



IT-säkerhetsinstruktion Användare

Styrande dokument för IT-användare i Härjedalens kommun i enlighet
med Krisberedskapsmyndighetens Basnivå för IT-säkerhet



INNEHÅLL

1	INLEDNING	2
2	INLOGGNING	2
3	HANTERING AV INFORMATION	3
4	INTERNET	4
4.1	Skydd mot skadlig programkod.....	4
4.1.1	Installation av program.....	5
5	ELEKTRONISK POST	5
6	INCIDENTER	5
6.1.1	Incidentrapportering.....	6
7	DISTANSARBETE OCH MOBIL DATORANVÄNDNING	6
8	BÄRBAR DATOR	6
9	INKOPPLING AV DATORER OCH ANNAN IT-UTRUSTNING	6
10	ARBETSPLATSEN	6

1 INLEDNING

Denna IT-säkerhetsinstruktion för användare är en del av Härjedalens kommuns IT-verksamhet och redovisar hur en användare av kommunens IT-system ska verka för att upprätthålla god säkerhet.

Du som användare har en stor del av ansvaret för kommunens informationssäkerhet. För att du ska kunna leva upp till de säkerhetskrav som ställs måste du känna till:

- vilket ansvar Du har
- vad Du ska göra vid olika incidenter
- var Du kan få stöd och hjälp

Förutom säkerhetsreglerna för datoranvändning finns fyra bilagor som ingår i säkerhetsinstruktionerna:

Bilaga 1: Ansökan - Behörighet till kommunens nät

Bilaga 2: Försäkran - Personligt ansvar för att upprätthålla en god IT-säkerhet

Dessa två dokument, bilaga 1 och 2, ska lämnas påskrivna till Din närmaste chef.

Bilaga 3: Allmänt om information

Bilaga 4: Offentlighet och Sekretess

2 INLOGGNING

Våra IT-system har en inbyggd behörighetskontroll för att säkerställa att det endast är behöriga användare som kommer åt kommunens information. Det är varje användares ansvar att följa de regler som kopplas till behörigheten. För att få behörighet gäller:

- att du skriver under försäkran om personligt ansvar
- att du fyller i en skriftlig ansökan om behörighet
- att din chef godkänner och beslutar om behörighet
- att IT-enheten lägger in din behörighet i nätverket, som resulterar i att Du får:
 - EN ANVÄNDARIDENTITET
 - ETT ENGÅNGSLÖSENORD

Första gången loggar du in med det tilldelade engångslösenordet. **Detta lösenord kan du bara använda för att logga in till kommunens nätverk och byta till ett personligt lösenord (din hemlighet).** Därmed säkerställs att endast du själv känner till lösenordet. Vissa arbetsroller har gruppgemensamt loggin, men ska likställas med personligt loggin och därmed gäller också samma regler och ansvar för gruppen.

Lösenordet ska bestå av minst 8 tecken vilket bör vara en blandning av bokstäver, siffror och specialtecken (till exempel "!" "%&" eller "?"). Välj inte enkla lösenord som ex. "abcd1234" eller andra lättforcerade såsom familjemedlems namn eller lösenord av typen "qwerty12" d.v.s. enkla tangentkombinationer.

Lösenordet är strängt personligt och ska hanteras därefter. Du ska därför:

- inte låna ut din behörighet
- inte avslöja ditt lösenord för andra
- skydda lösenordet väl
- omedelbart byta lösenordet om du misstänker att någon känner till det
- byta lösenord var 60:e dag (sker med automatik, du får varning i god tid)

Om du misslyckas med inloggningen – tänk på att lösenord är känsligt för små och stora bokstäver kontrollera först att 'CapsLock' inte är på. Om du fortfarande inte kan logga in – kontakta **IT-enhetens HelpDesk ankn 561 11 eller 0680-161 11**.

Om du glömmer ditt lösenord och försöker logga in med ett felaktigt lösenord kommer systemet att efter **tre** felaktiga försök att låsas – kontakta HelpDesk för att få ett nytt engångslösenord.

Tidigare använda lösenord kan du inte använda. När du byter lösenord kontrolleras att du inte använder något av de **fem** senaste lösenorden som du använt förut.

Du lämnar spår efter dig när du är inloggad. Systemens loggningsfunktion används för att spåra obehörigt intrång. Detta görs för att skydda informationen och för att undvika att oskyldiga misstänkliggörs om oegentligheter inträffar.

3 HANTERING AV INFORMATION

Viktig och kritisk information för kommunens verksamhet lagras i gemensamma servrar. Ett centralt system säkerhetskopierar varje natt alla förändringar till en särskild server och till magnetband. Om Du lagrar annan information på lokala datorer ansvarar Du själv för att denna blir säkerhetskopierad.

Kommunens IT-enhet rekommenderar att lokal lagring av information inte görs. För att inte fylla centrala servrar rekommenderas att bild- och videofiler som måste sparas kopieras till CD eller DVD.

För den information du lagrar lokalt på din hårddisk ansvarar du själv och innebär:

- att du själv ska ta säkerhetskopior
- att du ska tänka på att disketter, CD och DVD är känsliga för värme magnetism, damm, rök och tryck och måste hanteras därefter. Tänk på stöldrisken !
- att du ska tänka på att andra kan ha otillbörligt intresse av att komma över informationen

4 INTERNET

Kommunens lokala nätverk är anslutet till Internet via en s.k. brandvägg som reglerar in- och utgående trafik. När du använder Internet kan säkerheten påverkas i mycket hög grad beroende på ditt beteende. Du bör också vara medveten om att du, när du surfar på Internet, lämnar spår i en loggfil. Denna loggfil är offentlig handling och visar bland annat vilka webbplatser du har besökt. Loggfilen granskas kontinuerligt.

Vid användande av Internet gäller följande:

- spelprogram får inte laddas in i datorn
- gratisprogram får inte laddas i datorn utan att de godkänns och virustestats av IT-enheten
- fildelningsprogram får inte laddas in i datorn

Allmänt gäller att vid nerladdning av filer från Internet krävs att Du har gott omdöme och endast hämtar sådant som är relevant för arbetet och kommer från välrenommerade sidor. Utöver säkerhetsrisken kan en felaktig hantering innebära skadeståndskrav, till exempel vid brott mot upphovsrätten.

Kommunens datorer och nätverk får inte användas till att sprida, titta eller lyssna på material av pornografisk, rasistisk eller nazistisk karaktär. Förbudet gäller också material som är diskriminerande (religion, kön, sexuell läggning, nationalitet etc.) eller har anknytning till kriminell verksamhet.

När du surfar på Internet representerar du vår kommun. Gör det med gott omdöme och sunt förnuft 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 lämnar spår efter dig i form av kommunens IP-adress.

4.1 Skydd mot skadlig programkod

Ett datorvirus kan beskrivas som ett program eller en programsekvens vars uppgift är att kopiera sig själv och tränga in i andra program för att utföra något otillbörligt. Datorvirus är ofta ytterst smittsamma och smittkällan kan vara svår att identifiera. Gratisprogram, spelprogram och filer som laddas ner från Internet eller bilagor till e-post är de vanligaste smittbärarna.

Kommunen har centrala programvaror för virusbekämpning som kontinuerligt kontrollerar nätverket och de arbetsstationer som är anslutna. Även filer som du hämtar via Internet, e-post, CD, DVD, USB-minnen och disketter kontrolleras av dessa antivirusprogram.

Hela tiden kommer nya datorvirus och eftersom antivirusprogrammen inte kan garantera komplett skydd så gäller för samtliga:

- att vara observant på om datorn uppför sig ”konstigt”, exempelvis att onormala förändringar sker på skärmen eller att datorn arbetar mycket långsamt
- att inte använda datorn vid misstänkt virusangrepp
- att omedelbart avbryta allt arbete i datorn där du gjorde upptäckten
- att omedelbart anmäla det inträffade till IT-enheten
- att anteckna alla iakttagelser som misstänks ha samband med händelsen

4.1.1 Installation av program

Alla program, oavsett om de kommer från Internet eller andra källor, ska installeras av IT-enheten eller av dessa utsedd medarbetare med tillräcklig och godkänd behörighet.

5 ELEKTRONISK POST

E-post är ett rationellt hjälpmedel i arbetet men lagringskapaciteten är begränsad. Tänk därför på att regelbundet radera i mapparna ”Mottagna försändelser”, ”Skickade försändelser”, och ”Papperskorg” för att frigöra utrymme. Bifogade filer som du vill spara kan du spara på samma sätt som du lagrar annan information.

För att undvika risk för datavirus spridning och onödig belastning av systemresurser gäller:

- att det inte är tillåtet med automatisk vidarekoppling från privata e-postadresser
- att vara selektiv med att skicka eller vidarebefordra e-post som innehåller stora filer
- att endast öppna e-post och bifogade filer från avsändare du litar på eller känner till
- att det är samma regler för diarieföring av in- och utgående e-post, som för vanliga brev
- att om du misstänker virussmitta ska du agera som beskrivits i avsnittet om Internet
- att inte använda din kommunala användaridentitet och lösenord när du registrerar dig i konferenser eller publika e-postservrar
- att om du får hotelsebrev eller liknande ska du i första hand kontakta din närmaste chef, ta inte bort brevet

Mer information hittar du i bilaga 4 ”Offentlighet och sekretess”.

6 INCIDENTER

Möjliga oönskade hot mot säkerheten i våra IT-system betraktas som IT-säkerhetsincidenter. Med incident avses:

- dataintrång
- datavirus eller annan skadlig kod i nätverket
- driftavbrott eller fysisk skada såsom stöld, brand, vatten, blixtnedslag, värme och sabotage

För att i möjligaste mån förhindra att en eventuell incident trappas upp till ett verkligt hot gäller :

- att inte försöka åtgärda det inträffade på egen hand
- att omedelbart anmäla incidenten till IT-enheten
- att dokumentera alla iakttagelser i samband med upptäckten
- att notera tidpunkt då du upptäckte problemet och när du själv senast använde systemet

6.1.1 *Incidentrapportering*

För att ytterligare förstärka säkerheten i kommunens IT-system sammanställs rapporterade incidenter. Dessa ligger till grund för säkerhetshöjande åtgärder. Genom att rapportera händelser hjälper Du till att höja nivån på IT-säkerheten.

7 **DISTANSARBETE OCH MOBIL DATORANVÄNDNING**

Det är systemägarens ansvar att besluta om IT-systemet, eller delar av det, får användas vid distansarbete och mobil datoranvändning. Vid sådant arbete ska det alltid finnas ett avtal mellan användaren och systemägaren.

8 **BÄRBAR DATOR**

Bärbara datorer såväl som stationära datorer är arbetsredskap som kommunen tillhandahåller som ett hjälpmedel i det dagliga arbetet. Att använda bärbar dator utanför ordinarie arbetsplats sker under personligt ansvar och utgör alltid en säkerhetsrisk. Därför gäller att:

- hålla dator och datamedia under ständig uppsikt om du inte kan låsa in den
- inte lagra viktig och sekretessbelagd information på datorns lokala hårddisk
- se till att det finns en säkerhetskopia av datorns innehåll på din ordinarie arbetsplats
- tillse att senaste viruskydd och behörighetssystem finns installerat

9 **INKOPPLING AV DATORER OCH ANNAN IT-UTRUSTNING**

Endast datorer och annan IT-utrustning (skrivare m.m.) installerade av IT-enheten får anslutas till kommunens nätverk.

Privata datorer får inte anslutas till kommunens nätverk.

10 **ARBETSPLATSEN**

Om du lämnar arbetsplatsen ska du låsa datorn (Ctrl+Alt+Del) eller logga ut, även om det bara är för en kortare stund, för att inte riskera att obehöriga tar del av eller förstör information i våra system. Det är Du som ansvarar för allt som registrerats med din användaridentitet.

Utskrift av dokument ska i första hand ske till en gemensam nätverksansluten skrivare som IT-enheten har installerat. Endast om särskilda skäl finns, och att närmaste chef godkänt, kan skrivare direktanslutas till din arbetsdator. Om känsliga och sekretessbelagda dokument ska skrivas ut till gemensam skrivare finns funktioner som innebär att du måste gå till skrivaren och med en särskild knapptryckning kontrollerat beordra ut ditt dokument.

Startsida vid uppkoppling mot Internet ska alltid vara kommunens Intranät. Detta ingår i den standardinstallation som kommunens IT-enhet gör och ska inte ändras.

Stöd och hjälp med verksamhetssystem

Kontakta din systemförvaltningsansvarige inom din förvaltning.

Service och support för teknisk IT-utrustning

Vid problem med telefoni, datanät, dator, skrivare etc. **kontakta IT-enhetens HelpDesk** enligt följande turordning:

- 1. via Intranätets felanmälan,**
- 2. via E-post helpdesk@herjedalen.se**
- 3. via Telefon anknytning 561 11 eller 0680-161 11**

IT-enhetens Helpdesk är bemannad under normal kontorstid.