IT-Säkerhetsinstruktion: Användare

HÄLLEFORS KOMMUN
Postadress
IT-enheten
712 83 Hällefors

E-post
kommun@hellefors.se
Besöksadress
Sikforsvägen 15
Hällefors

Telefon
0591-641 00 vx

Organisationsnr
212000-1942
Fax
0591-109 76

Bankgiro
193-8950

PlusGiro
11808-3

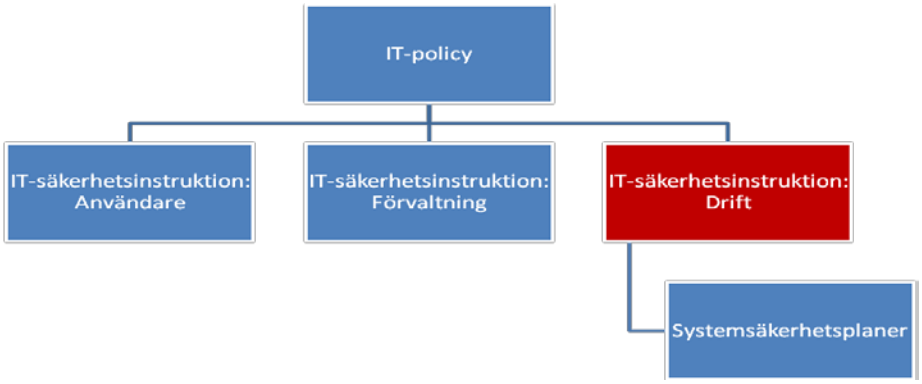
Innehåll

1 Målsättning

IT-säkerhetsinstruktion Användare roll i IT-säkerhetsarbetet
IT-säkerhet är en del i Hällefors kommuns lednings- och kvalitetsprocess som ska bidra till att ett IT-system kan användas på avsett sätt och med avsedd funktionalitet. Krisberedskaps-myndighetens rekommendationer om basnivå för IT-säkerhet (BITS) ska gälla som ramverk för IT-säkerhetsarbetet.
BITS – den säkerhetsnivå, som minst måste uppnås för ett IT-system, som bedöms nödvändigt, för att upprätthålla en viss verksamhets basförmåga.

2 Syfte

Styrande dokument för IT-säkerhetsarbetet är IT-policyn samt IT-säkerhetsinstruktionerna: Förvaltning, Drift och Användare. IT-säkerhetsinstruktionerna är en konkretisering av IT-policyn. Krav på och åtgärder för ett enskilt IT-system ska dokumenteras i en systemsäkerhetsplan. En sådan ska upprättas för de IT-system som bedöms som viktiga för verksamheten.



IT-policyn fastställs av kommunfullmäktige och IT-säkerhetsinstruktioner fastställs av kommunstyrelsen. IT-policyn redovisar ledningens viljeinriktning och mål för IT-säkerhetsarbetet och syftar till att klarlägga:

- Organisation och roller för IT-säkerhetsarbetet.
- Krav på riktlinjer för områden av särskild betydelse.

IT-säkerhetsinstruktion Förvaltning redovisar:

- Det ansvar som ingår i de olika rollerna.
- De riktlinjer som gäller för områden av särskild betydelse.

IT-säkerhetsinstruktion Drift redovisar:

- Organisation och ansvar för drift av IT-systemen.
- Regler och rutiner för vissa områden.
- Regler för systemutveckling, systemunderhåll, incidenthantering.
- Regler för säkerhetskopiering, lagring, driftadministration och kontinuitetsplanering.

IT-säkerhetsinstruktion Användare (detta dokument) syftar till att ge kunskaper och riktlinjer om hur man på ett säkert sätt använder IT-

stöden. Dokumentet skall också ligga till grund för framtagande och revidering av Systemsäkerhetsplanerna.

Uppslagsverk

Se gärna detta dokument IT-säkerhetsinstruktion som ett uppslagsverk och en viktig källa om hur IT-systemen och informationen får användas. Saknas någon information eller är felaktig, kontakta IT-samordnaren eller närmaste chef.

Allmänt

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 användarna känner till de krav som ställs på dem som anställda inom Hällefors kommun.

Användarna måste veta:

- Vilket ansvar de har.
- Vad de ska göra vid olika incidenter.
- Var de kan få stöd och hjälp.
- De allmänna säkerhetsbestämmelserna.
- Hur de får nyttja e-post och Internet.

Mål

Målet är att alla användare skall:

- Ansvara för informationens riktighet och att den skyddas mot obehörig insyn vid såväl inmatning, uttag och bearbetning av information.
- Rapportera fel och brister.
- Framföra behov av information och utbildning till systemadministratör.
- Föreslå utvecklande förändringar av IT-systemen.
- Meddela systemadministratör behovet av skydd för känslig information.
- Förstå IT-systemets struktur och rollfördelning inom organisationen.
- Förstå begränsningar och risker i användandet av e-post och Internet.

3 Ansvarsfördelning

Organisation och roller

Det övergripande ansvaret för Hällefors kommuns IT-system vilar på kommunchefen. Kommunchefen utser systemägare för respektive förvaltnings IT-system.

Hällefors kommun eftersträvar att ansvaret för IT-systemen skall följa linjeorganisationen för varje enskilt IT-system.

Systemägare - 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 verksamheten bästa sätt. Systemägaren beslutar om nyanskaffning, vidareutveckling eller avveckling av IT-system inom ramen för resurstilldelningen för sin verksamhet.

Operativt ansvarig (systemförvaltare) - Operativt ansvariga utses av systemägarna och är de personer som har ansvaret för den dagliga användningen av IT-systemet. Operativt ansvarig samverkar med IT-avdelningens systemadministratör för att säkerställa en säker och rationell drift av systemet.

IT-ansvarig - är systemägare inom området teknisk infrastruktur och har det övergripande ansvaret för att ett systems tekniska delar fungerar. IT-ansvarig samverkar med systemägare vad avser drift och resurstilldelning för ett IT-system.

Systemadministratören – kan tillhöra IT-enheten, innehar den tekniska kompetensen och ansvarar tillsammans med operativt ansvarig för att den dagliga driften upprätthålls enligt överenskommelse mellan systemägaren och IT-ansvarig.

Användaren - Användarna skall godkänna och följa gällande regler som dokumentet" Regler och riktlinjer för användare" anger. I detta ingår att noga ta del av och följa de säkerhetsregler som finns för de IT-system som den enskilde använder

- **IT-säkerhetssamordnaren** - understödjer arbetet med att uppnå IT-policyns mål och är ansvarig för att samordna IT-säkerhetsarbetet inom Hällefors kommun. Samordnaren är i IT-säkerhetsfrågor direkt underställd kommunchefen.
- **IT-säkerhetsledning** - Vid större oplanerade IT-relaterade händelser tillämpas Hällefors kommuns krisledningsplan.

Styrgrupper - Systemägaren utser vid behov en styrgrupp för sina IT-system. Styrgruppen fungerar som en rådgivande och stödjande funktion till systemägaren i diverse frågor som rör systemförvaltningen och håller sig informerade om huruvida systemet stödjer verksamheten.

4 Information klassning och lagring

Allmänt

I sitt dagliga arbete kommer användarna i kontakt med information som kommer levererad i många olika former. Det kan vara talad, på papper, lagrad i datorer via e-post m.m. För att användarna ska få den information de behöver, vid rätt tidpunkt och med korrekt innehåll har Hällefors kommun satt upp som övergripande mål för informationssäkerhetsarbetet att vi skall

- Behandla information på ett tydligt, korrekt, säkert och för sakfrågan relevant sätt.
- Kunna leverera och hämta information vid rätt tidpunkt.

- Uppnå och upprätthålla en god informationssäkerhet.

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

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

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

Hällefors kommun har idag inget dokumenthanteringssystem som stödjer ovanstående klassning, men man ska ha klassningen i åtanke när man arbetar med dokument.

Handling som är hemlig
Sekretessen för data som avser rikets säkerhet kan inte klassas enligt ovanstående modell. Hur sådana dokument skall hanteras måste beslutas från fall till fall.

Handlingar kan vara allmänna eller icke allmänna. Allmänna handlingar kan sedan vara offentliga eller hemliga . Alla allmänna handlingar måste registreras, arkiveras och diarieföras.

Det gäller även handlingar som inkommer via telefax eller e-post mm. Hur man ska hantera dessa handlingar framgår av dokumentet IT-säkerhetsinstruktion: E-post.
Huvudregeln är att allmänna handlingar är tillgängliga för alla som vill ta del av dem. En myndighet som vägrar lämna ut en allmän handling kan endast göra så med stöd av ett lagrum i sekretesslagen.
Sekretessen för data som avser rikets säkerhet skall hanteras enligt särskild instruktion. Om det råder tveksamhet skall närmaste chef eller säkerhetschefen kontaktas.

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

Om en medarbetare behöver upprätta särskilda register bör man samråda med sin närmaste chef i ett tidigt stadium i planeringen av registret.

Lagring av information
Allt arbetsmateriel 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 Hällefors kommun och dess verksamheter olika IT-baserade stödsystem bl.a. ekonomi- och lönesystem. 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 som skall och får tillföra, ändra och eventuellt tas bort (gallra). Om reglerna följs har vi goda möjligheter att klara kraven på en god informationssäkerhet i systemen
- Egna register/dokument
  Utöver att arbeta i våra stödsystem kommer användarna upprätta egna register, handlingar och dokument, exempelvis med Word eller Excel. Stödsystemens ”inbyggda skydd” används inte då. Detta kräver särskild uppmärksamhet. Det är viktigt att man tänker över säkerheten och hur man lagrar, klassar och hanterar informationen.

Oavsett om man använder stödsystem eller har skapat egna dokument så har användarna ett personligt ansvar för säkerheten i sin hantering av information i alla dess former. I detta ansvar ingår bl.a. att användarna själva måste känna till de regler som gäller när de hanterar information. När man hanterar information är man personligen ansvarig för informationens riktighet och att informationen skyddas mot obehörig insyn. Tveka inte att samråda med närmaste chef om det råder osäkerhet i dessa sammanhang.

När man skapar **egen** information är det viktigt att veta:

- Vilken informationsklass informationen tillhör. (se klassning sid 6 ovan)
- Var den ska lagras.

Rutiner finns för hantering av informationstillgångar i både fysisk och elektronisk form. För varje informationsklass gäller hanteringsrutiner för:

- Lagring.
- Kopiering.

- Elektronisk överföring. (fax, e-post, telefon etc.)
- Fysisk överföring. (papper, film etc.)
- Makulering. (se Arkivreglemente)
- Arkivering. (se Arkivreglemente)

Hanteringsrutiner för information på papper, film etc. – tabell.

	Basnivå	Hög nivå	Mycket hög nivå
Förvaring	Inlåst	Under direkt uppsikt	Under direkt uppsikt eller inlåst
Kopiering för annan person	Fri kopiering för personal med tillgång till handlingen	Kräver godkännande från innehavaren av originalet	Kräver godkännande från innehavaren av originalet
Distribution internt	Inga särskilda krav	Igenklistrat kuvert	Igenklistrat kuvert
Distribution externt	Inga särskilda krav	Normal försändelse	Ess-brev REK
Distribution via fax	Inga särskilda krav	Mottagaren uppringd. Bevakad mottagning	Krypterad överföring. Mottagaren uppringd. Bevakad mottagning
Makulering	Inga särskilda krav	Förstörs i papperstugg	Utfärdaren ska själv förstöra i papperstugg
Arkivering			

När information lagras elektroniskt finns större risk för obehörig förändring eller spridning, dessutom tillkommer risken för virusangrepp. Därav de högre kraven på denna typ av information.

Elektronisk lagring av information.

	Basnivå	Hög nivå	Mycket hög nivå
Lagring			
Diskett, fast eller lös hårddisk	Inlåst	Inlåst och krypterad	Inlåst och krypteras
Backup-media	Inlåst	Inlåst i brandklassat utrymmer skilt från server eller datorrum	Inlåst i brandklassat utrymmer skilt från server eller datorrum
Bärbar persondator med hårddisk	Inloggningsskydd	Inloggningsskydd och kryptering	Inloggningsskydd och kryptering
Destruktion av diskett, hårddisk etc	Diskett klipps itu. Andra media lämnas till IT-drift	Lämnas till IT-drift	Lämnas till IT-drift
Återanvändning av diskett, hårddisk etc	Är tillåten	Är tillåten efter total radering enligt IT-drifts rekommendation	Är tillåten efter total radering enligt IT-drifts rekommendation
Gemensam dator, t ex server i nätverk	Behörighetskontrollsystem och inlåst datorrum med tillträdesskydd	Behörighetskontrollsystem och inlåst datorrum med tillträdesskydd	Behörighetskontrollsystem och inlåst datorrum med tillträdesskydd
Kommunikation			
Inom organisationen nät (LAN)	Kan överföras öppet i nätverket	Säker överföring enligt Datainspektionens rekommendationer	Säker överföring enligt Datainspektionens rekommendationer
Externt via organisationens WAN	Kan överföras öppet i nätverket	Säker överföring enligt Datainspektionens rekommendationer	Säker överföring enligt Datainspektionens rekommendationer
Uppkopplad förbindelse till organisationen utifrån	Säker överföring enligt Datainspektionens rekommendationer. Särskilt avtal krävs	Säker överföring enligt Datainspektionens rekommendationer. Särskilt avtal krävs	Säker överföring enligt Datainspektionens rekommendationer. Särskilt avtal krävs

Den information som lagrar på våra gemensamma utrymmen och kan nås via nätet, säkerhetskopieras automatiskt. Man kan välja att lagra på enheterna, H: eller G:.

- H: (Personlig hemkatalog) är den personliga enhet som används för lagring av personligt arbetsmaterial. Om man väljer H-enheten kommer medarbetarna ej åt informationen.
- G: (Organisationsenhet) är en enhet för lagring av information som alla medarbetare på organisationen har tillgång till.
- I förekommande fall kan också ytterligare enhetsbeteckningar finnas.

Om användaren lagrar på sin lokala hårddisk **(C:)** är han/hon personligen ansvarig för att säkerhetskopiering sker, t ex på USB-minne eller CD. När man lagrar information på sin lokala hårddisk **(C:)** riskerar man att förlora information som inte kan återskapas till rimliga kostnader, vid t ex en diskkrasch, undvik därför lagring på **C:.**

Behörighet

IT-systemen är utrustade med behörighetskontrollsystem för att säkerställa att endast behöriga användare kommer åt information. De behörigheter man blir tilldelad beror på arbetsuppgiften och avgörs av närmaste chef. Vikarier och tillfällig personal som tilldelas behörigheter skall ha en tidsbegränsning inlagd i systemen som motsvarar anställningstiden.

Lösenord

Första gången man loggar in får man ett initialt lösenord av IT-enheten. Detta lösenord måste bytas till ett personligt vid första inloggningen för att komma in i nätverket. Denna rutin ska även gälla för övriga system. Lösenordet är strängt personligt och skall hanteras därefter. Man skall tänka på att användaren själv kan bli misstänkt om någon annan användare använder lösenordet för olämpliga ändamål.

Användaren skall därför:

- Inte avslöja sitt lösenord för andra eller låna ut sin behörighet
- Skydda lösenordet väl.
- Omedelbart byta lösenord om man misstänker att någon känner till det.
- Byta lösenordet var 47:e dag. I nätverket kommer det upp en ruta på skärmen när det är dags att byta. (olika system kan ha olika lång tid mellan bytena)

Användare skall även byta lösenord i de IT-system som du är behörig till i nätverket. I dessa ges dock oftast ingen påminnelse. Byt därför gärna lösenord på de IT-systemen samtidigt.

Lösenordet skall bestå av minst 7 tecken vara minst ett stort tecken och en siffra. Det skall konstrueras så att det inte lätt kan kopplas till användaren. 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.

Viktigast av allt är dock att välja ett lösenord som är lätt att komma ihåg.

Om man glömmer sitt lösenord och försöker logga in till systemet med ett felaktigt sådant, kommer systemet att låsas efter fem felaktiga försök. Om detta inträffar ska man vända sig till systemadministratören eller till IT-enheten. Man kommer då att få ett nytt initialt lösenord.

5 IT-säkerhet och kringutrustning

Allmänt

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

- Mjukvara (program) som inte godkänts av IT-enheten 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 man är i behov av ytterligare programvaror eller hårdvara t.ex. handdator, digitala kameror m.m. skall detta anmälas till närmaste chef.
- All installation och konfiguration av hårdvara och arbetsstationer ska ske av IT-enheten så att kommunens standard följs.
- Vid tillfällen när man inte har uppsikt över arbetsstationen kan man tillfälligt låsa arbetsstationen med kortkommandot**: CTRL+ALT+DEL**. Vid längre frånvaro skall arbetsstationen loggas ur.
- Vid arbetsdagen slut skall datorn stängas av.
- Vid fel på arbetsstation med tillhörande hårdvara skall man omgående anmäla detta till systemadministratören eller IT-enheten.
- Arbetsstation med tillhörande hårdvara är verksamhetens egendom och får ej bytas, förändras eller medtagas utan verksamhetschefens eller IT-ansvarigs medgivande.
- Inför service på utrustning som innebär att persondatorn lämnas bort eller kasseras måste känslig information på hårddisken tas bort (om sådan finns). Rådgör då med systemadministratören eller IT-enheten.

Bärbara - och hemdatorer

Om användaren har en egen bärbar- eller hemdator som används för distansarbete, tänka på att dessa kan utgöra en säkerhetsrisk och skall därför bara ske om särskilda skäl föreligger .

Tänk på att:

- Inte kopiera känslig information till CD / USB-minne som sedan tas med hem. Risk finns att obehöriga då kan ta del av den.
- Att man inte får lagra sekretessbelagd eller för verksamheten känslig information på den egna datorn.
- Lagringsmedia som används/skapas i hemdatormiljö på ext. disk, USB-minne m.m. får inte användas i kommunens nätverk förrän viruskontroll av lagringsmediet har skett. Kontrollen

sker mot ett uppdaterat program i av kommunen anvisad utrustning.

Kringutrustning med mellanlagringsmöjlighet
Plattor, handdatorer, digitala kameror, mobiltelefoner m.m. kan lätt bli virusbärare då man kan mellanlagra information mellan olika datorer i dessa. Därför skall man inte ansluta denna typ av kringutrustning mot en dator som man inte med säkerhet vet har ett uppdaterat virusprogram. All kringutrustning skall vara godkänd och installerad av IT-enheten.

Vårt lokala nätverk (LAN)
Nätverket är en mycket viktig gemensam resurs som ger alla möjlighet 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 på nätverket skall ske med användarens personliga lösenord.
- All inloggning eller försök till inloggning under annan, eller med annans identitet är absolut förbjuden.
- När användaren arbetar i kommunens nätverk loggas och registreras i allmänhet olika aktiviteter. Loggningsfunktioner används för att spåra obehörig verksamhet och intrång.

Detta görs:

- För att skydda informationen samt för att undvika att oskyldiga misstänks om oegentligheter inträffar.
- Information som sparas på gemensamma utrymmen i det lokala nätverket, skall lagras på anvisad plats.
- Det är absolut förbjudet att ansluta sig externt via egen icke godkänd uppkoppling t.ex. VPN, http m.m.
- Det är förbjudet att skaffa sig utökade systemrättigheter än det som tilldelats (hacking).

Om alla följer dessa regler så kan obehöriga inte komma åt informationen. Kom ihåg att användaren ansvarar för allt som registrerats med sin användaridentitet.

6 Internet och e-post

Internet
När man använder Internet kan säkerheten i kommunen lokala nätverk påverkas i mycket hög grad beroende på användarnas beteende.

Hällefors kommun förutsätter att den som laddar ned filer från Internet 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. Om en speciell programvara måste laddas ner från nätet och installeras skall detta ske av IT-enheten.

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.

När användare surfar på Internet representerar de vår kommun. Detta skall göras med ett gott omdöme så att agerandet på nätet inte skadar Hällefors kommun. Agerandet skall vara i enlighet med kommunens värderingar så att det som förmedlar på nätet inte skadar kommunen. Man bör tänka på att det lämnar spår i en fil som loggar Internettrafiken på organisationen. Denna loggfil är **offentlig handling** och visar vilka webbplatser användaren har besökt.

IT-hjälpmedlen är ett arbetsverktyg och skall således användas för arbetsrelaterade ärenden och bör inte utnyttjas för privat bruk. Missbruk av ett arbetsverktyg kan medföra disciplinära åtgärder.

E-post
E-post är ett rationellt hjälpmedel i arbetet men minneskapaciteten för det är begränsad. Därför skall mapparna ”Inkorgen”, ”Skickat”, och ”Borttaget” raderas för att frigöra utrymme så att inte e-post konton spärras. E-postsystemet skall inte användas som ett arkivsystem, meddelanden, bifogade filer m.m. som skall sparas görs på samma sätt som när annan information lagras.

Om användare under en längre period inte har möjlighet att kontrollera sin e-post skall han/hon sätta frånvarobesked med uppgift om vem som hanterar ”sina” ärenden.

Man skall vara extra uppmärksam då e-post används. 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 användare misstänker att det kommit in virus via e-postsystemet ska man agera som beskrivits i avsnittet om Incidenter.

Utformning
- Användare skall följa de råd om inställningar i och hantering av e-postsystemet som sägs av IT-enheten.
- Det är inte tillåtet med automatisk vidarekoppling till annan e-postadress om detta inte godkänns av IT-enheten.
- ämne skall alltid anges för meddelandet för att klargöra för mottagaren vad denne kan förvänta sig för innehåll i e-brevet.
- Känslig information skall inte skrivas i ämnesraden.
- Sekretessbelagd information skall **aldrig** bifogas i e-post (den kan lätt vidarebefordras!)

- Användare bör vara selektiv med att använda stora gruppadresser (massutskick) och med att skicka eller vidarebefordra meddelanden som innehåller stora filer.
- Skicka inte och vidarebefordra inte kedjebrev av någon sort.
- Sprid inte e-postadress till mindre seriösa ställen.
- Stryk dig från e-postlistor om du inte vill ha fler brev via dem eller är frånvarande en längre tid
- Om användare får hotelsebrev eller liknande, kontakta närmaste din chef. Ta inte bort brevet.

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

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

7 Incidenter, virus, stöld mm

Allmänt
Hällefors kommun bidrar till att öka IT-säkerheten i landet genom att löpande rapportera alla typer av IT –incidenter till PTS. Genom att rapportera händelser hjälper du till att förebygga. Informera IT-säkerhetssamordnaren som sammanställer rapporterna.

Obehörigt intrång
Om en användare misstänker att någon obehörig använt någon annans användaridentitet och varit inne i IT-systemet skall användaren:

- Notera när han/hon senast var inne i IT-systemet.
- Notera när han/hon upptäckte intrånget.
- Omedelbart anmäla till IT-säkerhetssamordnaren alternativt till systemansvarig, eller närmaste chef.
- Dokumentera alla iakttagelser i samband med upptäckten och försöka att fastställa om kvaliteten på den aktuella informationen har påverkats.

Stöld
Om ett inbrott har skett eller utrustning försvinner på annat sätt skall detta rapporteras till IT-säkerhetssamordnaren och till närmaste chef. Som i sin tur bedömer om en polisanmälan skall göras. En bedömning med utgångspunkt från ev. stulen information skall också göras. Om sekretesskyddad information eller information som kan skada Hällefors kommun eller tredje part bedöms finns med. Om så är fallet skall detta rapporteras till systemägaren som vidtar lämplig åtgärd.

Virus m.m.
Virus m.m. är ofta ytterst smittsamma och ”smittkällan” kan vara svår att identifiera. Gratisprogram, spelprogram och filer som laddas ner från Internet eller medföljande filer till e-post är de vanligaste smittbärarna.

Hällefors kommun har bra programvaror för viruskontroll och det görs kontroll i realtid vid aktiviteter i nätverket. Även e-post 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 initierat det t.ex. förändringar sker på skärmen (tecken flyttas, försvinner etc.) eller onormal aktivitet på hårddisken.
- Program uppförs sig onormalt.
- Datorn uppträder på ett onormalt sätt, t.ex. arbetar mycket långsamt.

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

- INTE stänga sin dator genom att slå av strömmen utan istället dra ur nätverkskabeln.
- Omedelbart anmäla förhållandet till endera IT-säkerhetssamordnaren, IT-enheten eller till närmaste chef. OBS! Anmälan ska ske per telefon eller besök, EJ per e-post.

Om man får brev med virusvarning där avsändaren talar om att ett virus är på gång skall man inte skicka meddelande om detta till alla på organisationen utan kontakta IT-enheten som kan avgöra om det är en seriös varning eller i sig självt ett virus. Man ska inte heller skicka någon varning externt innan man har kontrollerat med IT-enheten. Användare skall aldrig på begäran via e-post lämna ut kontouppgifter, lösenord eller annan information som kan ge tillträde till olika tjänster eller resurser. Sådan information skall alltid lämnas ut muntligt eller skriftligt på papper. Detta för att förebygga sk. ”fishing”.

8 Övrigt

Om användare misstänker stöld, brand, sabotage och dylikt, skall säkerhetschefen, IT-säkerhetssamordnaren eller närmaste chef kontaktas.

Om fel och brister upptäcks i de system som används skall detta rapporteras till IT-enheten, närmaste chef eller IT-säkerhetssamordnaren.

Hällefors kommun bidrar till att öka IT-säkerheten i landet genom att löpande rapportera alla typer av IT –incidenter till Post- och Telestyrelsen (PTS). Genom att rapportera händelser hjälper vi till att förebygga. IT-säkerhetssamordnaren skall informeras som sammanställer rapporterna.

Stöd och hjälp
För att få kunskap om vilka enheter som används, hur man lägger in skärmsläckare med lösenord etc. kan användarna få stöd och hjälp av IT-enheten, som hjälper till med inloggnings- problem och programvaror.

När användare slutar sin anställning
Ansvarar användaren för att:

- Rådgöra med sin chef om vilket av sitt arbetsmaterial som skall sparas. Notera att allt arbetsmaterial som framställts anses vara kommunens egendom och får inte tas med utan chefs godkännande.
- Privat material rensas och tas bort.

De behörigheter användaren fått i våra IT-system avbeställs genom ansvarig chefs försorg.
För detta finns blanketter eller funktion på kommunens Intranet plats.

HÄLLEFORS KOMMUN

IT-enheten 712 83 Hällefors
Besöksadress Sikforsvägen 15 Hällefors
Telefon 0591-641 00 vx • Fax 0591-109 76
kommun@hellefors.se