IT-Säkerhets -instruktion:

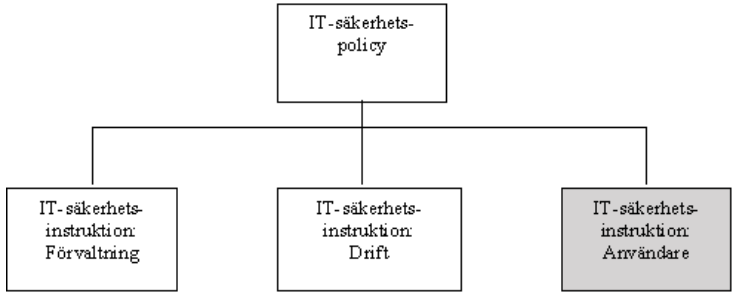
- Användare

Arvidsjaurs kommun

1. INLEDNING

IT-säkerhet är en del i Arvidsjaurs kommuns lednings- och kvalitetsprocess som skall bidra till att ett IT-system kan användas på avsett sätt och med avsedd funktionalitet. Krisberedskapsmyndighetens (KBM) rekommendationer om basnivå för IT-säkerhet (BITS) skall gälla som ramverk för IT-säkerhetsarbetet.

Styrande dokument för IT-säkerhetsarbetet är:



IT-säkerhetspolicy och IT-säkerhetsinstruktioner fastställs av kommunfullmäktige.

1.1 ALLMÄNT

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

Du måste veta:

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

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

1.2 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 närmaste chef,
- föreslå utvecklande förändringar av IT-systemen,
- meddela systemadministratör behovet av skydd för känslig information,
- förstå IT-systemets struktur och rollfördelning inom kommunen,
- förstå begränsningar och risker i användandet av e-post och Internet.

1.3 SYSTEMSTRUKTUR OCH ROLLFÖRDELNING

Det övergripande ansvaret för kommunens IT-system vilar på Kommunstyrelsen som också utser systemägare för kommunens IT-system. **För att uppnå samsyn skall en IT-beredningsgrupp inrättats för att analysera och förbereda IT-frågor för beslut.**

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

Systemägare – Systemägaren (resp. nämnd genom sin ordförande) initierar den egna verksamhetens behov av IT-stöd. Systemägaren har det övergripande ansvaret inför kommunfullmäktige 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.

Systemansvarig (Operativt ansvarig) – har den tekniska kompetensen inom respektive verksamhetsområde. Systemansvarig utses av systemägaren och är den person som har ansvaret för den dagliga användningen av IT-systemet. Systemansvarig samverkar med IT-avdelningen 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 systemansvarig vad avser drift och resurstilldelning för ett IT-system.

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

IT-säkerhetsansvarig – ***(Kommunchefen)*** understödjer arbetet med att uppnå IT-säkerhetspolicyns mål och är ansvarig för att samordna IT-säkerhetsarbetet inom kommunen. Samordnaren är i IT-säkerhetsfrågor direkt underställd Kommunstyrelsen.

IT-säkerhetsledning - Vid större oplanerade IT-relaterade händelser tillämpas kommunens krisledningsplan.

2. INFORMATION OCH LAGRING

2.1 ALLMÄNT

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

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

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

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

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

Kommunen har fastställt dokumenthanteringsplaner som du skall ha i åtanke när du arbetar med dina 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 och styrs av kommunens instruktion för hemliga handlingar.

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 m.m. Hur du skall hantera dina handlingar framgår av en särskild instruktion.
Huvudregeln är att allmänna handlingar är tillgängliga för envar 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 du är tveksam skall du kontakta din chef.

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

2.2 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 kommunen 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 du skall och får tillföra, ändra och eventuellt ta bort. 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 du att 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 du tänker över säkerheten och hur du lagrar, klassar och hanterar informationen.

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

När du skapar egen information är det viktigt att veta var den bör lagras. Den information du lagrar på våra gemensamma utrymmen, som kan nås via nätet, säkerhetskopieras automatiskt. Du kan välja att lagra på enheterna, H:, I: eller G:

- H: (Personlig hemkatalog) är din personliga enhet som du kan använda för lagring av personligt arbetsmaterial. Om du väljer H-enheten kommer dina medarbetare ej åt informationen.
- I: (Internt inom kommunhuset) är en enhet för lagring av information som alla medarbetare inom kommunhuset har tillgång till.
- G: (Gruppenhet) är en enhet för lagring av information som du och medarbetarna inom din egen verksamhet har tillgång till.

All lagring på din lokala hårddisk (C:) ska undvikas, eftersom du riskerar att förlora information som inte kan återskapas till rimliga kostnader, vid t.ex. en diskkrasch, stöld etc.

För åtkomst till eget data även utanför kommunens nätverk, kontakta IT-Avd. Det finns lösningar för både PC och mobila enheter att få åtkomst till sitt data utan att vara inloggad i kommnens nätverk.

2.3 BEHÖRIGHET

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

2.4 LÖSENORD

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

- inte avslöja ditt lösenord för andra eller låna ut din behörighet,
- skydda lösenordet väl,
- omedelbart byta lösenord om du vet eller misstänker att någon känner till det,
- byt lösenord när du får upp en ruta på skärmen som uppmanar dig att det är dags att byta.

Du 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-system du är behörig till samtidigt.

Lösenordet skall bestå av minst 6 tecken och skall konstrueras så att det inte lätt kan kopplas till dig som person. Enkla repetitiva mönster såsom t.ex. AAA111 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. Använd inte Å,Ä,Ö i lösenord.

Viktigast av allt är dock att du väljer ett lösenord som du kommer ihåg.

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

3. IT-SÄKERHET OCH KRINGUTRUSTNING

3.1 ALLMÄNT

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

- Mjukvara (program) som inte godkänts av IT-avdelningen får ej installeras eller användas i kommunens arbetsstationer eller nätverk. Det är inte heller tillåtet att kopiera eller använda kommunens program utanför kommunens verksamhet. Om du är i behov av ytterligare programvaror eller hårdvara t.ex. mobiltelefoner, läsplattor, digitala kameror mm skall du anmäla det till din chef.
- All installation och konfiguration av hårdvara och arbetsstationer skall ske av IT-avdelningen så att kommunens standard följs.
- Vid tillfällen när du inte har uppsikt över arbetsstationen kan du tillfälligt låsa arbetsstationen med kortkommandot: CTRL+ALT+DEL. Vid längre frånvaro skall arbetsstationen loggas ur.
- Vid fel på arbetsstation med tillhörande hårdvara skall du omgående anmäla detta till Helpdesk.
- Din arbetsstation med tillhörande hårdvara är kommunens egendom och får ej bytas, förändras eller medtagas utan verksamhetschefens medgivande.
- Inför service på din utrustning som innebär att din persondator lämnas bort eller kasseras måste känslig information i din hårddisk tas bort. Rådgör då med IT-avdelningen.

3.2 BÄRBARA- OCH HEMDATORER

Av kommunens IT-säkerhetspolicy framgår att arbete utanför kommunens lokaler som kräver uppkoppling mot det interna nätverket i normala fall ej är tillåtet. Kontakta IT-avd om sådant behov finns. Om du har en egen bärbar- eller hemdator som du använder för hemarbete bör du tänka på att dessa kan utgöra en säkerhetsrisk. Tänk på att:

- Inte kopiera känslig information till exernt lagringsmedia som du sedan tar med hem. Risk finns att obehöriga då kan ta del av den.
- Att du inte får lagra sekretessbelagd eller för verksamheten känslig information på den egna datorn.
- Lagringsmedia som du använder/skapar i hemdatormiljö på USB-minnen, brända skivor, zip-disk 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. Kontakta Helpdesk om du har frågor.

3.3 KRINGUTRUSTNING MED MELLANLAGRINGSMÖJLIGHETER

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

3.4 VÅRT LOKALA NÄTVERK (LAN)

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

- Inloggning på nätverket skall ske med ditt personliga lösenord (se avsnitt 3 och 4).
- All inloggning eller försök till inloggning under annan, eller med annans identitet är absolut förbjuden. Sådan handling betraktas som dataintrång och är straffbar enligt lag.
- När du arbetar i kommunens nätverk loggas och registreras i allmänhet dina 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 (se kap 2).
- Det är förbjudet att skaffa sig utökade systemrättigheter än det som tilldelats.

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

4. INTERNET OCH E-POST

4.1 INTERNET

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

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

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

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

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

4.2 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” och ”Skickat” för att frigöra utrymme. E-postsystemet skall inte användas som ett arkivsystem, meddelanden, bifogade filer m.m. som du vill spara, sparar du på samma sätt som du lagrar annan information.

Om du inte har möjlighet att kontrollera din e-post skall du ge någon annan fullmakt att kontrollera din brevlåda.

Var extra uppmärksam då Du använder E-post. E-post med bilagor utgör ett stort hot när det gäller spridning av virus.

Allmänt

- e-postsystemet är ett arbetsverktyg och all användning ska ske med gott omdöme,
- det är samma regler för diarieföring av e-post, som för vanliga brev,
- om du misstänker att det kommit in virus via e-postsystemet skall du agera som beskrivits i avsnittet om Incidenter,
- tänk på att e-post i princip är jämförbart med att sända vykort.

Utformning

- du skall följa de råd om inställningar i och hantering av e-postsystemet som du får av IT-avdelningen,
- det är inte tillåtet med automatisk vidarekoppling till annan e-postadress,
- ange alltid ämne för meddelandet för att klargöra för mottagaren vad denne kan förvänta sig för innehåll i e-brevet,
- skriv inte någon känslig information i ämnesraden,
- skriv korta brev. Tänk på att mottagaren kanske får stora volymer e-post,
- använd ”läskvittens” endast för interna meddelanden när du har behov av detta,
- du bör vara selektiv med att använda stora gruppadresser (massutskick) och med att skicka eller vidarebefordra meddelanden som innehåller stora filer,
- skicka inte och vidarebefordra inte kedjebrev av någon sort,
- sprid inte din 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,
- använd inte heller din vanliga användaridentitet och ditt lösenord när du registrerar dig i konferenser eller publika e-postservrar,
- om du får hotelsebrev eller liknande, kontakta din chef. Ta inte bort brevet,
- om du är osäker på om ett e-brev innehåller virus – kontakta Helpdesk.

Bilagor

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

5. INCIDENTER, VIRUS, STÖLD M.M.

5.1 OBEHÖRIGT INTRÅNG

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

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

5.2 VIRUS

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.

Kommunen har bra programvaror för viruskontroll och det görs kontinuerligt kontroll i nätverket. Exernt lagringsmedia (USB.minnen) och filer som du hämtar från Internet ska 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),
- pip eller hälsningar på skärmen,
- datorn uppträder på ett onormalt sätt, t.ex. arbetar mycket långsamt.

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

- INTE stänga din dator genom att slå av strömmen utan istället dra ur nätverkskabeln,
- omedelbart anmäla förhållandet till Helpdesk. OBS! Anmälan skall ske per telefon eller besök, EJ per e-post.

Om du får brev med virusvarning där man talar om att ett virus är på gång skall du inte skicka meddelande om detta till alla på arbetsplatsen, utan kontakta IT-avdelningen som kan avgöra om det är en seriös varning eller kanske bara ett skämt. Skicka inte heller någon varning externt innan du kontrollerat med Helpdesk.

5.3 STÖLD M.M.

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

Om du upptäcker fel och brister i de system du använder skall du rapportera dessa till Helpdesk eller din närmaste chef.

Kommunen 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 du till att förebygga. Informera IT-avdelningen som sammanställer rapporterna.

6. ÖVRIGT

6.1 STÖD OCH HJÄLP

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

6.2 NÄR DU SLUTAR DIN ANSTÄLLNING

Ansvarar du för att:

- rådgöra med din chef om vilket av ditt arbetsmaterial som skall sparas, notera att allt arbetsmaterial du framställt anses vara kommunens egendom och får inte tas med utan chefs godkännande,
- rådgöra med din chef om hantering av din e-post
- kontaktuppgifter raderas från hemsidor o.dyl.
- avregistrera alla prenumerationer och medlemskap
- avregistrera konton för mobila enheter på Apple & Google m.fl
- privat material raderas
- återlämna taggar/brickor för inpassering och utskrifter
- återlämna all utrustning, dator, mobil,platta, mobilt bredband etc.
- Allt sparat material och användare raderas 2 månader efter avslutad anställning

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