



# Älvdalens kommun

SERVICEKONTORET

Datum

(Efter remiss)

Referens

Ert datum

Er referens

Anders Barke, IT-gruppen  
Tel 0251-80 456  
e-post: [anders.barke@edu.alvdalen.se](mailto:anders.barke@edu.alvdalen.se)



Fastställd

## IT-policy och säkerhetsmanual, Älvdalens kommun

Föreliggande dokument utgör IT-gruppens i Älvdalens kommun förslag till "IT-policy och säkerhetsmanual" för IT-användningen inom Älvdalens kommun. Ett av syftena med IT-policyn är att medvetandegöra användarna om de risker och regler som följer med den ökande användningen av IT.

Policyn föredrogs i Älvdalens KS 20001205, och antogs i Älvdalens kommunfullmäktige 20010219.

E u  
Anders Barke

## **Innehållsförteckning**

<b>Avsnitt</b>	<b>Sid</b>
Definition	3
Mål, strategi	3
Webbplats	4
E-post	4
Etiska regler, generellt	5
Säkerhetsmanual	6
• Inledning	6
• Etiska regler för din arbetsplats	6
• Inköp av datorer	6
• Lösenord och användar-ID	7
• Skydd av datorn	7
• Skydd av dokument	7
• Offentlig och allmän handling	8
• Sekretess	8
• E-post, gallring	9
• Yttrande- och meddelarfrihet	9
• PUL, Personuppgiftslagen	9
• Diarieföring	10
• Öppnande av annans e-postlåda	10
• Virus	10
• Server	11
• Behörigheter	11
• Reservrutiner	12

## DEFINITION

Med IT avses utnyttjande av datasystem samt interna och externa nät för hantering och bearbetning av information.

## 2. GENERELLT

### 2.1 MÅL

Målen för Älvdalens Kommuns IT-verksamhet är

1. att användning av IT skall leda till en effektivisering av arbetet vid Älvdalens kommun.
2. att studerande och personal vid Älvdalens kommun skall lära sig att använda IT inom sina respektive verksamhetsområden. Att kunna hitta rätt i informationsflödet samt att uppöva förmåga att kritiskt värdera information är väsentligt.
3. att effektivt sprida information och att kommunicera via nätet, genom främst webbsidor och e-post. Detta är ett viktigt medel för administrativ rationalisering i vad gäller såväl kontakt inom kommunen som externt. Hittillsvarande flöde av papper bör kunna reduceras.
4. att IT skall utnyttjas som ett väsentligt medium för marknadsföring av Älvdalens Kommun, ex via hemsidan.
5. att informationsgivning i hög grad skall ske med hjälp av IT-tillämpningar istället för med tryckt material.

Mål, strategier och policy för IT-verksamheten måste ständigt omprövas med beaktande av nya tekniker och tillämpningar.

### 2.2 STRATEGI

I ”IT-strategi för Älvdalens kommun 2000”, antagen vid fullmäktigemötet i december 1999, anges ett antal aktiviteter för olika områden inom kommunens IT-användande. Dessa aktiviteter ska ha hög prioritet. IT-strategi och policy skall revideras och uppdateras årligen.

### **3. WEBBPLATS**

#### **3.1 MÅL**

Målen med webbplatsen är

1. att kommunens olika verksamheter skall presenteras på webbsidor, vilket till del bör kunna ersätta traditionella trycksaker och annan form av distribution.
2. att marknadsföra kommunen genom aktuell information om verksamheter, evenemang, service, taxor, kulturhistoria, näringsliv mm.

#### **3.2 STRATEGI**

1. En ansvarig för respektive avdelnings information på webbsidorna skall finnas. I dennes uppgifter skall ingå att tillse att avdelningens information är aktuell och förenlig med nedan angivna etiska regler. Denna person kan vara samma person som är "supportkontakt" på avdelningen.
2. Efter hand skall ges möjlighet till respektive avdelnings informationsansvarige att själv lägga in ny information på webbplatsen.
3. En standard utarbetas för de presentationer av kommunens verksamheter som läggs ut på webbplatsen.

### **4. E-POST**

#### **4.1 MÅL**

Målet för Älvdalens kommuns e-post är att e-post skall vara ett primärt medel för såväl intern som extern kommunikation för anställda och studerande inom Älvdalens kommun.

#### **4.2 STRATEGI**

Anställda och studerande skall använda e-post för överföring av för sådan distribution lämpade dokument. I fall då pappersutskrift erfordras av mottagaren eller merparten av mottagarna, skall dock traditionell distribution tillämpas, i förekommande fall i kombination med överföring med hjälp av e-post.

## 5. ETISKA REGLER

1. Kommunen tillhörigt lagringsmedium får inte användas för lagring av information i någon form, som innebär missaktning för folkgrupp eller annan sådan grupp av personer med anspelning på t ex ras, kön, hudfärg, nationellt eller etniskt ursprung, trosbekännelse eller pornografiska bilder.
2. Anslutning till kommunens nät får inte användas för spridning av sådana bilder eller sådana texter som har angetts i punkten 1. Kommunens webbsidor och sidor som dessa är länkade till får inte innehålla information av sådant slag. Sådan information får inte heller plockas upp på datorskärm eller via kommunens nät överföras till annat medium, oavsett om så sker på egen eller kommunen dator eller datormedium. Den som av misstag får upp bild av angivet slag är skyldig att omedelbart koppla ned anknytningen i fråga.
3. Pressetiska regler skall tillämpas i fråga om vad som får presenteras inom ramen för kommunens anslutning till nätet genom e-post, webbsidor eller på annat sätt.
4. Anslutning till kommunens nätverk får inte användas på sådant sätt, att annan persons integritet kränks, även om det inte innebär en överträdelse av ovan angivna regler.
5. Kommunens nät får inte utnyttjas för spridande av kommersiell reklam genom e-post till grupper av mottagare eller samtliga anslutna eller på annat sätt.
6. Den av varje studerande/förälder undertecknade ansvarsförbindelsen om datoranvändning vid Älvdalens skolor skall innehålla ett åtagande att respektera de i IT-policyn angivna reglerna.

## Säkerhetsmanual

### INLEDNING

Den här säkerhetsmanualen har två syften. Dels att skydda vårt arbetsmaterial från otillbörlig påverkan. Dels att skydda sekretessbelagt material från spridning. Älvdalens kommun är en offentlig myndighet. Därför är en del av vår datahantering lagreglerad. Manualen innehåller enkla beskrivningar av dessa lagar och förordningar, samt hur vi ska tillämpa den.

Manualen är också framtagen för att vi skall kunna hålla en så driftsäker datamiljö som möjligt. Ibland kan den kanske kännas överdrivet petig. Men faktum är att även små avsteg från reglerna kan få ganska stora konsekvenser.

Det är alltså därför inte bara en rekommendation att Älvdalens kommuns anställda följer manualen. Det är ett krav!

Säkerhetsansvarig för IT-verksamheten är IT-ansvarige. Kontakta alltid denne om du är osäker.

### ETISKA REGLER FÖR DATAANVÄNDNINGEN I ÄLVDALENS KOMMUN

Du är som användare själv ansvarig för din arbetsstation och allt som görs med användning av ditt användar-ID och lösenord.

Det är inte tillåtet att försöka få tillgång till nätverksresurser du inte har behörighet till.

Det är inte tillåtet att försöka ändra i andra mappar och dokument i servern än dina egna.

Det är inte tillåtet att försöka göra intrång i andra användares konton, mappar och dokument.

Vid användning av elektronisk post skall vanliga Umgängesregler iakttas.

Kommunens nätverk får inte användas för privat vinning eller andra privata syften.

Du får inte installera programvara som kan förorsaka störningar på nätverket. Datautrustningen är ett arbetsredskap för effektivisering av arbetet. Ändringar av inställningar i utrustningen kan medföra driftsstörningar.

Du förbinder dig som anställd att följa kommunens säkerhetsregler för IT-verksamheten.

### REGLER FÖR DIN ARBETSPLATS

Som sades inledningsvis är du själv ansvarig för din dator och att reglerna efterföljs. Det innebär att du är skyldig att omedelbart rapportera fel och onormala händelser (t ex om någon försökt ta sig in på din dator på något sätt) till IT-ansvarig eller nätverkstekniker. Genom loggar kan vi identifiera varifrån eventuella intrång skett.

### INKÖP AV DATORER

Datorer till arbetsplatser skall alltid beställas via IT-gruppen. Byten av maskiner inom eller mellan kontor skall också anmälas till IT-gruppen.

## LÖSENORD OCH ANVÄNDAR-ID

För att skydda dina data från otillbörliga ändringar måste du ansluta till nätverket med det användar-ID du tilldelats samt med det lösenord du själv angivet.

Du får absolut inte ”låna ut” ditt användar-ID och lösenord mer än i undantagsfall. Har du gjort det måste du omedelbart därefter byta lösenord.

Du får inte heller ha funktioner aktiverade som gör att din dator ”kommer ihåg” ditt lösenord och loggar in dig automatiskt när du slår på datorn.

Lösenordet skall bytas minst var tredje månad. Du kommer automatiskt att få en påminnelse när tiden för ditt gamla lösenord gått ut. Lösenordet består av tecken och kan vara en kombination av siffror och bokstäver.

Måste du skriva upp ditt lösenord får du inte förvara det i direkt anslutning till datorn.

## SKYDD AV DATORN

Lämnar du rummet skall du logga ut. Lämna inte fönster öppna. Följ i övrigt rutiner för larmning osv. Låsanordningar för datorerna får användas. Betänk dock att det oftast är innanmätet i datorn tjuvarna vill åt. Ibland kan låsanordningarna vara mer till skada än till nytta. Tänk på hur du förvarar din ev. bärbara dator. Det är absolut förbjudet att t ex lämna den obevakad i bilen.

## SKYDD AV DOKUMENT

I normalfallet skall du spara dina dokument på servern. På den tas säkerhetskopior varje dygn. Om du sparar dokumentet på din egen hårddisk bör du ta egen säkerhetskopior, t ex på diskett. Förvara disketten på säker plats.

Din mapp på servern har bara du och nätverksadministrationen tillgång till, om du inte meddelat att även andra skall ha tillgång till uppgifterna.

Låt inte dokument du skrivit ut ligga framme.

## MJUKVARA

All installerad programvara på arbetsstationerna skall omedelbart rapporteras till IT-ansvarige. Det är inte tillåtet att lägga in privata program på arbetsstationerna. Kontrollera med IT-ansvarig innan du installerar program. Varje förvaltning utser ansvarig som ser till att rapporteringen fungerar. IT-ansvarig ser till att installerad programvara är licensierad. Icke licensierad programvara får inte användas.

Originalskivor av programmen skall förvaras i säkerhetsskåp (OBS att datamedia kräver en speciell förvaring. De förstörs nämligen vid en lägre temperatur än t ex papper.) Lämpligast är att skivorna förvaras hos IT-ansvarige och/eller nätverkstekniker, samt om möjligt, i annan lokal än där programmen är installerade.

## OFFENTLIG OCH ALLMÄN HANDLING

Vi jobbar på en offentlig förvaltning, Merparten av det material vi arbetar med är därför att betrakta som allmän eller offentlig handling, oavsett i vilken form vi bearbetar den. Våra uppdragsgivare, dvs. kommuninvånarna kan då och då vilja se vad vi jobbar med. Det följande gäller behandling av uppgifter vare sig de sker på papper, ljud eller bildmedia, elektroniskt eller på annat sätt.

## ALLMÄN HANDLING

En allmän handling är en handling som kommit till myndigheten eller som upprättats av myndigheten. En handling som myndigheten själv upprättar blir allmän antingen när ärendet är slutbehandlat eller när handling expedieras. Handlingar som inte hör till något speciellt ärende blir allmän handling när de färdigställts hos myndigheten.

## OFFENTLIGHET ELLER SEKRETESS

Det finns två sorters allmänna handlingar: Offentlig eller sekretessbelagda. Principen är enkel: Alla handlingar är offentliga som inte sekretessbelagda enligt Sekretesslagen.

Sekretess gäller:

1. Rikets säkerhet
2. Rikets finans-, penning- och valutapolitik
3. Intresset att förebygga och beivra brott
4. Det allmännas ekonomiska intresse
5. Skydda enskildas personliga eller ekonomiska förhållanden.

Vanligast är sekretess inom socialtjänsten och sjukvården.

## UTLÄMNANDE AV ALLMÄN, OFFENTLIG HANDLING

För att lämna ut en handling måste den givetvis finnas förvarad eller förvaltd på förvaltningen när den sökande vill ta del av den. (Har någon lånat hem handlingen skall den också lämnas ut inom rimlig tid.)

En allmän offentlig handling skall alltid lämnas ut genast eller snarast möjligt. Sökanden har alltid rätt till en kopia till självkostnadspris. Vi får inte ta betalt för framtagning av handlingen.

## SEKRETESS

Sekretesslagstiftningen styr vad som skall sekretessbeläggas. Av nämndens delegationsordningen framgår vem som beslutar om sekretess för varje avdelning.

Om någon begär att få ta del av en handling måste det först prövas om handlingen skall vara sekretessbelagd. Om en handling, helt eller delvis, bedöms vara sekretessbelagd och därför inte kan lämnas ut måste man alltid ange vilken paragraf i Sekretesslagen som man stöder sig på. Den sökanden ska också upplysas om att kommunens beslut om sekretess kan överklagas hos Kammarrätten.

---

**Postadress**  
Box 100  
796 22 ÄLVDALLEN

**Besöksadress**  
Permatsvägen 1

**Telefon (växel)**  
0251-800 00

**Telefax**  
0251-804 79

**Webadress**  
[www.alvdalen.se](http://www.alvdalen.se)

## E-POST

E-post är att betrakta som en inkommen handling och skall hanteras på samma sätt som vanliga pappershandlingar.

Även meddelanden, brev eller annan kommunikation som kommer via e-post och som på något sätt berör myndigheten är allmän handling. På samma sätt som med papperspost avgör innehållet om det är offentlig eller sekretessbelagd handling.

Det är viktigt att komma ihåg att det som kommer till alla våra e-postlådor i kommunen i regel är allmänna och offentliga handlingar och ska lämnas ut om någon begär det.

Undantag är om man får ”privata” meddelanden via sin e-post. Dessa blir inte allmänna handlingar men å andra sidan bör vi undvika att styra vår privata post, e-post eller annan, via kommunen eftersom misstag kan ske.

E-post liksom papperspost får kastas om de inte är av vikt för kommunen eller berör något ärende:

Ex på sådan som kan rensas/kastas:

- Ni får kasta handlingar och e-post som inte påverkar något ärende. Är de hemligstämplade av någon anledning skall de finnas kvar i huset sex månader efter ankomstdatum.
- Dubbletter och kopior får ni kasta.
- Tillfälliga listor och register som ni använt i ert eget arbete får ni kasta om ni inte behöver dom, eller dom påverkar något ärende.
- Enkäter, rapporter, förfrågningar som inte rör något specifikt ärende får kastas.
- Reklam, inbjudningar får kastas.
- Handlingar som inte berör kommunens verksamhet får kastas. Även s k cookiefiler och e-post.
- Alla loggar för e-post (personliga brevlådor etc.) och webbsidor får rensas från meddelanden och cookiefiler som inte behövs för att ta fram meddelanden med anknytning till ett ärende.
- Arbetskopior, idéskisser, ej färdiga skrivelser (s k arbetsmaterial) får kastas när dom inte längre behövs. (”Slutdokumentet” får däremot inte kastas)
- E-post, webbsidor och annat som skrivits ut och diarieförts eller lagrats på annat sätt får kastas.
- Felaktiga och inaktuella handlingar, e-post och webbsidor som rättats/uppdaterats får kastas.
- Ni får kasta e-post, webbsidor etc. om ni också fått informationen på annat sätt och vice versa. Den kastade handlingen får inte innehålla någon information av vikt för ärendet som inte finns på den sparade versionen.
- Ni får radera telefonmeddelanden, röstbrevlådemeddelanden osv. om ni gjort tjänsteanteckningar på sånt som är av betydelse för ett ärende.
- Handlingar med skriv-, räkne-, eller tankefel får kastas när nya rättade handlingar finns.
- Säkerhetskopior får ersättas av nya.

## YTTRANDE- OCH MEDDELARFRIHET

Enligt tryckfrihetsförordningen och yttrandefrihetslagen får var och en rätt att lämna ut uppgifter och underrättelse till press, radio, tv och andra massmedia. Källan får inte efterforskas.

Yttrandefriheten är inte helt oinskränkt. Den kan begränsas genom lag för bl a rikets säkerhet, privatlivets helgd eller för förebyggande och beivrande av brott. Meddelarfriheten innebär att t ex en anställd på kommunen kan lämna ut sekretessbelagda uppgifter till media. Däremot är det aldrig tillåtet att utlämna en handling som omfattas av tystnadsplikt.

Arbetsgivaren får inte vare sig i generella sammanhang eller i enskilda fall påverka arbetstagaren i yttrande- och meddelarfrihetsfrågor. Arbetsgivaren har dock rätt att kräva att arbetsuppgifterna fullgörs även om detta innebär en faktiskt begränsning av de anställdas möjligheter att begagna sig av yttrandefriheten.

## PERSONREGISTER

### PUL

Personuppgiftslagen har ersatt den gamla datalagen. Den är omdiskuterad och kommer säkerligen att omformuleras inom kort. Grundprincipen är dock att du inte får ha register med personuppgifter på din dator eller på annat sätt, utan att anmäla det till personuppgiftsombudet. Du skall berätta vilka uppgifter som finns i registret och vad du skall ha det till. Vem som är personuppgiftsombud står i personregistret i denna manual. Du måste tala om för den registrerade vad som står om denne, om han frågar.

## UPPGIFTER PÅ HEMSIDAN

Namn och andra personuppgifter (tel nr, e-postadress, foto osv.) får inte läggas ut på hemsida eller på annat sätt publiceras elektroniskt utan personens medgivande.

## E-POST OCH TELEFAX

E-postmeddelanden och telefaxmeddelanden omfattas av samma regler som för övriga handlingar. Här följer instruktioner om hur du bär dig åt med e-post och fax

## E-POSTSYSTEM

Inom kommunen finns två olika e-postsystem. Administrationen använder sig av Group Wise, personal och elever inom skolan använder sig av FirstClass, som internt och externt mailprogram. Programmen är olika, men funktionerna ungefär desamma. Tänk på att även handlingar i e-postlådor i princip är att betrakta som allmän handling. Undvik för din egen skull att ha personliga meddelanden i din e-postlåda, om du tycker att de kan vara känsliga.

Glöm inte att samma lösenordsregler gäller för e-postlådorna som för nätverksuppkopplingen

## DIARIEFÖRING

Meddelanden som du får i e-postlådan, och som innebär att du därmed öppnar ett nytt ärende eller tillför något till ett gammalt, skall skrivas ut på skrivare och diarieföras. Arbetsmaterial behöver inte diarieföras. I övrigt: se gallringsreglerna

## E-POSTADRESSER

Med ditt e-postkonto får du en arbetsadress för e-post. Den är konstruerad enligt principen [fornamn.efternamn@alvdalen.se](mailto:fornamn.efternamn@alvdalen.se) för administrativ personal, [fornamn.efternamn@edu.alvdalen.se](mailto:fornamn.efternamn@edu.alvdalen.se) för pedagogisk personal. Bokstäverna å, ä och ö ersätts alltså i e-postadresser med a, a och o.

## ÖPPNANDE AV ANNANS E-POSTLÅDA

Ibland måste kanske någon annan på kontoret eller avdelningen kunna öppna din brevlåda för att få fram meddelanden som rör ett pågående ärende medan du är frånvarande. För detta krävs dock en fullmakt från innehavaren av e-postlådan. Använd blanketten som finns som bilaga till säkerhetsföreskrifterna.

## FAX

Kom ihåg att risken är stor för att obehöriga kan komma åt dina handlingar som du skickar eller tar emot via fax. Du vet inte vem som står vid den andra maskinen. Även en handling som du får per fax är allmän. Kontrollera om det är ett ärende som skall diarieföras. Datummärk mottagna och avsända fax.

## VIRUSSKYDD

### TÄNK PÅ VAD DU LADDAR NER!

Arbetsstationer som är anslutna till nätverket uppdateras kontinuerligt med nytt viruskydd. Fristående datorer skall förses med viruskydd. Kontakta IT-ansvarige eller nätverksteknikern om du är osäker.

De flesta virusen sprids i dag via internet. Tänk på vad du laddar ner! Filer med prefixet .exe skall ni vara helt säkra på vad det är innan ni plockar hem. Skicka inte heller vidare filer som du inte vet vad de innehåller

Den som medvetet sprider virus eller på annat sätt saboterar IT-funktionerna polisanmäls enl. datalagen.

## SERVERN

## ANSVAR OCH ANVÄNDNING

För kommunens servrar ansvarar IT-gruppen. Varje avdelning bör upparbeta rutiner så att sårbarheten minskar genom att viss kunskap i felsökning finns hos någon på avdelningen.

## BEHÖRIGHETER

Varje avdelning ansvarar för att den anställda har de behörigheter denne är berättigad till. Anställd skall skriva på en försäkran för sina behörigheter.

## UTFORMNING AV SERVERRUM

Servern skall vara placerad i ett låst väl ventilerat utrymme. Skärm till servern skall i normalfallet vara avstängd. (Skärmarna är den vanligaste orsaken till brand i serverrum) I serverrummet skall finnas brandsläckare. Räddningstjänsten skall ha tillgång till nyckel till serverrummet. Därutöver skall man vara mycket restriktiv med att ge folk tillträde till serverrummet. Rummet skall vara inbrottssäkert.

## RESERVROUTINER FÖR LÄNGRE AVBROTT

Hur mycket vi än jobbar för att få till stånd driftsäkra system får vi aldrig glömma Murphys lag. Dvs. allt som kan gå åt skogen gör det förr eller senare. Därför måste varje avdelning utarbeta alternativa manuella rutiner för de uppgifter som är väsentliga för verksamheten.

*OBS! Uppgifterna på denna sida är ej kompletta,  
ska kompletteras med namn och checklistor, rapporter,  
blanketter etc../AB*

#### KONTAKTPERSONER

#### TEKNIKERBESTÄLLNING

Teknikerbeställning skall i första hand göras hos IT-gruppen som prioriterar arbetena.

IT-ansvarig  
Nätverkstekniker

#### ***Säkerhetsansvariga***

Räddningsschef & säkerhetsansvarig  
IT-säkerhet  
Beredskapssamordnare

Sekretess och register

Sekretessansvarig  
Personuppgiftsombud

IT-ansvariga i verksamheten.

*OBS! Uppgifterna på denna sida är ej  
kompletta,  
ska kompletteras med namn och  
checklistor, rapporter, blanketter  
etc../AB*

BUN  
Skolorna:

#### **Checklistor/Rapporter/Fullmakter och försäkringar**

Målsmansblankett för e-postadress till elever

Medgivande för namnpublicering, anställd och förtroendevald.

Säkerhet för personuppgifter, Datainspektionens allmänna råd

.....  
.....  
.....