Dnr
62/2004/100

Gäller fr. o. m.
2004-04-01

Antagen
Kf 2004-03-29 § 22

SÄKERHETSINSTRUKTION IT

FÖR ANVÄNDARE

SÄKERHETSINSTRUKTION IT FÖR ANVÄNDARE

Innehåll: Sid

1. INLEDNING

Kommunernas Säkerhetspolicy IT beskriver närmare hur vi arbetar med IT-säkerheten och hur ansvaret för säkerheten fördelas. Vår Säkerhetspolicy IT följer Krisberedskapsmyndighetens (KBM´s) rekommendation ”Basnivå för IT-säkerhet (BITS)”. I detta dokument, ”Säkerhetsinstruktion IT, för användare”, klargörs de regler som gäller för personalens arbete i Blekinge Väst IT-miljö.

Mål

Denna instruktion syftar till att ge dig kunskaper och riktlinjer om hur Du hanterar

- olika former av information,
- den teknik vi använder,
- e-post, internet,
- incidenter m.m.

Instruktionen syftar också till att skydda de värden som informationen representerar och att förebygga att uppgifter och information som omfattas av sekretess röjs, ändras eller förstörs.

Instruktionen skall ge alla medarbetare kunskap och kännedom om hur information, kommunikationsnät, datasystem och arbetsplatser skall hanteras för att felaktigheter och störningar skall undvikas.

2. HANTERING AV INFORMATION

Den information Du lagrar på nätverket säkerhetskopieras automatiskt. Du skall därför lagra din information i egen, alternativt verksamhetsgemensam hemkatalog.

- Egen hemkatalog är ditt personliga arkiv, som Du skall använda för lagring av personlig information. De filer Du sparar i din hemkatalog kan endast Du nå.

- Gemensam katalog är ett arkiv för lagring av gemensam information för en förvaltning, avdelning eller ett arbetslag.

Om Du lagrar information på din lokala hårddisk (ex C:\) är Du personligen ansvarig för att säkerhetskopiering sker, t ex på diskett. När Du lagrar information på din lokala hårddisk (ex C:\) riskerar Du att förlora information, som inte kan återskapas till rimliga kostnader. Du försvårar också möjligheten att dela information med Dina medarbetare.

Tänk också på att den information Du lagrat på lokal disk är tillgänglig för alla som kan starta din dator. Man behöver ofta inte använda något lösenord för att komma åt dessa diskar.

Med stöd av ovanstående gäller att:

Ingen lagring på lokala diskar skall förekomma.

3. BEHÖRIGHET

Våra datasystem (nätverk, servrar och program) är utrustade med behörighetskontrollsystem för att säkerställa att endast behöriga användare kommer åt information. Vilken behörighet Du får till lagrad information och till våra datasystem beror helt på dina arbetsuppgifter och avgörs av din chef. (Din chef lämnar skriftlig beställning till IT-enheten för tilldelning av behörigheter.)

För att få behörighet krävs att

- Du informerats om innehållet i denna säkerhetsinstruktion och om kommunens Säkerhetspolicy IT,
- att Du fått utbildning på de datasystem Du kommer att använda.

När IT-enheten registrerat dig som användare får Du en **användaridentitet** uppbyggd på delar av ditt förnamn och efternamn. I undantagsfall kan gruppidentitet användas för tillgång till basinformation.

4. INLOGGNING

Primärt skall inloggning ske med personlig användaridentitet. Sker inloggning med gruppidentitet får ingen personlig information lagras på gemensam enhet. Första gången Du loggar in får Du ett **tillfälligt lösenord** av IT-enheten. Du blir uppmanad av systemet att byta till ett personligt lösenord. Om Du inte byter lösenord blir Ditt användarid låst.
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 misstänker att någon känner till det,
- byta lösenordet var 90:e dag. Du får en påminnelse på skärmen när det är dags att byta.

Även i andra datasystem än nätverket bör Du byta lösenord var 90:e dag. I dessa datasystem ges dock oftast ingen påminnelse.

Lösenordet skall bestå av minst 6 tecken och skall konstrueras så att det inte lätt kan kopplas till dig som person. Tecknen å, ä och ö får inte användas i lösenord. **Undvik** enkla repetitiva mönster såsom t ex ”ABC1234”, ”AAA1111” får inte användas. Använd inte heller andra lättforcerade lösenord, såsom eget eller familjemedlems namn eller enkla tangentkombinationer av typen ”QWERTYU”. För att väsentligt försvåra lösenordsknäckning bör bokstäver, siffror och specialtecken (#&+) blandas i lösenordet.

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

Tidigare använda lösenord kan inte återanvändas. När Du byter till ett nytt lösenord kontrollerar systemet att Du inte använder något av de senaste 13 lösenorden. **Om Du glömmer ditt lösenord** och försöker logga in i nätverket eller i ett verksamhetssystem med felaktigt lösen, kommer ditt användar-id att spärras efter tre felaktiga försök. Om detta inträffar vänder Du dig till IT-enheten, samt i vissa verksamhetssystem till systemansvarig. Du kommer då att få ett nytt tillfälligt lösenord.

5. EN SÄKER ARBETSPLATS

Kommunen eftersträvar att alla skall ha en säker arbetsplats, inte bara avseende IT-säkerheten. Med arbetsplats avses de personliga utrymmen och material som Du har tillgång till och förfogar över i ditt arbete, som t ex ditt tilldelade tjänsterum, de utrymmen vi gemensamt använder och de utrymmen Du använder vid distansarbete. Utöver de regler som finns under kapitel 2, 3 och 4 gäller följande regler:

Arbetsstation

Följande gäller för samtliga datorarbetsplatser:

- När Du tillfälligt lämnar arbetsplatsen skall lösenordsskyddad skärmsläckare användas.
- Vid längre frånvaro, ex rast, lunch, skall arbetsstationen loggas ur.
- Du är ansvarig för den arbetsstation med tillhörande hårdvara som Du förfogar över.
- Fysiska ingrepp i din arbetsstation med tillhörande hårdvara får endast utföras av IT-enheten.
- Vid fel på arbetsstation med tillhörande hårdvara skall Du omgående anmäla detta till IT-enheten.
- Arbetsstationen med tillhörande hårdvara får inte bytas ut, förändras eller medtagas utan IT-enhetens medgivande.
- Installation och konfiguration av hårdvara får endast utföras av IT-enheten eller av IT- enheten anvisad/godkänd person.

- Mjukvara (program) skall godkännas och installeras av IT-enheten eller av IT-enheten anvisad/godkänd person.

Dator, som Du använder **utanför** din ordinarie arbetsplats kan utgöra en säkerhetsrisk.

Därför skall:
- Du hålla utrustningen och datamedia under ständig uppsikt om Du inte kan låsa in den.
- Du tänka på att Du inte får lagra sekretessbelagd eller för verksamheten känslig information på datorn.
- Du förvarar en säkerhetskopia av all information i din hemmakatalog på nätverket.
- Datorn vara utrustade med system för behörighetskontroll, virusskydd och brandvägg.

Lagringsmedia som Du använder i hemdatormiljö skall viruskontrolleras innan de får användas i kommunens nätverk.

Anm.
Med dator avses alla enheter som kan behandla och/eller lagra information, ex handdatorer (s.k. PDA), mobiltelefoner, bärbara datorer etc.

Kringutrustning med mellanlagringsmöjlighet

Handdatorer, digitala kameror, mobiltelefoner mm kan lätt bli virusbärare då Du kan mellanlagra information för transport 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.

Vårt lokala nätverk (LAN)

Vårt nätverk 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:

- Information, oavsett media, som enligt lagar, förordningar och interna regler bedöms som sekretessklassad med hänsyn till rikets säkerhet får ej lagras i vårt lokala nätverk (LAN).
- Inloggning på nätverket skall primärt ske med din personliga användaridentitet (se kap 3 och 4).
- All inloggning eller försök till inloggning under annan, eller med annans identitet är absolut förbjuden.

- Destruktivt arbete på det lokala nätverket med t ex avsikt att skada lagrad information, ses som mycket allvarligt och är absolut förbjudet och kommer att beivras.
- När Du arbetar i kommunens nätverk förekommer loggning och registrering av dina transaktioner.
- Utskrifter av dokument på gemensam skrivare skall snarast hämtas.
- Information som sparas på det lokala nätverket skall lagras på anvisad plats. (Se kap 2)
- Det är förbjudet att ansluta sig till externt nätverk via egen icke godkänd uppkoppling t.ex. modem.
- För att få tillgång till resurser i vårt interna nätverk med extern uppkoppling, för att t.ex. arbeta från hemmet, skall ett avtal tecknas mellan verksamhetsansvarig och den anställde som reglerar teknik och datasäkerhet m.m.
- Det är förbjudet att utnyttja felkonfigureringar och programfel eller att med andra metoder skaffa sig utökade systemrättigheter eller annan personlig rättighet än den som tilldelats av systemägaren.

Kom ihåg att Du ansvarar för allt som registrerats med din användaridentitet.

6. INTERNET

När Du använder Internet kan säkerheten påverkas i mycket hög grad beroende på Ditt beteende. Inga program får utan särskilt tillstånd laddas ner från Internet (ex spelprogram, skärmsläckare, gratisprogram eller andra program). Det är inte tillåtet att via Internet 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 eller satanism. Undantag får göras när materialet är viktigt för planering och genomförande av undervisning.

För att få ett effektivt resursutnyttjande av Internet-kapaciteten och förhindra att skadlig kod kommer in i nätverket filtreras datatrafiken. När Du surfar på Internet representerar Du kommunen. Gör det med gott omdöme så att ditt agerande på nätet inte skadar kommunens anseende. Agera i enlighet med våra värderingar så att det Du förmedlar på nätet inte skadar kommunen. Du bör tänka på att Du lämnar spår i loggfiler som lagrar information om Internettrafiken till och från kommunen. Loggfilerna är offentliga handlingar och visar vilka webbplatser Du har besökt. Allmänt gäller att den som laddar ner filer från Internet har gott omdöme och endast hämtar sådan information som är relevant för arbetet, är tillåten och kommer från välrenommerade webb- eller ftp-platser. **Se vidare aktuell Internetpolicy.**

7. E-POST

E-post är ett redskap som primärt skall användas i tjänsten. E-post ska behandlas på samma sätt som övrig post. Brevlådan bör tömmas varje dag. Den som av någon anledning inte kan göra det bör se till att någon annan sköter tömningen. Det är inte förbjudet att ta emot och skicka personlig post. Den personliga posten bör dock snarast tas bort från användarens brevlåda.

Skicka aldrig sekretesshandlingar eller integritetskänsliga uppgifter som E-post.

Tänk på upphovsrätten när filer bifogas så att Du inte gör dig skyldig till upphovsrättsintrång. Informationsinnehåll får inte kränka en eventuell upphovsmans eller annans lagliga rättigheter. Om Du har tillstånd att använda bild eller text skall Du alltid ange källa.

För att undvika risk för virusspridning via e-post och onödig belastning av systemresurser:

- bör Du endast öppna bifogade filer från avsändare Du känner till. Kontrollring avsändaren om Du är osäker på innehållet,
- skall Du följa de råd om inställningar i och hantering av e-postsystemet som Du får av din IT-funktion,
- bör Du vara selektiv med att använda stora gruppadresser (massutskick) och med att skicka eller vidarebefordra meddelanden som innehåller stora filer,
- skall Du inte sprida din e-postadress till mindre seriösa ställen varifrån Du t ex kan förvänta dig reklam,
- tillåts inte bifogade filer som är större än 10 mb.

Använd inte heller din vanliga användaridentitet och ditt lösenord när Du registrerar dig i konferenser eller publika e-postservrar.

Om Du misstänker att det kommit in virus via e-postsystemet skall Du agera som beskrivs i avsnittet om ”Incidenter, virus mm”. (Se 8) Filtrering av e-post, se under avsnitt ”Incidenter, virus mm”. (Se 8). **Se vidare aktuell E-postpolicy.**

8. INCIDENTER, VIRUS M.M.

Om Du misstänker att någon obehörig använt din användaridentitet och varit inne i systemet skall Du:

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

Kort om datavirus

Datavirus 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. I värsta fall kan datorns hårddisk raderas eller kan viruset kopiera sig självt i det oändliga tills hela systemet bryter samman. Datavirus 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 programvaror för viruskontroll som kontinuerligt kontrollerar nätverket. Även disketter och filer som Du hämtar från Internet kontrolleras av antivirusprogram i nätverket.

Tecken på datavirus kan vara att

- datorn utför operationer/arbete utan att Du själv startat 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 virus i datorn skall Du

- avbryta allt arbete på det ställe i programmet där Du gjorde upptäckten,
- se till att ingen använder datorn/programmet,
- omedelbart anmäla förhållandet till IT-enheten, systemansvarig. OBS att anmälan skall ske per telefon eller personligt**, EJ** per e-post,
- skriva ner alla iakttagelser som Du tror kan ha samband med händelsen.

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 inom kommunen utan kontakta IT-enheten som kan avgöra om det är en seriös varning eller bara ett skämt. Skicka inte heller någon varning externt innan Du kontrollerat med IT-enheten. För att förhindra att virus kommer in i det interna nätverket sker filtrering av datatrafiken. IT-enheten svarar för att filtrering sker utifrån aktuella virusvarningar.

9. STÖD OCH HJÄLP

Genom IT-enheten kan Du få stöd och support avseende Garanti-/funktionsarbetsplatsen. För verksamhetsspecifika program kan Du kontakta respektive systemansvarig. Är Du osäker kan Du dock alltid vända dig till IT-enheten för råd. Synpunkter och förslag till förändring av ”Säkerhetsinstruktion IT, för användare” anmäler Du till respektive kommuns IT-säkerhetsråd.

10. NÄR EN ANSTÄLLNING UPPHÖR

När en anställning upphör skall:

- det material Du har sparat rensas och tas bort. Arbetsmaterial skall överlämnas till
  anvisade medarbetare,
- ansvarig chef avsluta den anställdes behörigheter i nätverket och i verksamhetssystemen genom anmälan till IT-enheten respektive systemansvarig,
- ansvarig chef anmäla till systemansvarig för e-post-systemet hur kontot skall hanteras.

_____