Krokoms kommun
KROKOMEN TJÏELTE

IT-säkerhetspolicy

Vi gör plats för växtkraft

Krokoms kommuns styrdokument

STRATEGI – avgörande vägval för att nå målen
PROGRAM – verksamheter och metoder i riktning mot målen
PLAN – aktiviteter, tidsram och ansvar
POLICY – Krokoms kommuns hållning
RIKTLINJER – rekommenderade sätt att agera
REGLER – absoluta gränser och ska-krav

Fastställt av: Kommunstyrelsens arbetsutskott
Datum: 1998-05-20, Dnr KS98/034, reviderad: December 2005
För revidering ansvarar: IT-chef
Dokumentet gäller för: [Klicka och skriv]
Dokumentet gäller till och med: Tills vidare

Förord

IT är en förkortning av InformationsTeknologi.

Denna instruktion ska vägleda Dig i användningen av såväl Krokoms kommuns gemensamma IT-kommunikationsnät som din egen datorarbetsplats så att användningen sker på ett riktigt och säkert sätt. I kommunens IT-strategi ingår säkerheten som en viktig del och denna anvisning ger en beskrivning hur säkerheten ska uppnås på bästa sätt. Det är Din skyldighet som användare att känna till denna instruktion.

Du måste som användare vara medveten om vilka säkerhetsregler som gäller i Krokoms kommun och vad som förväntas av Dig och andra befattningshavare. Ett stort ansvar för IT-säkerheten vilar på Dig som vanlig användare. Alla som på något sätt nyttjar kommunens IT-system har ett ansvar för sin egen användning av systemen.

De instruktioner som redovisas i detta dokument gäller för alla IT-system i Krokoms kommuns gemensamma IT-kommunikationsnät. Därutöver kan det finnas särskilda instruktioner som gäller för de enskilda IT-system som används typ biblioteksystem, äldreomsorgssystem m.m. och som utfärdas av respektive systemförvaltare för specifikt system.

Ibland förekommer beteckningen ADB som beskrivning av delar av IT. Detta beror ex. på att lagstiftningen inte riktigt hängt med utvecklingen.

ADB kan betraktas som en viktig del av IT men det finns annat inom IT som inte är ADB. I begreppet IT inkluderar vi idag telefoner, fax, video, telebild och andra former för informationsspridning via tekniska hjälpmedel.

Om Du har frågor kring IT-säkerhet, vänd Dig i första hand till IT-enheten eller till din chef.

Innehåll

1 Anvisningar för alla användare

Om Du är tveksam vilka regler som gäller kontakta då IT-enheten eller din chef.

1.1 Fysiskt tillträdesskydd.

Stäng dörren till ditt kontorsrum när Du lämnar det. En stängd dörr hindrar eld att sprida sig och försvårar även stöld av utrustning under dagtid. Om Du lämnar rummet obevakat mer än tillfälligtvis ska Du logga ur datanätet. Du får aldrig vara inloggad i något av de centrala IT-systemen och lämna datorn obevakad under annat än för kortare stunder.

Låt inte okända personer använda din arbetsplats. Om Du är osäker hänvisa till din IT-enheten eller chef som kan besluta om personen ska få tillgång till din dator.

1.2 Stöldmärkning och stöldskydd.

All IT-utrustning i kommunen ska vara märkt. IT-enheten hjälper till med registrering och stöldmärkning av IT-utrustning. Du bör själv förvissa Dig om att din utrustning är stöldmärkt. Om din

utrustning inte är märkt meddela detta till IT-enheten. Normalt ska systemenhet, bildskärm, skrivare och annan utrustning vara märkt med en etikett med blå eller röd etsningstext ”Krokoms kommun”, samt ett löpnummer.

Utrustning som står oskyddad och är särskilt utsatt för stöldrisk kan förses med någon form av stöldskydd. Skyddet kan vara speciella låsskenor för att fästa datorn vid skrivbordet eller att systemenheten tas bort vid arbetets slut och låses in i något slags stöldsäkert skåp. Det senare ska göras med de bärbara persondatorerna som är särskilt stöldutsatta. Förvara alltid nycklar till stöldlås så att någon obehörig ej kan komma åt dem.

1.3 Installation av utrustning och program.

Installation av datorer och annan utrustning i det gemensamma IT-kommunikationsnätet får endast utföras av personal från IT-enheten.

Utrustning får inte flyttas från en anslutning i datanätet till en annan utan att IT-enheten informerats.

Endast centralt godkända program får installeras i persondatorer som är anslutna till gemensamma kommunikationsnätet. Programmen ska installeras av personal från IT-enheten. Installation av övriga program får endast ske efter samråd med IT-enheten på Krokoms kommun.

Disketter/CD-/DVD-skivor/USB-minnen som inte kommer från noga kontrollerad källa får inte sättas in i kommunens persondatorer. Om Du får en diskett/CD-

/DVD-skiva/USB-minne med information som Du behöver i din persondator ska Du först skicka den IT-enheten för att de ska kontrollera att den inte innehåller datavirus. Om Du ofta behöver flytta data t.ex. mellan en dator i hemmet och din dator på arbetet ska Du be IT-enheten installera viruskontrollprogram i din dator.

Alla disketter/CD-/DVD-skivor/USB-minnen som kommer från annan än IT-enheten ska testas i en persondator med viruskontrollprogram innan data från dessa läggs in i Din persondator. Godkänd programvara för denna test är "Panda Platinum Internet Security 2006 eller Panda ClientShield".

Märker Du datavirussmitta är Du skyldig att genast meddela IT-enheten eller din chef. Undvik därefter att använda persondatorn tills dess den hunnit kontrolleras.

Observera att spelprogram på inga villkor får användas i Krokoms kommuns datorer.

1.4 Säkerhetskopiering (Back-up)

Säkerhetskopiering av den information som finns lagrad i de centrala och gemensamma systemen sker genom IT-enheten försorg varje natt, måndag till och med fredag natt. Dessa säkerhetskopior sparas i fyra veckor. Dessutom tas var fjärde vecka en månatlig backup som sparas i två år. Alla datafiler i det gemensamma systemen skyddas på detta sätt mot förstörelse. Data som lagrats under arbetsdagen innan backup kan dock riskera att förstöras om allvarligt haveri inträffar mellan säkerhetskopieringarna. Vissa system skyddas dock via s.k. spegling eller med särskilda loggfiler mot databaser.

Data som lagrats på din egen persondators lokala skivminne säkerhetskopieras inte centralt. Detta måste Du själv se till att göra och finna rutiner för. Rutiner och funktioner för detta kan IT-enheten hjälpa Dig med att upprätta eller föreslå lösningar på.

Säkerhetskopior med sekretessbelagd information på eller känsliga uppgifter får inte föras ut utanför förvaltningens byggnad.

1.5 Skriv- & Lässkydd

Det åvilar Dig som användare att skriv- och/eller lässkydda filer(dokument) som Du som bedömer som nödvändiga att skydda på detta sätt. Var också uppmärksam om det finns någon regel eller anvisning som säger att filer av visst slag ska skyddas med skriv- och/eller lässkydd. Som exempel kan nämnas nämndsprotokoll som alltid ska skrivskyddas innan de läggs ut på gemensam katalog (T).

Om Du behöver hjälp med detta vänd Dig till IT-enheten, så hjälper de Dig.

1.6 Gallring

Du ska som enskild användare minst två gånger per år gallra bland de dokument som ligger i din ”W-katalog” samt i ”T-katalogen” eller finns i andra system, t ex GroupWise. Om Du även lagrar information på din persondators hårddisk ska Du även gallra denna information. Gallring ska dessutom göras när det finns behov av hårddiskutrymme.

Tänk på att det finns särskilda regler och lagar som styr gallringen. Du får t.ex. inte gallra sådant som måste arkiveras. Finns informationen redan arkiverad i pappersform kan Du gallra. Om Du är osäker vad som gäller så fråga din chef eller IT-enheten.

1.7 Felrapportering

Fel i IT-systemen kan uppstå av många olika orsaker. Det är ofta svårt för en användare att avgöra vad felet beror på. När ett fel uppstått är det förstås viktigt att snabbt få rättelse, men det är också viktigt att

felen dokumenteras så att man kan undvika dem i framtiden.

Om Du som användare råkar ut för fel ska Du först själv försöka att avgöra vilken typ av fel det rör sig om. Ta för vana att anteckna eventuella felmeddelanden på skärmen - om möjligt, ta en skärmbild genom att trycka ner knappen ”PrtSc”.

Försök sedan att klistra in denna skärmbild i t ex Word och skriv ut felmeddelandet på papper - innan Du går vidare och begär hjälp.

Hjälp kan Du få av systemförvaltaren/systemadministratören för det system Du använder eller från IT-enheten.

1.8 Behörighetsregler

Innan Du kan få tillgång till kommungemensamma system i kommunens nät måste ansvarig verksamhetschef avgöra om och vad Du ska ha tillgång till. Denne ska sedan lämna en undertecknad ansökan om detta till IT-enheten.

Du ska ha behörighet endast till de funktioner och de data (information) som Du behöver för att kunna sköta ditt arbete. Observera att det ej är tillåtet att söka information som ej behövs för ditt arbete, även om Du genom behörighetssystemet fått tillgång till informationen.

I samband med att Du ges behörighet skall Du kvittera ett exemplar av detta dokument – ”Krokoms kommuns IT-säkerhetspolicy”.

Det lösenord som hör till din egen användareidentitet ska Du hålla hemligt för andra personer. Lösenord får Du inte heller registrera i persondator eller anteckna och förvara där det finns risk för obehörig åtkomst. Du är som enskild användare personligt ansvarig för vad som händer i systemet med hjälp av din användaridentitet.

Lösenordet ska innehålla minst 5 tecken. Bokstäverna å, ä och ö ska Du inte använda. Däremot kan Du använda kombinationer av bokstäver och siffror.

Försök att hitta på ett lösenord som Du inte tror att någon annan kan lista ut. Lösenord ska ej vara personrelaterade (bilnummer, namn eller dylikt).

Eftersom lösenordet ger Dig tillgång till alla system som Du är berättigad att använda är det mycket viktigt. Om Du skulle glömma ditt lösen ord ska Du vända Dig till systemförvaltaren för respektive system. Dessa kan hjälpa Dig att få ett nytt lösenord. Du bör byta lösenord ungefär var tredje månad.

Om Du misstänker att någon obehörig fått tillgång till ditt lösenord ska Du omedelbart byta detta mot ett nytt.

Tänk på att den påloggning Du gör när Du startar en persondator som är ansluten till datornätet inte ger någon säkerhet för den information som finns lagrad i persondatorn. Den påloggning Du gör i persondatorn är endast till för att skydda informationen i det system Du kopplar upp Dig mot från persondatorn via datanätet. Dessa system kan vara PA-system, KIS, Individ & Familjeomsorg, äldreomsorgssystem m.m.

Lagra därför aldrig känslig information i din persondator och ta säkerhetskopior på all information Du lagrar där.

Lämna aldrig en dator eller terminal påloggad i ett system. Avsluta alltid din session så att det krävs en ny påloggning för att komma åt systemet när Du lämnar datorn/terminalen.

1.9 Ombud och vikarier

Ibland kan det vara nödvändigt för Dig att ge någon annan tillgång till samma behörighet som Du själv. I första hand ska problemet lösas genom att använda gemensamma register och arbetsmappar i de aktuella systemen om Du är uppkopplad mot dessa.

Vill Du ge någon annan tillgång till din egen behörighet ska Du alltid kontakta den som är systemförvaltare för det aktuella systemet först. Den som är systemförvaltare ska sedan avgöra om behörigheten får delas. Alternativet är att lägga upp en helt ny behörighet på denna person. I så fall ska ansvarig verksamhetschef lämna undertecknad ansökan om sådan behörighet till IT-enheten.

1.10 Tystnadsplikt och dataintrång

I offentlig verksamhet gäller sekretesslagens bestämmelser om tystnadsplikt. För uppgifter i kommunens ADB-register gäller datalagens bestämmelser om dataintrång. Den som olovligen bereder sig tillgång till, eller ändrar eller utplånar uppgift i ADB-register kan dömas till böter eller fängelse i högst 2 år (§ 21 Datalagen).

Tänk på att om Du lämnar rummet när Du är "påloggad" så finns det risk för att obehöriga kan komma åt data med hjälp av din behörighet. Du kan då bli personligt ansvarig för eventuella skador. Om något sker med hjälp av din användareidentitet ser det ut som om det är Du som gjort det.

1.11 Kvalitetsskydd

Det är viktigt att alla data som registreras i våra IT-system är riktiga. Ditt viktigaste bidrag till i detta sammanhang är att alltid vara noggrann både när det Du registrerar och när Du söker data i systemen.

Om Du är tveksam om hur information ska lagras eller sökas i ett IT-system, ska Du alltid kontakta den som är systemförvaltare för hjälp.

Var vaksam, anmäl misstänkta fel eller företeelser samt om Du upptäcker felaktiga data till IT-enheten eller din chef.

1.12 Hemliga uppgifter

Sprid inte information till andra utanför Din förvaltning hur system är uppbyggda, fungerar eller vilka system som används i Din persondator.

Vid tveksamhet angående detta vid eventuella studiebesök eller liknande kontakta alltid IT-enheten.Följande är strängt förbjudet att sprida om Du skulle ha kännedom om detta: Modem nummer, IP-adresser, Loginnamn och lösenord.

1.12.1 Speciellt angående faxar

Tänk på att inte faxa känsliga dokument. Det händer då och då att faxning sker till annan än det var meningen att faxa till.

1.12.2 Mobiltelefoner

Tänk på att mobiltelefoner kan avlyssnas.

1.13 Brandtillbud

Om Du skulle drabbas av brand i Din PC, försök att dra ut elsladden om detta är möjligt utan att Du utsätter Dig för fara. Larma räddningstjänsten! Om Du kan, försök kväva elden genom att kasta en filt eller dylikt över PC:n. Till sist kan Du försöka att få ut PC:n ur Ditt arbetsrum t ex genom ett fönster. Men tänk på att det kan vara farligt att inandas gaser från den smälta plasten. Ett alternativ kan vara att lämna Ditt arbetsrum och stänga dörren efter Dig.

2 Aviseringar för systemförvaltare

Systemförvaltare för ett IT-system utses av respektive verksamhetschef i samråd med IT-enheten. Systemförvaltaren ansvarar, under respektive nämnd/förvaltning för administration, förvaltning och användning av ett visst IT-system.

Systemförvaltaren ska försäkra sig om att säkerheten i IT-systemet ligger på en tillfredsställande nivå.

Systemförvaltaren ansvarar också för att särskilda instruktioner finns tillgängliga för användarna så att användningen kan ske på ett säkert sätt. I detta arbete ingår ett ansvar för nödvändig utbildning och stöd för den personal som använder systemet. För detta ändamål kan kommunens utbildningslokal Ansätten användas.

Systemförvaltaren ska i samråd med berörd/a verksamhetschef/er upprätta reservrutiner för hur verksamheten ska upprätthållas i händelse av att verksamhetens IT-stöd av någon anledning skulle sluta fungera för en längre tidsperiod.

Systemförvaltaren ska tillse att berörd personal informeras om de nödvändiga utbildningar som bedöms erfordras och som IT-enheten genomför.

Det ligger på systemförvaltaren att bedöma behovet av utbildning i kommunens IT-system.

I de kommunövergripande systemen ska systemförvaltarna tillsammans utforma de regler som ska gälla för systemet.

Systemförvaltaren bedömer behovet av säkerhetskopieringar på centrala servrar utöver de som IT-enheten normalt utför. Dessa utförs normalt av IT-enheten nätterna mellan måndag-tisdag, tisdag-onsdag, onsdag-torsdag, torsdag-fredag och fredag-lördag. IT-enheten gör inga säkerhetskopieringar mellan lördag-söndag och söndag-måndag.

Om extra behov av säkerhetskopieringar föreligger ska systemförvaltaren komma överens med IT-enheten om hur den ska utföras.

Systemförvaltaren ska se till att aktuell dokumentation om IT-systemet finns tillgänglig. Systemförvaltare ska se till att användarna har aktuella instruktioner till sitt system.

Systemförvaltare beslutar om gallring i IT-systemet. Särskilda regler gäller för gallring, vilket måste beaktas.

2.1 Behörighetsregler.

Systemförvaltaren ska utfärda behörighetsregler och behörighetsinstruktion för IT-systemet. Detta ska dokumenteras och tillsändas IT-enheten samt användarna.

Systemförvaltare ska ansvara för att användarna av ett IT-system är tillräckligt utbildade för att kunna använda systemet på rätt sätt. Detta omfattar bl. a att användarna ska förstå vad datakvalitet innebär i det enskilda IT-systemet

3 Anvisningar för IT-enheten

IT-enheten ansvarar för driften av servrarna i de kommungemensamma datanätet.

IT-enheten ansvarar för säkerheten i de kommungemensamma datanätet. IT-enhetens personal är de som praktiskt arbetar med stöd och service av kommunens IT-system.

3.1 Fysiskt skydd och stöldmärkning

IT-enheten ansvarar för att tillträdesskyddet fungerar för de viktigaste lokalerna (datahall, korskopplingar m.m.). Datahallen i förvaltningshuset ska alltid vara låst och tillträde till denna av andra än personal från IT-enheten får endast ske i sällskap med behörig personal. Under icke kontorstid ska datahallen vara larmad. Datahallen är utrustad med brand-, värme- och inbrottslarm. Dessutom är hallen utrustad med reservkraft - UPS - som ska svara för strömförsörjning till utrustningen för en tid av 30 minuter, nödbelysning samt programvara för att på ett säkert sätt ”ta ner” datahallens utrustning. Det är IT-enhetens ansvar att regelbundet se över dessa säkerhetsinstallationer i syfte att säkerställa deras funktionalitet.

IT-enheten ska utföra stöldmärkning av datorutrustning. All utrustning ska vara märkt med etsningstexten ”Krokom kommun”, samt ett löpnummer. All IT-utrustning som levererats till kommunen men inte installerats på avsedd plats ska förvaras stöldskyddat. Det är IT-enhetens ansvar att se till att så sker. IT-enheten ska också dagligen kontrollera förvaltningshusets lastkaj, för att säkerställa att inte utrustning blir stående på lastkajen utan övervakning.

3.2 Installation av utrustning och program

IT-enheten ansvarar för förberedelser, genomförande, dokumentation och IT-tekniker för installation av maskinutrustning i det gemensamma datanätet.

Vid installation av utrustning i det gemensamma nätet åvilar det IT-enheten att beakta IT-säkerhetsaspekterna. Till exempel ska skrivare som kan komma att skriva ut sekretesskyddat material placeras i låst utrymme dit bara berörd personal har tillträde alternativt ska utskrifterna lösenordskyddas.

Installation av utrustning i det gemensamma datanätet får endast utföras av IT-enhetens personal. Om extern personal ska utföra installationen får detta endast ske under övervakning av personal från IT-enheten.

IT-enheten ansvarar för förberedelser, genomförande och dokumentation av systemprogrammering och programinstallationer i det gemensamma datanätet.

Program och andra datamängder får endast installeras i det gemensamma datanätet efter beslut av

IT-enheten. Generellt gäller att endast programvaror som godkänts av IT-strategigruppen i Krokoms kommun får installeras.

3.3 Säkerhetskopiering (Back-up)

IT-enheten ansvarar för säkerhetskopiering i de gemensamma servrarna. Säkerhetskopiering (dagliga och periodisk) ska utföras enligt dokumenterade anvisningar av personal från IT-enheten. IT-enheten ska också regebundet kontrollera gjorda säkerhetskopieringars kvalité för att säkerställa deras fulla funktionalitet

Säkerhetskopiering utförs normalt enligt följande, nätterna mellan måndag-tisdag, tisdag-onsdag, onsdag-torsdag, torsdag-fredag gör s.k. dagsback-up. . Dessutom tas varje månadsskifte en månatlig backup som sparas i två år. Vid dessa säkerhetskopieringar körs hela systemen av på band. Banden lagras därefter i brandsäkert datamediaskåp. IT-enheten gör normalt inga säkerhetskopieringar mellan lördag-söndag och söndag-måndag..

3.4 Felrapportering

Alla fel som kommer till IT-enhetens kännedom och som bedöms vara av vikt ska registreras som underlag för framtida felavhjälpning. Även vidtagna åtgärder för att komma till rätta med problemet ska dokumenteras.

IT-enheten ska i fall då det bedöms som viktigt anmäla programfel/systemfel till systemleverantören.

3.5 Behörighetsregler

Registrering av användareidentiteter i det gemensamma datanätet ska endast utföras av personal på IT-enheten. Registrering innebär att användarna ges de generella behörigheter som är nödvändiga för att utnyttja de olika IT-systemen.

IT-enheten ansvarar för högsta behörighet i det gemensamma datanätet. Normalt ska endast personal vid IT-enheten ha högsta behörighet i det gemensamma datanätet. Servicetekniker från leverantör kan vid behov utnyttja högsta behörighet men detta ska då ske under övervakning från personal från IT-enheten. En sådan behörighet får endast tilldelas tillfälligtvis och ska omedelbart deaktiveras efter det att serviceteknikerna utfört sitt arbete. En användares behörighet i systemen ska inte sättas högre än vad som behövs för att användaren ska kunna utnyttja de funktioner som hon/han ska vara behörig till.

IT-enheten ska på uppdrag av respektive systemförvaltare registrera de särskilda behörigheter som krävs för användningen av installerade IT-system.

Systemöversikter och viktigare detaljer som berör det gemensamma datanätet ska vara dokumenterade. Dokumentationen ska så klart som möjligt återspegla aktuell status vad gäller installerad utrustning, applikationer i drift samt behörighetssystem. IT-Tekniker ansvarar för att dokumentationen är aktuell och tillförlitlig.

3.6 Skydd mot datavirus

För att skydda det gemensamma datanätet från att infekteras av datavirus ska IT-enheten tillse att endast "godkända" disketter/CD-/DVD-skivor används vid installationer i persondatorer anslutna till det gemensamma datanätet.

Användarna är uppmanade att alltid låta IT-enheten kontrollera disketter/CD-/DVD-skivor/USB-minnen innan dessa används i kommunens persondatorer. IT-enheten har ett särskilt ansvar att bevaka händelseutvecklingen inom detta område, anskaffa program som kan spåra och eliminera datavirus samt att ge noggranna instruktioner till användarna. IT-enheten ska se till att användare som ofta flyttar information via diskett får ett godkänt viruskontrollprogram installerat på sin dator.

3.7 Tystnadsplikt och sekretess

IT-enheten har, på grund av sin höga behörighet, ett särskilt ansvar för att inte utnyttja information från de gemensamma systemen eller annan information som de ges tillgång till genom sitt arbete. Reglerna i datalagen om dataintrång gäller fullt ut trots att personal på IT-enheten har teknisk tillgång till systemen.

3.8 Återvinning/destruktion av IT-utrustning

All återvinning och destruktion av kasserad IT-utrustning ska ske av IT-enheten. Detta för att säkerställa att arbetet sker på ett IT-säkerhetsmässigt och miljöanpassat sätt.

4 Systemansvar

IT-enheten ansvarar för följande system utöver ren systemprogramvara i Novell 6.5 servrar och Windows 2002/2003-servrar.

- KIS - KontorsInformationsSystem
- TEKNISKA – Tekniska verksamhetssystem
- EKONOMI - Ekonomisystem
- SOCIALA - Sociala verksamhetssystem
- P/A-System - Personaladministrativa system
- BUN - Barn- & UtbidningsNämndens verksamhetssystem

5 Inkopplingsregler

Nedanstående föreskrifter gäller för inkoppling av datautrustning till kommunens IT-kommunikationsnät. Förutom dessa föreskrifter gäller också Krokoms kommuns övriga föreskrifter inom IT-säkerhetsområdet.

5.1 Det centrala nätet

Krokoms kommuns centrala IT-kommunikationsnät består av flera olika delar.

Det administrativa nätet är uppbyggt med Ethernet-teknik och har flera centralt i förvaltningshuset placerade servrar under operativsystemet Novell 6.5 och 2000/2003-servrar.

Idag består kommunadministrationens datormiljö av 25 servrar varav 3 Novell (inloggningsserver) och 19 Windows servrar (2000/2003), 1 Unix och 2 övrig. Dessa är lokaliserade till kommunens datahall i förvaltningshuset, Krokom.

Kommunen har ett gemensamt datanät (Ethernet), nätverksoperativsystem är Novell NetWare, med IP-trafik som är uppbyggt på följande sätt:

Mot förvaltningshusets fastighetsnät är Centrumhuset, Räddningstjänsten, Kom Vux/Gymansieskola och Krokoms sjukhem anslutna via egen fiber.

2) Enheter (cirka 45 st) utanför centralorten Krokom är i huvudsak anslutna med ISDN (med en avlämningspunkt) mot det fasta nätet via router. Innan 2005 års slut är det avtalat att samtliga ISDN-förbindelser ska ersättas av nytt förvaltningsnät av typen xDSL med lägst 2 Mbyte kapacitet.

De lokala enheterna kopplas mot avlämningspunkterna m h a lokala Ethernet-nät

Funktionellt sett består kommunnätet av 2 huvudnät, ett administrativt nät (cirka 240 persondatorer) och ett utbildningsnät (cirka 730 persondatorer - används av elever och lärare inom skolorna). Näten är separerade från varandra och omvärlden och skyddas av en brandvägg. Trafik mellan administrativa nätet och utbildningsnätet är helt spärrat för alla typer av trafik. Eventuellt informationsutbyte sker via godkända tjänstefunktioner i brandväggen.

Fjärranslutning till det kommunala nätet är möjlig från Internet och xDSL. För säkra anslutningar från Internet använder kommunen en VPN-lösning.

5.2 Uppkoppling av lokala nätverk

Lokala nätverk som ska kopplas upp mot de centrala näten måste vara uppbyggda med samma säkerhetskrav som de centrala näten. Om man lokalt ska ha administrativa system knutna till det centrala administrativa nätet måste arbetsplatserna vara åtskilda från andra delar av nätet (utbildningsnätet). Om lokala nätverk både ska kopplas upp mot de centrala administrativa nätet och det öppna nätet (Internet) måste kommunikationen åtskiljas. Normalt sker detta genom att använda en router som har två ingångar, en för det administrativa nätet och en för det öppna nätet. Routern ska sedan vara konfigurerad så att båda näten åtskiljs.

Alternativet är att varje nät har egen dedicerad förbindelse till varje nät (en för utbildning och en för administration).

Om en lokal server ansluts till nätet ska denna endast anslutas till ett av näten. Om man i undantagsfall vill ansluta en server både till öppna och det slutna nätet ska denna vara konfigurerad på så sätt att båda näten hålls helt åtskilda (t. ex 2 st kommunikationskort).

Huvudregel: undervisningsnäten får aldrig kopplas in på det administrativa nätet.

6 Fysiska krav på det lokala nätverket

I det lokala nätverket ska routrar och korskopplingspaneler vara inlåsta i ventilerade skåp eller utrymmen. Om det lokala nätet har egen server ska denna förvaras i separat låst och larmat utrymme med kylanläggning. I första hand bör man välja ett utrymme utan fönster och gärna i ett rum med förstärkta väggar.

Nödbelysning skall finnas. Reservkraft av typ UPS skall vara installerad. (Drifttid 30 min) Nedtagningsprogram kopplad till UPS'n skall finnas för kontrollerad nedtagning av server vid strömavbrott.

6.1 Behörigheter

Behörighet till de administrativa delarna av nätet får endast tilldelas person som behöver detta i sitt arbete. För varje delsystem i det centrala administrativa nätet ska respektive verksamhetschef avgöra vilka som ska ha behörighet till systemen. Behörigheter ska vara personliga och varje person som tilldelas en behörighet är personligen ansvarig för att denna ej missbrukas. Varje ny användare ska kvittera Krokoms kommuns IT-säkerhetspolicy (denna handling).

Behörighet till de öppna delarna av systemen ska tilldelas på motsvarande sätt men för dessa ställs inte samma säkerhetskrav. För de öppna delarna av systemen kan behörighet tilldelas en grupp användare t. ex en klass.

Om en server är ansluten till kommunens centrala nät via kommunikationsutrustning ska den högsta behörigheten (t. ex Supervisor eller root) endast tilldelas kommunens IT-enhet.

6.2 Ansvar

För varje lokalt nätverk som ska anslutas till de centrala näten ska det finnas en utsedd server/säkerhetsansvarig. Denne ansvarar för att ingen obehörig får tillgång till de lokala systemen och ska dessutom vara ansvarig för att ingen obehörig får tillträde till kabelsystemställ, kommunikationsutrustning eller servrar. Den lokale server/säkerhetsansvarige ska i samråd med IT-enheten utforma de behörighetsregler och andra regler som krävs för att säkerheten ska kunna garanteras. Konfigurering av routrar och annan kommunikations-utrustning får endast utföras av kommunens IT-enheten. Om det i det lokala nätet finns en server som på något sätt är ansluten till både det öppna och det slutna nätet får denna konfigureras endast av IT-enheten eller person som utses av IT-enheten.

Vid oklarhet om vilka bestämmelser som gäller ska alltid kommunens IT-enhet kontaktas.

6.3 Fjärranslutning

Vid fjärranslutningar ska användarID samt lösenord alltid användas på samma sätt som då anslutning sker från arbetsplats i förvaltningshuset. Alla fjärranslutningar ska regelmässigt ske med VPN-anslutning som ett led i en större IT-säkerhet.

7 Om datalagens tillämpning

Datalagen innehåller de lagregler som gäller för hur man får lägga upp och handha personregister.

Datalagen medför ett speciellt ansvar för nämnder/styrelser i samband med IT-förda personregister.

Denna bilaga redogör översiktligt för datalagens innehåll och konsekvenser för organisationen och IT-säkerhetsarbetet.

Datalagen tillkom 1973 och har sedan dess ändrats flera gånger.

7.1 Datainspektionen (DI)

Datainspektionen har till uppgift att övervaka att de regler som anges i datalagen efterlevs. Speciella regler finns som anger hur datainpektionens tillsyn kan utövas. I arbetet ingår att utfärda licenser enligt datalagen samt pröva frågor om tillstånd att föra vissa personregister. Datainspektionen lämnar också råd och anvisningar till myndigheter, organisationer och enskilda.

7.2 Beskrivning av datalagen

För mer utförlig information se broschyren "Datalagen - information från Datainspektionen".

7.3 Datalagens syfte

Datalagen förutsätter att registrering av personuppgifter ska få förekomma. Dess syfte är att hindra att hanteringen av IT-förda personregister medför otillbörligt intrång i den personliga integriteten

Intrång i registrerads personliga integritet uppkommer i princip varje gång vi använder uppgifter om en registrerad utan personens vetskap eller medgivande. Detta är ibland nödvändigt för att kunna utföra viss verksamhet. Observera datalagens formulering otillbörligt intrång vilket bl. a betyder att uppgifterna inte får användas till annat än i enlighet med registrets ändamål.

7.4 Viktiga begrepp och definitioner

En personuppgift är en upplysning som avser enskild person. Som exempel kan nämnas namn och personnummer (identitetsuppgifter). Uppgifter som rör enskilda personers förhållanden som t ex skattebetalare, anställd, bilägare etc är också personuppgifter.

Ett personregister är ett register, förteckning eller annan anteckning som förs med hjälp av IT och som innehåller personuppgift som kan hänföras till en bestämd person. Vilka register som räknas till personregister kan ibland vara svårt att avgöra. Ändamålet med registret är här av stor betydelse När det gäller ordbehandlingsdokument (löpande text) har datainspektionen inte bedömt detta som personregister även om texten innehåller namnuppgifter.

Begreppet registrerad avser enskild person om vilken förekommer personuppgift i personregister.

Registeransvarig är den för vars verksamhet personregister föres, om han förfogar över registret. Att förfoga över register innebär att man kan påverka innehållet i registret samt överföra uppgifterna till läsbar form. Servicebyrå eller IT-enheten, som endast tekniskt bearbetar registret, är ej registeransvarig. Om personregister förs för flera nämnders räkning blir samtliga registeransvariga under förutsättning att de helt eller delvis kan bestämma över registrets innehåll.

Registeransvarig är normalt den nämnd eller styrelse för vars verksamhet registret förs.

Den verksamhet som använder, förvaltar och administrerar ett IT-system benämns systemägare. En nämnd eller styrelse kan vara ägare till ett system som används av andra nämnder. Observera att en nämnd kan vara registeransvarig utan att vara systemägare.

8 Skyldigheter enligt datalagen

8.1 Licens- och tillståndsplikten

Varje registeransvarig ska ha licens utfärdad av datainspektionen. För vissa register, som bedöms innebära särskilda risker för otillbörligt intrång i enskilds personliga integritet, krävs dessutom särskilt tillstånd.

Observera att "samkörning" av flera register i allmänhet är att betrakta som ett nytt register som kan erfordra särskilt tillstånd.

Vissa undantag finns från tillståndsplikten, bl a inom socialtjänsten.

8.2 God registersed

Alla personregister ska inrättas och föras på ett sådant sätt att inte otillbörligt intrång i registrerads personliga integritet uppkommer.

8.3 Förteckningsskyldighet

Den registeransvarige ska förteckna de personregister som han är ansvarig för. Förteckningen ska vara aktuell och innehålla vissa specificerade uppgifter. En aktuell kopia av förteckningen ska alltid sändas till IT-enheten som ajourhåller en gemensam förteckning över alla Krokoms kommuns personregister.

Förteckningen ska hållas tillgänglig för datainspektionen och ska på begäran sändas in.

8.4 Uppgift om avsändare

Namn och adress på den registeransvarige, eller licensnummer, ska anges på handlingar som sänds till den registrerade om handlingar innehåller uppgifter ur personregister.

8.5 Rättelseskyldighet

Den registeransvarige ska utan dröjsmål rätta, ändra eller utesluta oriktiga eller missvisande uppgifter i personregister.

Den registeransvarige ska utse en eller flera kontaktpersoner som ska bistå den registrerade vid misstanke om oriktiga eller missvisande uppgifter. Uppgift om vem som är kontaktperson ska hållas tillgänglig för allmänheten.

8.6 Förbud att lämna ut personuppgift

Före utlämning av uppgift ska den registeransvarige undersöka om det finns anledning att anta att uppgiften ska användas för IT i strid med datalagen. I detta fall ska uppgiften inte lämnas ut.

Ska uppgift utlämnas till utlandet krävs medgivande från datainspektionen.

För Krokoms kommun gäller att utdrag till föreningar, myndigheter eller enskilda från kommuninvånareregister och fastighetsregister inte får göras. Sådana utdrag ska hänvisas till Sparregistret som gör en prövning om vad utdraget ska användas

till. Krokoms kommun har endast rätt att göra utdrag till kommunala förvaltningar, stiftelser och bolag.

8.7 Rätten till insyn i personregister

Den registeransvarige är skyldig att på skriftlig begäran av enskild underrätta denna om uppgifter om henne eller honom som finns registrerade i personregister (begäran om utdrag enligt 10 § datalagen).

Rätten till insyn kan begränsas av sekretessbestämmelser (t ex inom socialtjänsten m.m.).

8.8 Bevarande och gallring

Personuppgift ska utgå ur register då uppgiften inte längre behövs med hänsyn till ändamålet med registret.

8.9 Anmälan om upphörande

Registeransvarig ska meddela datainspektionen då man upphör att föra ett tillståndspliktigt register. Dessutom ska IT-enheten meddelas för att registerförteckningen ska kunna hållas aktuell.

8.10 Tystnadsplikt

I myndighets verksamhet gäller sekretesslagens bestämmelser i första hand. Inom en verksamhet gäller dessutom de behörighetsregler som fastställts av den registeransvariga nämnden.

9 Ansvar enligt datalagen

Registeransvaret som är grundläggande ansvarsbegreppet i datalagen, ligger på nämnden/styrelsen och kan inte delegeras. Den registeransvarige är enligt datalagen skyldig att se till att IT-säkerheten är tillfredsställande.

Den som bryter mot bestämmelserna i datalagen kan dömas till böter eller fängelse samt, i vissa fall, bli skadeståndsskyldig.

Det straffrättsliga ansvaret för överträdelser mot datalagen ligger på nämnden/styrelsen och kan delegeras.

Observera dock, att ansvaret för IT-säkerhet bara kan delegeras till personer som har tillräcklig kompetens för uppgiften och som fått erforderliga instruktioner.

Observera även att ledningen är skyldig att gripa in om det visar sig att det föreligger brister vid utförandet av uppgiften. Om ledningen varit oaktsam vid delegeringen eller inte ingripit trots att det förelegat brister vid utförandet av uppgift som delegerats kan ledningen bli ansvarig för eventuella överträdelser.

Den registeransvarige är skadeståndsskyldig för skada som tillfogas registrerad genom att ett personregister innehåller oriktiga eller missvisande uppgifter om honom.

9.1 Dataintrång

Nämnden/styrelsen är skyldig att se till att personregister förs enligt "god registersed". Detta innebär bl a att bevaka säkerheten i det behörighetssystem som används för åtkomst i IT-register. Det finns naturligtvis en viss risk för att behörighetssystemet inte skyddar i tillräckligt hög grad.

Därför bör varje enskild användare av IT-systemen vara medveten om bestämmelserna i 21 § i datalagen som handlar om dataintrång.

Den som olovligen (dvs allt utanför tilldelad behörighet) bereder sig tillgång till eller ändrar eller utplånar uppgifter i myndighets IT-register kan dömas till böter eller fängelse i högst 2 år. Detsamma gäller försök till dataintrång. Observera att även om man har behörighet till ett personregister får man endast använda det för att sköta de arbetsuppgifter som behörigheten är knuten till.

10 Om offentlighet och sekretess

Offentlighetsprincipen är mycket gammal inom svensk förvaltning. Lagbestämmelsen kring offentlighet är en av rikets grundlagar.

Motiven för denna offentlighetsprincip är:

- Kontrollen av myndigheternas verksamhet blir effektivare. Förtroendet för myndigheterna blir större om de arbetar under insyn.
- Informationen om allmänna angelägenheter sprids bättre både genom enskilda och massmedia.
- Samhällsdebatten kan föras med ett bättre underlag.

Sedan 1960-talet har det varit klart att offentlighetsprincipen också omfattar IT-upptagningar.

De grundläggande bestämmelserna finns i 2 kapitlet 1949 års tryckfrihetsförordning (TF), som är en av våra grundlagar.

TF:s bestämmelser om allmänna handlingars offentlighet kompletteras i vissa delar av sekretesslagen (1980:100). I denna lag finns bestämmelser om sekretess, registrering av IT-upptagningar, upplysningsplikt mm som har stor betydelse för kommunens IT-användning.

10.1 Offentlighetsprincipen

Allmänheten och massmedia ska, enligt TF, ha insyn i statens och kommunernas verksamhet. Detta innebär för kommunernas verksamhet bl a att vem som helst får läsa kommunernas handlingar, förutsatt att dessa är allmänna och inte är hemliga. Dessutom gäller, i vissa fall, att tjänstemän och andra i kommunal tjänst har rätt att berätta vad de vet för utomstående. Det finns också speciella möjligheter att lämna uppgifter till massmedia.

Det kan för en enskild tjänsteman ofta vara svårt att avgöra vad som är en handling och om den är allmän och offentlig. En handling är allmän om den förvaras hos myndighet och enligt TF:s regler anses som inkommen eller upprättad. En allmän handling som inte är hemlig är offentlig.

Det är viktigt att notera det anonymitetsskydd som gäller. Man får alltså inte, "i större utsträckning än som behövs för att myndigheten ska pröva om hinder föreligger mot att handlingen lämnas ut" (TF 2:14), efterforska vem som begär en handling utlämnad eller i vilket syfte handlingen begärs utlämnad. En sådan efterforskning får med andra ord endast göras om den efterfrågade handlingen är hemlig. I vissa fall får nämligen även sekretessbelagda uppgifter lämnas ut, men då bara till en begränsad krets av personer.

10.2 Offentlighetsprincipen och IT

I TF, 2:a kapitlet, anges vad som menas med allmän handling. Där finns också grundläggande regler om vilka allmänna handlingar som får hållas hemliga och hur allmänheten får tillgång till allmänna handlingar som inte är hemliga.

En handling är inte bara en framställning i skrift eller bild utan också upptagningar som endast kan avläsas med hjälp av tekniska hjälpmedel, t ex ADB.

10.3 Allmänhetens tillgång till allmänna handlingar

Den som vill ta del av allmänna handlingar ska vända sig till myndigheten som förvarar handlingen. Myndigheten är då, enligt TF, skyldig att ta ställning till denna framställning och om den bifalls, lämna ut handlingen. En begäran om utlämning ska prövas skyndsamt. En giltig anledning att dröja med utlämning av allmän handling är att myndigheten måste pröva om handlingen är hemlig enligt någon bestämmelse i sekretesslagen. Utlämning kan vägras om handlingen är hemlig.

En allmän, ej hemlig, handling får läsas på plats, skrivas av, fotograferas eller spelas in. Om en handling delvis är hemlig, ska de delar som inte är hemliga tillhandahållas i avskrift eller kopia.

Utlämning kan i ADB-sammanhang ske genom att visa handlingen på en bildskärm eller genom att göra en utskrift. Däremot finns inga krav på att handlingen ska utlämnas i dataläsbart skick t ex på diskett.

Den sökande har också rätt att mot fastställd avgift få en kopia av den allmänna handlingen. Avgiftstaxan har fastställts av kommunfullmäktige och ska tillämpas av alla förvaltningar.

Den som får avslag på framställning enligt ovan har rätt att överklaga detta beslut.

10.4 Sekretesslagen och IT

Huvuddelen av sekretesslagen (som alltså inte är en grundlag) består av bestämmelser som anger vilka begränsningar som gäller i rätten att ta del av allmänna handlingar samt vilka tystnadsplikter som gäller i det allmännas verksamhet. I 15:e kapitlet finns bestämmelser om diarieföring av allmänna handlingar, hemligstämpling, upplysningsplikt och överklagande. Där finns också särskilda bestämmelser om ADB-upptagningar.

10.5 Sekretessen och IT

Flertalet av de särskilda sekretessbestämmelserna i sekretesslagen avser information i alla typer av allmänna handlingar, men några gäller särskilt ADB-upptagningar.

Några bestämmelser har samband med det integritetsskydd som datalagen avser att ge. Hos myndigheter gäller sekretess för personuppgifter i sådana personregister som avses i datalagen om det kan antas att ett utlämnande skulle medföra att uppgifterna används för automatisk databehandling i strid med datalagen.

Det finns också en bestämmelse som har till syfte att motverka att personuppgifter används för databehandling i utlandet som kan innebära otillbörligt intrång i någons personliga integritet.

10.6 Registrering av IT-upptagningar

Varje myndighet är enligt sekretesslagen i princip skyldig att registrera sina allmänna handlingar. För IT-register finns vissa undantag från denna huvudregel

om flera nämnder/styrelser har tillgång till ett gemensamt register. Som exempel kan nämnas att endast den myndighet som tillför ett IT-register en ADB-upptagning, som är att betrakta som allmän handling, är skyldig att registrera denna som en allmän handling.

10.7 Upplysningsplikt

Myndighet ska, enligt sekretesslagen, på begäran lämna ut allmänna handlingar som förvaras hos myndigheten (om dessa inte är hemliga). Man är också skyldig att, muntligt eller skriftligt, lämna upplysningar om hur man rent praktiskt går till väga för att ta del av ADB-upptagningar. Detta betyder att om man ger tillgång till allmän handling via presentationsterminal ska man också ge hjälp med hur terminalen används. Sådan skyldighet föreligger dock endast i den mån "arbetets behöriga gång" inte hindras.

10.8 Allmänna krav på IT-systemen

I sekretesslagen finns en uttrycklig bestämmelse om att myndighet som använder ADB ska ordna denna med beaktande av offentlighetsprincipen. Denna bestämmelse har framförallt betydelse vid införande av nya IT-system och vid ändringar i existerande.

Man ska alltså tänka på att t. ex kunna lämna ut allmänna handlingar med den snabbhet som TF kräver. Vidare är det viktigt att kunna skilja på och hålla isär hemliga och icke hemliga handlingar.

Det kan vara lämpligt (även om det inte finns någon allmän skyldighet) att i vissa IT-system överväga behovet av "presentationsterminaler", dvs särskilda terminaler som inte medför risk för åtkomst av icke allmänna handlingar eller att uppgifter kan förvanskas eller förstöras.

10.9 Rätt att använda terminal

Skrivningen i sekretesslagen medför att enskilda får använda sig av myndigheternas terminaler. Vissa förutsättningar måste dock vara uppfyllda. För det första att terminalanvändningen inte medför tillgång till IT-upptagningar som inte är att anse som allmänna handlingar, för det andra att det inte finns någon bestämmelse om sekretess som omfattar alla delar av de uppgifter som är tillgängliga genom terminalen, för det tredje att det inte finns risk för att IT-upptagningarna förvanskas eller förstörs och för det fjärde, att det inte finns hinder mot användningen av hänsyn till "arbetets behöriga gång" hos myndigheten.

En begäran från enskild att använda terminal måste prövas och - vid positivt ställningstagande - tillmötesgås snarast. Negativa beslut kan överklagas på samma sätt som om sökanden fått avslag på en begäran enligt TF att få ta del av en allmän handling hos myndigheten.

10.10 Beskrivning av IT-register

Enligt sekretesslagen ska myndigheterna för allmänhetens räkning ha beskrivningar av IT-register som förs hos dem. Skyldigheten omfattar inte de register som inte till

någon del anses som allmän handling eller om det uppenbarligen inte har betydelse ur offentlighetssynpunkt.

Beskrivningarna ska normalt innehålla följande uppgifter:

- IT-registrets benämning.
- IT-registrets ändamål.
- Vilka typer av uppgifter som registret innehåller (eller myndigheten har tillgång till om registret används av flera myndigheter).
- Hos vilka andra myndigheter IT-registret är tillgängligt för överföring till läsbar form.
- Vilka terminaler eller andra tekniska hjälpmedel som enskilda själva kan få utnyttja hos myndigheten (t ex presentationsterminaler).
- Vilka bestämmelser om sekretess som myndigheten vanligen ska tillämpa på uppgifter i IT- registret.
- Vem som hos myndigheten som kan lämna närmare upplysningar om IT-registret och dess användning i myndighetens verksamhet.

Beskrivningar av IT-register som används av flera nämnder ska upprättas centralt i Krokoms kommun men sedan finnas tillgängligt hos respektive nämnd.

Beskrivningar ska hållas tillgängliga för allmänheten. Skulle någon eller några uppgifter som ska finnas i en beskrivning vara hemliga, får uppgifterna inte tas med. Sekretesskäl ska nämligen inte hindra att allmänheten får tillgång till beskrivningen.

11 IT-Säkerhetsorganisation

Respektive nämnd är ansvarig för all IT-verksamhet inom nämndens verksamhetsområde. Dessa stöds av IT-enheten.

För varje IT-system i Krokoms kommun finns systemförvaltare som har det övergripande ansvaret för säkerheten inom respektive system.

Normalt har varje förvaltning en person utsedd som IT-säkerhetsansvarig med en person utsedd som ersättare. Normalt fungerar förvaltningens systemförvaltare som säkerhetsansvarig.