Tullverkets författningssamling

ISSN 0346-5810
Utgivare: Chefsjuristen Per Kjellsson, Tullverket, Box 12854, 112 98 Stockholm

Föreskrifter om ändring i Generaltullstyrelsens föreskrifter och allmänna råd (TFS 1999:19) om informationssäkerhet för Tullverket;

TFS 2005:12

Utkom från trycket den 18 april 2005

beslutade den 12 april 2005.

Med stöd av 10 § förordningen (2001:646) om behandling av uppgifter i Tullverkets verksamhet, 15 § förordningen (2001:88) om behandling av personuppgifter i Tullverkets brottsbekämpande verksamhet och 18 § verksförordningen (1995:1322) föreskriver[1] Tullverket i fråga om Generaltullstyrelsens föreskrifter och allmänna råd (TFS 1999:19) om informationssäkerhet för Tullverket

dels att 5 kap. 11 § och 12 kap. skall upphöra att gälla,

dels att de allmänna råden till 2 kap. 1 och 4 §§ samt 7 kap. 3 § skall upphöra att gälla,

dels att i 2 kap. 6 §, 5 kap. 2 och 8 §§, 6 kap. 6 och 8 §§, 7 kap. 2 §, 9 kap. 1 och 2 §§, 11 kap. 6 § samt i rubriken närmast före 2 kap. 5 § ordet "IT-avdelningen" skall bytas ut mot "kompetenscenter IT",

dels att författningens rubrik, 1 kap. 1 och 2 §§, 2 kap. 3—5, 7 och 8 §§, 3 kap. 1—5 §§, 5 kap. 4, 6, 7, 9, 12 och 13 §§, 6 kap. 1, 2, 5 och 7 §§, 7 kap. 1, 3 och 4 §§, 8 kap. 1—3 §§, 10 kap. 2 §, 11 kap. 1, 2, 5 och 7 §§ samt rubriken närmast före 11 kap. 1 § skall ha följande lydelse,

dels att de allmänna råden till 5 kap. 5 §, 7 kap. 5 §, 9 kap. 2 §, 10 kap. 1 § samt 11 kap. 1 och 5 §§ skall ha följande lydelse.

Föreskrifter och allmänna råd om informationssäkerhet i Tullverket

1 kap.

1 § Denna författning gäller säkerhet vid hantering av information i datasystem som Tullverket förfogar över. Sådan information skall vara tillgänglig för behörig användare, vara aktuell och tillförlitlig samt vara skyddad från sekretessintrång. Transaktioner och bearbetningar som görs i ett datasystem skall ske i enlighet med systemets ändamål och i efterhand kunna spåras. Särskilda regler om användning av Internet i Tullverket

[1] Dnr 0030-3738/04.

finns i Tullverkets föreskrifter och allmänna råd (TFS 2004:23) om användning av Internet i Tullverket.

2 § I denna författning förstås med

säkerhet: ett tillstånd som uppnås med hjälp av åtgärder mot identifierade hot mot person, organisation och verksamhet såsom brand, våld, stöld, sabotage, organiserad och ekonomisk brottslighet samt mot oavsiktligt felaktigt beteende,

informationssäkerhet: säkerhet vid hantering av information för önskad tillgänglighet, riktighet, sekretesskydd och spårbarhet, uppdelas i *administrativ säkerhet* och *IT-säkerhet*,

administrativ säkerhet: säkerhet som uppnås med hjälp av administrativa regler och rutiner,

IT-säkerhet: säkerhet i IT-system, kan delas upp i *ADB-säkerhet* och *kommunikationssäkerhet,*

ADB-säkerhet: säkerhet och skydd av data och system mot obehörig åtkomst och obehörig eller oavsiktlig förändring eller störning vid databehandling,

kommunikationssäkerhet: säkerhet i samband med överföring av information eller styrsignaler, i syfte att förhindra att känslig information kommer obehöriga till del, att information förvanskas eller inte når mottagaren och att missledande information eller signaler introduceras i kommunikationen eller i systemet,

tillgänglighet: möjlighet för behöriga användare att utnyttja definierade resurser efter behov, i förväntad utsträckning och inom önskad tid,

riktighet: att information och systemfunktioner, t.ex. program och nät, har rätt detaljeringsgrad samt är aktuell, tillförlitlig och stabil,

sekretesskydd: skydd för handling eller uppgift som enligt sekretesslagen (1980:100) inte får lämnas ut,

spårbarhet: möjlighet att kunna fastställa vilka transaktioner eller bearbetningar i datasystem som en identifierbar användare utfört, varifrån (t.ex. vilken terminal) och när,

systemägare: befattningshavare som har det formella och övergripande ansvaret för ett datasystem så att dess ändamål uppfylls på ett för verksamheten korrekt sätt och med ansvar för informationssäkerheten i systemet och för budget som skall disponeras för användning, förvaltning, drift och säkerhet av systemet,

central datordrift: datordrift vid kompetenscenter IT i Luleå för betjäning av den verksgemensamma datormiljön,

lokal datordrift: drift av datorer och annan utrustning i Tullverkets olika lokala nätverk,

lokalt nätverk: lokalt avgränsat datakommunikationsnät som ansluter datorer, arbetsplatser, skrivare och annan utrustning,

verksgemensam datormiljö: informationssystem, datakommunikationsnät, datorer och allterminaler som drivs för och anlitas av hela Tullverket,

allterminal: persondator ansluten i Tullverkets datakommunikationsnät och försedd med säkerhetsprogramvaran TFS Desktop,

datasystem: dataprogram (mjukvara) och teknisk utrustning (hårdvara) som är organiserade med uppgift att genomföra elektronisk informationsbehandling,

verksgemensamma datasystem: datasystem som drivs i Tullverkets verksgemensamma datormiljö,

informationssystem: konstellation av information, datasystem inklusive dess behörighetskontrollsystem, maskinella och manuella rutiner samt dokumentation med regelverk och rutinbeskrivningar,

evaluering: syftar till att visa om och hur säkerhetsfunktionerna i produkter och system uppfyller specificerade säkerhetskrav med hänsyn till korrekthet och ändamålsenlighet, vilket innebär t.ex. att specifikationen för en komponent – om den skall kunna certifieras – skall stämma överens med dess verkliga egenskaper eller att ett program skall vara korrekt i förhållande till systemspecifikationen,

certifiering: officiellt fastställande av resultat från evaluering genom ett formellt beslut av kompetenscenter IT som underlag för driftsättning.

2 kap.

3 § Chefen för arkitekturfrågor vid kompetenscenter IT har ansvaret för samordningen av kompetenscentrets IT-säkerhetsfrågor. Denne har ett särskilt ansvar för att tilldelning av rättigheter och privilegier i systemapplikationer och operativsystem är förenlig med kraven dels på effektivitet och rationalitet i verksamheten, dels på informationssäkerhet.

4 §[2] Chefen för driftfrågor vid kompetenscenter IT svarar för samordningen av informationssäkerhetsfrågor vid övriga kompetenscenter. Inom ramen för denna verksamhet skall kompetenscenter IT, genom lokala IT-samordnare vid varje kompetenscenter

— genomföra säkerhetsanalyser och upprätta förslag till handlingsplan enligt 7 kap. 5 §,

— följa upp att gällande säkerhetsföreskrifter efterlevs och att beslutade säkerhetsåtgärder genomförs,

— ta emot och förmedla rapporter om säkerhetsincidenter och andra säkerhetsrelaterade händelser i enlighet med föreskrift,

— svara för information och utbildning i informationssäkerhet inom kompetenscentret,

— följa upp att datasystemen används i enlighet med föreskrivna ändamål,

— lämna stöd och hjälp till datoranvändare i samband med inträffade säkerhetsincidenter för förhindrande av upprepning,

— genomföra sådan kontroll av logg som anges i 6 kap. 5 §.

5 § Säkerhetschefen ansvarar i samråd med chefen för kompetenscenter IT för förslag till särskilda skydds- och säkerhetsföreskrifter för verksamhet-

[2] Ändringen innebär bl.a. att de nuvarande första och sista strecksatserna utgår.

en vid kompetenscentret samt för uppföljning och aktualisering av dessa föreskrifter, vilka även skall innefatta bestämmelser om säkerhet i driften av datasystem i Tullverkets nät.

7 §[3] Kompetenscenter IT skall upprätta planer för periodiskt förebyggande underhåll av de tekniska installationerna i Tullverkets lokala datorrum. Med lokala datorrum avses rum i vilka förutom datorer och tillhörande kommunikationsutrustning installerats klimatanläggning, avbrottsfri kraft (UPS), drifts- och inbrottslarm m.m.

8 § För systemutveckling skall användas en systemutvecklingsmetod som skall utarbetas av kompetenscenter Strategisk utveckling i samråd med kompetenscenter IT. I samband med att utvecklingsprojektet påbörjas, skall säkerhetschefen genomföra en sårbarhetsanalys i enlighet med etablerad metod för att identifiera eventuella risker med projektet och — om sådana risker konstateras föreligga — lämna förslag på vilka säkerhetsåtgärder som bör vidtas för att säkra att projektet når sitt mål i rätt tid, till budgeterad kostnad och med en produkt som kvalitetsmässigt svarar mot kraven i projektdirektiven. När utvecklingsarbetet nått tillräckligt långt och senast i samband med utformning av systemets användarkravspecifikation (AKS) skall säkerhetschefen i denna specificera vilka tekniska och administrativa säkerhetskomponenter som bör vara inbyggda i det färdiga systemet.

3 kap.

1 § För Tullverkets drift av verksgemensamma datasystem vid kompetenscenter IT skall finnas en avbrottsplan. Planen skall täcka olika situationer, från kortare avbrott, med för verksamheten lindriga konsekvenser, till rena katastrofsituationer då kompetenscentrets resurser inte räcker för att återuppta datordriften inom den tidsram som i en särskild sårbarhetsanalys angivits som längsta acceptabla avbrottstid.

2 § Säkerhetschefen ansvarar för att avbrottsplanen upprättas och hålls uppdaterad. Kompetenscenter IT skall hålla säkerhetschefen underrättad om sådana förändringar i datormiljön som kan medföra att avbrottsplanen behöver revideras.

3 § En särskild ledningsgrupp skall leda och samordna insatserna i de fall ett avbrott inte kan bemästras inom ramen för den ordinarie drifts- och förvaltningsorganisationens möjligheter och befogenheter. Ledningsgruppen utses av generaltulldirektören genom ett särskilt beslut.

4 § För att lindra följderna av längre avbrott i ett lokalt nätverk, skall en aktuell avbrottsplan finnas. Med längre avbrott avses sådana avbrott som

[3] Ändringen innebär bl.a. att andra stycket upphävs.

chefen för kompetenscenter IT beräknar bli så långvariga att ekonomiska och andra konsekvenser för Tullverket och andra intressenter bedöms bli oacceptabla.

Planen skall upprättas och underhållas av biträdande processägaren för IT-processen i samråd med säkerhetschefen.

5 § Säkerhetschefen ansvarar för att avbrottsplan enligt 1—4 §§ testas och revideras i samråd med chefen för kompetenscenter IT i samband med införande av systemförändringar, ny teknik, förändrad organisation o.d.

5 kap.

4 § Med beslut om behörighet avses såväl beslut att ge behörighet till åtkomst och användning av ett eller flera delsystem inom det verksgemensamma datasystemet, som beslut att återkalla sådan tidigare tilldelad behörighet.

Generaltulldirektören får besluta om behörighet för egen del och för underställd personal inom Tullverket.

Vid huvudkontoret får processägare och chef för stabsfunktion besluta om behörighet för egen del och för underställd personal.

Inom ett kompetenscenter får kompetenscenterchefen besluta om behörighet för egen del och för annan personal som hör till kompetenscentret.

Rätten att besluta om behörighet kan delegeras till underställd personal i chefsställning.

Allmänna råd till 5 §

Åtgärden att för en tid dra in behörighet är en administrativ åtgärd för att upprätthålla säkerheten. Det kan finnas skäl att vidta ytterligare åtgärder, såsom information och utbildning, innan det kan bli aktuellt att återge behörigheten. Allvarligare fall av misskötsel kan leda till att den anställde omplaceras till andra arbetsuppgifter eller till att ärendet tas upp i personalansvarsnämnden, vilket kan leda till att den anställde skiljs från sin anställning i Tullverket.

6 § Processägaren för IT-processen eller den underordnade chef som han utser får temporärt tilldela extern personal, t.ex. en konsult, behörighet till ett produktionsregister, om det är nödvändigt för avhjälpande av fel eller brist i något av Tullverkets datasystem eller i centrala driftsmiljön.

Behörigheten skall så långt möjligt begränsas till viss fil, visst register eller program. Tillgång till funktioner på operativsystemnivå eller tillgång till allmänna funktioner i nätverket skall vara begränsad till nivå som motiveras av aktuellt uppdrag och som rekommenderas av berörd delprocessägare vid kompetenscenter IT, vilken svarar för att anlitad konsult är insatt i de säkerhetsregler som gäller för aktuellt uppdrag och för att behörigheten omedelbart tas bort efter att konsulten avslutat sitt uppdrag.

7 § Ärenden om användares behörighet till de verksgemensamma informationssystemen skall handläggas av kompetenscenter Administration genom en behörighetsadministratör eller ersättare för denne. Som behörighetsadministratör eller ersättare för sådan kan utses även tjänsteman med

annan placering än vid kompetenscenter Administration. Sådan tjänsteman är i frågor avseende behörighetsadministration underställd kompetenscenter Administration.

Behörighetsadministratör skall

— vid behov informera användare om gällande regler och rutiner för behörighetsadministration,

— tillse att ansökan med begäran om behörighet är rätt ifylld och undertecknad av användaren,

— ombesörja att begärd behörighet i Tullverkets verksgemensamma datasystem med delsystem förmedlas till kompetenscenter IT,

— ansvara för att begärd behörighet beslutas i vederbörlig ordning och att beslutshandling arkiveras,

— vara kontaktman mot kompetenscenter IT och mot respektive systemförvaltning i frågor om behörighet,

— såvitt angår eget ansvarsområde regelbundet och minst en gång per år kontrollera att register över användare och behörighet är aktuella.

Det är ett gemensamt ansvar för alla processer att se till att erforderliga resurser avsätts för behörighetsadministrationen.

9 § Varje chef ansvarar för att uppgift lämnas till behörighetsadministratör om underställd tjänsteman till följd av ändrade arbetsuppgifter bör ha ändrad behörighet eller att behörigheten skall upphöra på grund av att tjänstemannen slutar sin anställning eller av annan anledning.

12 § Av 2 § förordningen (1958:272) om tjänstekort framgår att Tullverket har behörighet att utfärda tjänstekort för personal i Tullverkets tjänst. Ärenden om utfärdande av tjänstekort och ID-kort skall handläggas av kompetenscenter Administration genom särskilt utsedda kortadministratörer eller ersättare för dessa. Som kortadministratör eller ersättare för sådan kan utses även tjänsteman med annan placering än vid kompetenscenter Administration. Sådan tjänsteman är i frågor avseende utfärdande av kort underställd kompetenscenter Administration.

Bestämmelser om allterminalkort meddelas i särskild ordning.

Det är ett gemensamt ansvar för alla processer att se till att erforderliga resurser avsätts för kortadministrationen.

13 § Inför den första inloggningen i verksgemensamma datasystem skall användaren tilldelas ett initialt lösenord av i 12 § nämnd kortadministratör eller av driftsenheten vid kompetenscenter IT. Detta lösenord får endast användas för byte till ett eget lösenord, vilket inte får meddelas till någon annan. Lösenordet skall ha den sammansättning som anges i den behörighetshandbok som avses i 2 §.

Lösenord skall bytas om misstanke föreligger att det kommit till någon annans kännedom.

6 kap.

1 § Verksgemensamma datasystem skall vara försedda med en *säkerhetslogg* som om möjligt minst skall registrera

— datum och klockslag för in- och utloggning,

— användaridentitet,

— säkerhetsrelaterade händelser enligt specifikation upprättad av systemägaren i samråd med säkerhetschefen,

— registrering och avregistrering av behörighet.

Säkerhetsloggar skall arkiveras i minst 2 år.

2 § Transaktioner i Tullverkets informationssystem skall loggas i en *transaktionslogg* om databehandlingen avser

— listning eller sammanställning av uppgifter om företags eller enskilds import eller export om uppgifterna kan vara föremål för sekretess enligt 9 kap. sekretesslagen (1980:100),

— registrering, ändring eller fråga om sådana spärrar om vilka föreskrivs i Tullverkets föreskrifter och allmänna råd (TFS 1998:9) om spärrar i tulldatasystemet,

— registrering av och ändring i uppgifter i de verksgemensamma informationssystemens behörighetskontrollsystem.

5 § Befattningshavare enligt 5 kap. 4 § får med hjälp av uppgifter i logg stickprovsvis eller på förekommen anledning låta kontrollera användningen av de verksgemensamma informationssystemen. När det gäller Tullverkets register i brottsbekämpande verksamhet skall stickprovsvis kontroll göras minst en gång per år. Rapport med redovisning av gjorda iakttagelser skall redovisas till säkerhetschefen.

Säkerhetschefen får på eget initiativ företa sådan kontroll som anges i första stycket.

Loggutdrag skall beställas genom Tullverkets säkerhetschef från kompetenscenter IT respektive, i fråga om vissa register i brottsbekämpande verksamhet, från Rikspolisstyrelsens informationssäkerhetsenhet.

7 § De standardinställningar i allterminalens programvaror som gjorts i enlighet med kompetenscenter IT:s anvisningar får inte ändras av tjänsteman annat än efter medgivande från kompetenscentrets driftsenhet.

7 kap.

1 § Datamedia som innehåller uppgifter i något av Tullverkets verksgemensamma datasystem skall förvaras i datamediaskåp av lägst klass 120D och vara märkta enligt en metod som godkänts av säkerhetschefen.

Sekretessbelagd information på diskett eller annat flyttbart medium eller på hårddisk skall vara krypterad om den medförs i dator, i handbagage eller transporteras på annat sätt.

3 § Vid bedömning av vilket skydd som behövs för olika slags information, skall den som hanterar informationen ta hänsyn dels till sekretesskrav enligt sekretesslagen (1980:100), dels till det värde informationen har för verksamheten samt den skada som kan bli följden om informationen förloras eller röjs för obehörig.

4 § Tulltjänsteman som misstänker försök till dataintrång, förekomst av datavirus eller annat hot mot informationssystem eller brist däri, skall omgående rapportera detta tjänstevägen till kompetenscenter IT:s driftsenhet, som skall vidarebefordra rapporten till säkerhetschefen samt till befattningshavare vid kompetenscentret i enlighet med intern instruktion. Detsamma gäller rapportering av generella hot mot samhällets informationssystem som kommer till tjänstemans kännedom och som skulle kunna utgöra ett hot även mot Tullverkets informationssystem.

Rapport som meddelats muntligt eller per telefon skall kompletteras med en skriftlig rapport (per post, telefax eller e-post) om detta inte är uppenbart obehövligt med hänsyn till omständigheterna i det enskilda fallet.

Allmänna råd till 5 §

Målet för en säkerhetsanalys är att utröna vilken säkerhetsnivå som föreligger inom ett visst avgränsat område, vilka brister som måste åtgärdas och i vilken prioriteringsordning detta bör ske. En säkerhetsanalys kan utföras på olika sätt beroende på storlek och omfattning på det system eller den verksamhet som skall analyseras. Det är vanligt att man i mindre och avgränsad verksamhet — t.ex. lokala PC-tillämpningar — använder *checklistor* för att identifiera brister i dessa och *scenarioteknik* vid analys av större och mer komplicerade system.

Följande enkla ”scenariometod” torde räcka som hjälpmedel i arbetet med att nå fullgod informationssäkerhet i de flesta datormiljöer i Tullverket. Analysen bör genomföras som grupparbete under ledning av säkerhetschefen eller lokal IT-samordnare. Det är viktigt att det bland deltagarna finns dels tjänstemän som är väl insatta i olika sidor av Tullverkets verksamhet både på lednings- och handläggarnivå, dels sådana som är väl insatta i verkets IT-verksamhet.

1. Identifiera hot, dvs. negativa händelser som kan inträffa (och som kanske har inträffat) och behandla ett hot/en händelse i taget enligt nedan.
2. Identifiera brist som gör händelsen möjlig.
3. Bedöm risken för att händelsen skall inträffa.
4. Bedöm ekonomiska och andra konsekvenser av händelsen.
5. Identifiera tänkbar åtgärd för att eliminera hotet eller minska risken.
6. Bestäm med ledning av risk- och konsekvensanalys enligt p. 3 och 4 hur åtgärden skall prioriteras.
7. Upprätta och fastställ en handlingsplan med förteckning över säkerhetshöjande åtgärder med uppgifter för varje åtgärd om
   — prioritet,
   — beräknad kostnad,
   — om och när den skall vara genomförd,
   — vem som ansvarar för genomförandet.

Befattningshavare enligt 5 kap. 4 § bör återkommande följa upp att åtgärderna i handlingsplanerna vidtas. Planerna bör ligga till grund för Tullverkets budget för informationssäkerhet.

8 kap.

1 § Innan ett dataprogram eller annan systemkomponent får användas i allterminal skall produkten evalueras och certifieras. Detta gäller oavsett om det rör sig om ett informationssystem, ett delsystem till detta eller om produkten är egenutvecklad eller inköpt. Chefen för kompetenscenter IT kan medge undantag från kravet på evaluering och certifiering om det är uppenbart att produkten inte kan påverka funktioner i Tullverkets IT-miljö.

2 § Evaluering skall ske vid kompetenscenter IT. Över evalueringen skall upprättas protokoll i vilket bl.a. skall framgå i vilken grad egenskaper som identifierats i evalueringsprocessen stämmer överens med krav i kravspecifikation eller deklarerade egenskaper i annan dokumentation.

Av protokollet över evaluering skall framgå vem som är ägare av evaluerat system — systemägare — och vem som i förekommande fall är betalningsansvarig för licensavgifter och avgifter för uppgradering av till Tullverket inköpta programvaror eller andra systemkomponenter.

3 § Certifiering beslutas av kompetenscenter IT, varvid protokoll från evalueringen skall ligga till grund för beslutet.

9 kap.

Allmänna råd till 2 §

Med dagens omfattande användning av Internet och utväxling av information på disketter och andra datamedia, är risken stor att man förr eller senare drabbas av datavirus. Antalet virus ökar stadigt och man skall vara medveten om att installerad antivirusprogramvara bara skyddar mot kända virus. Effekterna av virusangrepp kan vara allvarliga med i värsta fall förlorad eller förvanskad information, även om farligheten ofta överdrivs.

Det är särskilt viktigt att inte virus sprids av pc-användare i Tullverket till externa mottagare, t.ex. till företag eller enskilda som är föremål för tullrevision eller annan myndighetsutövning.

För att undvika datavirus bör man

— aldrig använda piratkopior av program (vilket dessutom är förbjudet i lag),

— viruskontrollera disketter som kommer utifrån, särskilt sådana med okänt ursprung,

— undvika spelprogram och demonstrationsprogram från okända leverantörer,

— om man använder fristående pc: alltid använda originalprogram och sköta säkerhetskopieringen så att man har en oskadad kopia av informationen, förvarad åtskild från egen miljö,

— regelbundet testa att informationen kan återskapas från säkerhetskopiorna.

Olika tecken på smitta:

— filer blir större,

— olika texter och symboler kommer upp på skärmen,

— texten faller till botten,

— det går långsamt att starta datorn,

— datorn blir ”slö”,

— vissa tecken försvinner eller förändras,

— all information på disken försvinner.

Lämpliga åtgärder vid virussmitta:

— stäng av och isolera utrustning som drabbats,

— underrätta kompetenscenter IT:s driftsenhet,

— underrätta alla som berörs och antas beröras, även externa intressenter,

— underrätta IT-samordnare eller annan som kan hjälpa till med sanering av smittade datorer,

— försök fastställa när och på vilket sätt smittan kan ha skett,

— försök fastställa när senaste programladdning skett,

— sanera alla disketter och hårddiskar som smittats,

— återstarta med garanterat smittfria programdisketter,

— dokumentera hela händelseförloppet och sänd en kopia till säkerhetschefen.

10 kap.

Allmänna råd till 1 §[4]

Den som har ansvar för säkerheten vid användning av en pc bör

— fortlöpande tillse att datorn är i driftsdugligt skick,

— förteckna de program och versioner av dessa som installerats i datorn,

— kontrollera att datorn och viktiga komponenter i denna är vederbörligen stöldskyddsmärkta,

— tillse att disketter och andra datamedia märks, förtecknas och förvaras stöld- och brandsäkert när de inte används,

— se till att datamedia eller utdata som innehåller eller kan innehålla sekretesskänslig eller av annan anledning skyddsvärd information inte kommer i orätta händer eller förloras i samband med transport eller annan hantering,

— tillse att hårddisk avlägsnas innan dator lämnas till service, säljs eller skrotas,

— förstöra disketter som kan innehålla sekretessbelagd information som inte längre behövs i tjänsten,

— ansvara för att datorn är försedd med programvara för virusskydd i enlighet med kompetenscenter IT:s rekommendation, samt

— rapportera eventuell förekomst av datavirus eller andra säkerhetsincidenter i enlighet med 7 kap. 4 §.

2 § Av tulltjänsteman privat disponerad persondator får inte användas för bearbetning i tjänsten av sekretessbelagd information.

Processägare, chef för stabsfunktion vid huvudkontoret och chef för kompetenscenter får i samråd med säkerhetschefen i enskilt fall medge undantag från första stycket, om det finns särskilda skäl.

[4] Ändringen innebär bl.a. att sista strecksatsen tas bort.

11 kap.

Uttag av uppgifter ur tulldatasystemet (TDS) för vidare bearbetning

1 § Uppgifter ur tulldatasystemet (TDS) får kopieras till datamedium för vidare bearbetning, om det är förenligt med ändamål som beskrivs i 1 kap. 4 eller 5 § lagen (2001:185) om behandling av uppgifter i Tullverkets verksamhet. Kopiering skall beställas skriftligen hos sakansvarigt kompetenscenter.

Vid behandling av personuppgifter som inte sker i databasen gäller även 22 § personuppgiftslagen (1998:204).

Kopiering får ske på diskett som postas till beställaren eller via datakommunikation direkt för mellanlagring till datafil som disponeras av beställaren. Om kopiering skett till diskett skall denna assureras vid postbefordran.

Allmänna råd

Ändamålen med tulldatabasen framgår av lagen (2001:185) om behandling av uppgifter i Tullverkets verksamhet. Enligt 1 kap. 4 § 2 och 2 kap. får uppgifter behandlas i databasen för tillhandahållande av information som behövs hos Tullverket för övervakning, revision och annan analys- eller kontrollverksamhet.

Det kan i vissa lägen vara svårt att skilja dessa uppgifter från spanings- och underrättelsetjänst, t.ex. ”registerspaning” och annan underrättelseinhämtning. Särskilt gäller det användningen av Efterkontrollsystemet, vilket kan innehålla uppgifter som skulle kunna vara värdefulla för underrättelseverksamhet inom tullbrottsbekämpningens område men som alltså inte får användas för det ändamålet.

Även ”samkörning” med andra register eller systematisering av registeruppgifter i syfte att ta fram underlag som kan ge stöd för misstanke om brott strider mot föreskriften i lagen om behandling av uppgifter i Tullverkets verksamhet om ändamålet med behandlingen.

Däremot får det anses tillåtet att med hjälp av TDS inhämta uppgifter ur ett ärende i samband med en redan inledd förundersökning avseende detta ärende, jfr prop. 1989/90:40 s. 19.

Tjänsteman som tagit ut uppgifter ur TDS eller annat register med sekretessbelagt innehåll i enlighet med paragrafen bör vara medveten om att uppgifterna behåller sin sekretess oavsett vilket medium de förts över till.

2 § För kopiering enligt 1 § gäller följande

— behörighet att beställa kopierade uppgifter får tilldelas tjänsteman (nedan nämnd beställare) som förordnats att utföra tullrevision, tjänsteman med uppgifter i riskanalys samt tjänsteman som är verksam med att lämna uppgifter inom verksamheten för kontroll, revision och övervakning till utländsk tullmyndighet i enlighet med avtal om ömsesidigt tullsamarbete,

— överföring av uppgifter ur TDS för mellanlagring i dator i Tullverkets nät får endast ske till skriv- och lässkyddat utrymme som enbart beställaren och den tjänsteman vid kompetenscenter IT som levererar beställda uppgifter har tillgång till,

— beställning av överföring skall vara skriftlig och undertecknad av den som enligt 21 kap. 13 § Tullverkets föreskrifter och allmänna råd

(TFS 2000:20) om tullförfaranden m.m. (tullordning) får besluta om tullrevision eller av riskanalyschefen vid kompetenscenter Företag,

— uppgift om utförd överföring skall loggas med uppgifter om beställare, slag av uppgifter, namn och organisationsnummer på företag som är föremål för kontrollåtgärd samt datum och tid när beställning effektuerats,

— överförda uppgifter skall raderas omedelbart efter att beställaren kopierat uppgifterna till den egna datafilen, dock senast efter tre kalenderdygn, oavsett om beställaren kopierat överförda uppgifter eller inte.

5 § Telefax får användas för förmedling av sekretesskyddad information om det enligt avsändarens bedömning i det enskilda fallet kan ske utan risk för att informationen kan komma obehörig till del. Faxning av uppgifter som faller under 2 kap. 2 § sekretesslagen (1980:100) (sekretess till skydd för rikets säkerhet) får endast ske krypterat.

Sekretesskyddad information i klartext får förmedlas som e-post endast internt inom Tullverket.

All försändning med e-post av sekretessbelagd information till mottagare utom Tullverkets nät skall krypteras.

Allmänna råd

Det är tämligen vanligt att telefaxmeddelanden kommer till fel abonnent. Även om det kommer till rätt abonnentnummer, finns alltid risken att meddelandet läses där av någon som inte är behörig.

För att minska risken för felsändning till mottagare som man ofta sänder sekretesskänslig information till, bör man i första hand använda s.k. kryptofax eller, om sådan inte finns, förprogrammera faxnummer. En annan säkerhetsåtgärd är att ringa upp mottagaren och förvissa sig att rätt person tar emot meddelandet (s.k. kontrollerad faxning).

Mycket känslig information, t.ex. underrättelser om misstänkt grov smuggling, grov narkotikasmuggling eller grovt tullbrott, eller uppgifter om enskilds ekonomiska förhållanden enligt 8 eller 9 kap. sekretesslagen och som av handläggaren klassas mycket sekretesskänsliga, bör inte faxas utan förmedlas på ett säkrare sätt, t.ex. via assurerad eller rekommenderad post, kryptofax eller krypterad datakommunikation.

Användning av e-post för förmedling av okrypterad information i Tullverkets nät är säkrare än telefax. Meddelanden med mycket känslig information om misstänkt brott, såsom uppgifter i Tullverkets register i den brottsbekämpande verksamheten samt uppgifter för vilka gäller sekretess enligt 2 kap. sekretesslagen, bör dock krypteras även vid försändning med e-post internt inom Tullverket.

7 § Datakommunikation med uppgifter i register som förs med stöd av lagen (2001:85) om behandling av personuppgifter i Tullverkets brottsbekämpande verksamhet skall vara krypterad i enlighet med specifikation för allterminalen, såväl i Tullverkets gemensamma nät (Wide Area Network, "WAN") som i varje lokalt nätverk.

Beskrivning av krypteringsteknik och administration av kryptonycklar m.m. skall framgå av den behörighetshandbok som avses i 5 kap. 2 §.

Denna författning träder i kraft den 1 juni 2005.

TULLVERKET

KARIN STARRIN

Torgny Johansson
(Rättssekretariatet)