heller andra lättforcerade lösenord, t.ex. eget, familjemedlems eller husdjurs namn, eller lösenord bestående av enkla tangentkombinationer t.ex. ”QWERTY”. (De sex första tecknen på tangentbordets näst översta rad.) Inloggningssystemet tillåter inte heller att tecknen å ä ö eller att delar av ditt för eller efternamn ingår i lösenordet.

För att skapa ett bra lösenord kan du t.ex.:

- välja en uttalbar, men meningslös sekvens, till exempel BAMROK
- välja ett välbekant ord t.ex. ”fönster” och skapa ditt lösenord med hjälp av tangenterna ovanför bokstäverna i ordet fönster dvs. RPHW534.
- ta första (andra/tredje/sista) bokstaven i en för dig bekant textsträng, boktitel eller melodi, till exempel FVDDFM från ”Främling vad döljer du för mig...”.

Tidigare använda lösenord

kan du inte återanvända. När du byter lösenord kontrollerar systemet att du inte väljer ett lösenord som du använt tidigare.

Om du glömmer ditt lösenord

och försöker att logga in i nätverket med ett felaktigt lösenord kommer systemet att låsas efter tio felaktiga försök. Om detta inträffar kan du vända dig till IT-avdelningens supportpersonal (tel. 88 53 00), uppge vem du är och be om ett nytt initialt lösenord. Om de är osäkra på din identitet är de skyldiga att göra en motringning alternativt tala med din chef för att förvissa sig om att ingen obehörig försöker skaffa sig tillträde till din dator.

Du lämnar spår efter dig

när du är inloggad och arbetar i systemen. Systemens loggningsfunktion används bl.a. för att spåra obehöriga intrång. Detta görs för att skydda informationen och för att undvika att oskyldiga misstänks om oegentligheter inträffar.

Om du byter arbetsuppgifter

måste din verksamhetschef meddela det till IT-avdelningens support så att din behörighet kan ändras.

Om du slutar din anställning

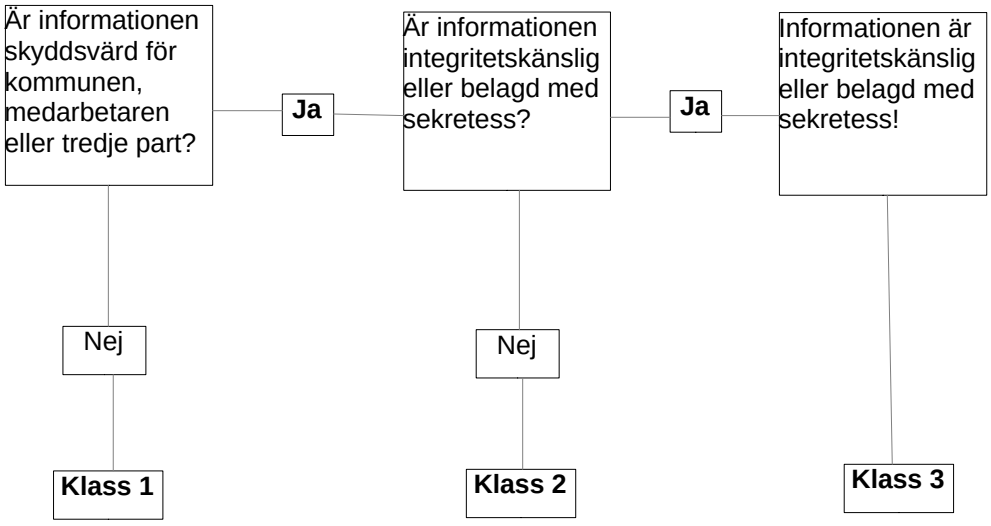
i kommunen låses ditt konto och du kan inte längre logga in. Tre månader senare raderas ditt kontot, din e-post och dina filer. Innan du slutar måste du tillsammans med din chef avgöra vilken information som måste föras över till andra medarbetare innan kontona raderas.

3 HANTERING AV INFORMATION

I kommunen finns information av en mängd olika slag där det bl.a. ställs olika krav på sekretess, riktighet mm. För att minimera risken för att känslig information hamnar hos obehöriga finns riktlinjer för hur information får hanteras. Riktlinjerna är framtagna för att vara ett redskap vid klassificering av kommunens information vad gäller dess skyddsvärde.

Klassificeringen delar in informationen i tre olika informationsklasser där den minst känsliga informationen finns i klass 1 och den mest känsliga informationen i klass 3. Klasserna beskriver hur informationen får hanteras och var den får lagras. Det måste poängteras att riktlinjerna inte säger något om hur informationen får publiceras eller om den utgör allmän offentlig handling.
Behandling av information som innehåller personuppgifter ska alltid anmälas till förvaltningens personuppgiftsombud.

3.1 Informationsklassning



Klass 1
Hit räknas information som kan spridas till en obestämd krets utan risk för några negativa konsekvenser. Informationen får lagras på kommunens servrar, datorns lokala hårddisk, molntjänst eller annan lagringsplats. Informationen får även lagras på USB-minnen eller andra flyttbara media utan restriktioner. Informationen får överföras elektroniskt utan kryptering, till exempel via e-post, såväl internt som externt.

Klass 2
Skyddsvärdet
Hit räknas intern information som inte kan spridas till en obestämd krets men inte heller är integritetskänslig eller belagd med sekretess.

Informationen ska alltid lagras på eller regelbundet kopieras till en central server. Informationen får inte enbart lagras på datorns lokala hårddisk eller flyttbara media. Informationen får överföras elektroniskt utan kryptering. När informationen lagras på lokal hårddisk, flyttbara media, mobiltelefoner eller surfplattor ansvarar den anställde själv för att vidta nödvändiga skyddsåtgärder så att inte informationen kommer på avvägar.

Klass 3
Skyddsvärdet
Hit räknas till exempel all integritetskänslig och sekretessbelagd information. Likaså all information som omfattas av Patient Data Lagen (PDL), lag om behandling av personuppgifter inom socialtjänsten eller som klassas som integritetskänslig i enlighet med Person Uppgifts Lagen (PUL). Informationen ska normalt enbart lagras på centrala servrar och inte på datorns lokala hårddisk eller flyttbara media. Informationen får i undantagsfall lagras på bärbar dator och flyttbart media under förutsättning att informationen krypteras samt att mediat hålls inlåst när det inte används. Dessa media får inte lämnas utan uppsikt och inte förflyttas utanför kommunens lokaler såvida det inte skickas till annan behörig mottagare. All överföring av informationen måste vara krypterad.

Du är skyldig att känna till och att hantera informationen utifrån denna klassifikation. Observera att nätverkets servrar är omgärdade med stränga säkerhetsregler och informationen säkerhetskopieras varje dygn. Väljer Du att lagra klass 1 information på den lokala arbetsstationen, USB-minnen etc. är det Du själv som ansvarar för informationens säkerhet och att den blir säkerhetskopierad. IT-avdelningen hjälper inte till med att återskapa förlorad information på t.ex. lokala hårddiskar och USB-minnen. Mer upplysning om informationsklassning finns i den generella säkerhetsinstruktionen.

4 INTERNET

Kommunens nätverk är anslutet till Internet via en brandvägg som reglerar in- och utgående trafik. I brandväggen sker också en registrering av vilka sidor användarna besöker på Internet. Den informationen är till för att kunna spåra brott mot gällande lagar och säkerhetsregler och för att upptäcka intrångsförsök.

När du surfar på Internet representerar du kommunen. Agera i enlighet med våra värderingar och policy så att det du förmedlar på nätet inte skadar kommunen. Tänk på att du lämnar spår efter dig t.ex. i form av kommunens adress. Brandväggen har även en möjlighet att filtrera bort kategorier av webb-sidor som bedömts som olämpliga att besöka t.ex. sidor med pornografiskt innehåll. Försöker du komma till en sådan sida får du ett meddelande om att du är på väg till en ”otillåten webbsida”. Trots att den klassas som olämplig kan det finnas goda yrkesmässiga skäl för dig att besöka sidan. Du kan då gå vidare till den aktuella sidan men var medveten om att all information loggas.

Utöver dessa säkerhetsregler finns det också lagar och riktlinjer som du är skyldig att känna till när du använder kommunens datorer. Du bör därför också ta del av dokumentet ”*Riktlinjer för ärendehantering, e-post och Internet.”* (KS 2010/0067)

Ett av de största hoten mot vår information är

datavirus och andra former av skadlig kod och det vanligaste sättet att få in skadlig kod i datorn är via Internet. Internetanvändandet är ett område där säkerheten i mycket hög grad avgörs av användarnas beteende. **Vid användande av Internet gäller därför följande:**

- att du ska ha ett gott omdöme och endast besöker de sidor som är relevanta för ditt arbete.
- Inga program får laddas ner i kommunens datorer och nätverk av enskilda användare. På vissa hemsidor kan du ibland bli uppmanad att ladda ner ett program. Acceptera aldrig detta! De kan innehålla skadlig kod t.ex. spionprogram, (spyware), som gör samma skada som ett datavirus. Saknar du något program som du behöver i ditt arbete, ber vi att du vänder dig till IT-avdelningens

support som bedömer om programmet kan installeras i nätverket. Om programmet medför licenskostnader måste också din chef fatta ett beslut om inköp av programmet.

Tecken på datavirus eller annan skadlig kod kan t.ex. vara att

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

Om du misstänker att datorn innehåller virus ska du

- stäng av datorn och koppla ur nätverkskabeln.
- se till att ingen annan använder datorn.
- omedelbart anmäla det som skett till IT-avdelningens support.

5 E-POST

E-post är ett bra hjälpmedel i arbetet. Med tiden sparar du kanske på dig stora mängder meddelanden som dessutom innehåller bifogade filer. Dessa tar en hel del plats på nätverkets servrar. Tänk därför på att regelbundet gallra och radera i din inkorg och utkorg! Regler för vad som kan gallras och vad som ska diarieföras mm finner du i dokumentet ”Riktlinjer för ärendehantering, e-post och Internet.” (KS 2012/00452)

För att förhindra spridning av känslig information och för att minska risken för virusspridning samt för att undvika onödig belastning av nätverkets resurser gäller följande:

- Känslig och/eller sekretessbelagd information får inte skickas till adresser utanför nätverket.
- Av samma skäl är det inte tillåtet med automatisk vidarekoppling av e-post till adresser utanför nätverket.
- Var återhållsam med att skicka eller vidarebefordra meddelanden som innehåller stora filer.
- Var försiktig med att öppna e-post från avsändare du inte känner igen eller har en relation till.
- Vidarebefordra inte meddelanden av typen virusvarningar, insamlingar, kedjebrev etc. till andra användare i nätverket.
- Undvik att göra utskick till stora grupper. Istället rekommenderas att använda kommunens intranät för information till större grupper.

6 SÄKERHETSINCIDENTER

Om du misstänker att någon obehörig använt din användaridentitet och varit inne i systemet ska du:

- notera tidpunkt då du senast själv var användare i systemet
- notera tidpunkt då du upptäckte förhållandet
- anmäl omedelbart till IT-avdelningens support och din chef
- dokumentera alla iakttagelser i samband med upptäckten samt försök att fastställa om kvaliteten på informationen har påverkats.

Om din IT-utrustning blir stulen eller har kommit bort.

- Meddela din närmaste chef som avgör om stöden skall polisanmälas. Kontakta också IT-avdelningens support och meddela vilken utrustning som kommit bort. Om det är en smart mobiltelefon eller en surfplatta kan IT-avdelningen hjälpa dig att radera informationen och spåra enheten.

7 BÄRBARA DATORER, MOBILTELEFONER, SURFPLATTOR OCH ANDRA EXTERNA LAGRINGSMEDIA

Bärbara datorer, smarta mobiltelefoner, surfplattor och andra portabla lagringsmedia utgör alltid en säkerhetsrisk och är dessutom ofta mycket stöldbegärliga.

Därför ska du:

- hålla utrustningen under uppsikt om du inte kan låsa in den.
- om möjligt undvika att lagra verksamhetskritisk information på den.
- omedelbart anmäla stöld eller förlust till IT-avdelningen.
- logga in på datorn med användarnamn och lösenord
- aktivera pinkod eller annat inloggningsskydd på surfplattor och smarta mobiltelefoner.

Ytterligare säkerhetsåtgärder kan bli aktuella beroende på vilken information som finns på lagringsmediet (se kap 3 informationsklassning).

8 ARBETSPLATSEN

Om du lämnar arbetsplatsen

ska du använda skärmsläckaren alternativt logga ut, även om det bara är för en kortare stund. Glömmer du det finns det risk för att informationen är tillgänglig för obehöriga. Kom ihåg att du ansvarar för allt som registrerats med din användaridentitet.

Utskrifter av dokument

Används gemensamma skrivare bör dessa vara utrustade med teknik för säkerhetskod eller kort. På det sättet förhindras att dokument hamnar i orätta händer.

Service på utrustning

Om du har problem med din dator ska du kontakta IT-avdelningens support som avgör hur felet ska hanteras. Behöver din dator lämnas på service måste du se till att eventuell känslig information avlägsnas från hårddisken.

För att lösa vissa datorproblem kan IT-supporten behöva ta över och fjärrstyra din dator. Detta får bara ske om du godkänt denna åtgärd. När du själv inte är inloggad har dock systemteknikerna rätt att, utan ditt godkännande, fjärrstyra datorn i samband med nödvändigt tekniskt underhåll.

Känner du inte igen den servicepersonal som kommer till dig för att åtgärda ett datorproblem ska du kräva att få se dennes legitimation. Det går också bra att kontrollera med IT-avdelningen att personalen är behörig.

Att arbeta hemifrån

Har du tillgång till Internet kan du komma åt kommunens webbtjänster från hemmet eller annan plats. Tänk bara på att du inte bör spara verksamhetsrelaterad information på privata datorer (se kap 3 informationsklassning).

Det är din närmaste chef som bestämmer om du ska distansarbeta och i vilken omfattning. Personalavdelningen har utarbetat särskilda riktlinjer för distansarbete som beskriver vilka regler som gäller i samband med detta. För att få tillgång till vissa system krävs en inloggning med engångslösenord via SMS. Den tjänsten kan beställas hos IT-avdelningen.

Stöd och hjälp

Om du distansarbetar är du givetvis välkommen att höra av dig till IT-avdelningens support om du behöver hjälp eller har några frågor.

Ytterligare information

hittar du i:

- **Kommunens IT-säkerhetsplan**
  Säkerhetsplanen anger mål och ansvarsfördelning inom IT-säkerhetsområdet.
- **Generell systemsäkerhetsplan för Falköpings kommun**
  Systemsäkerhetsplanen anger vilka säkerhetsnivåer som ska gälla.
- **Generell säkerhetsinstruktion för Falköpings kommuns nätverk.**
  Den generella säkerhetsinstruktionen innehåller en komplett beskrivning av gällande säkerhetsregler samt när eventuella undantag kan göras från regelverket. Därför rekommenderar vi att du läser den om du vill ha mer fördjupade kunskaper om vilka säkerhetsregler som gäller.