UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF TEXAS

Entered September 12, 1997

In the Matter of Computing Resources §§
Acceptable Use and Security Handbook §§ General Order No. 1997-7

ORDER

The attached *Computing Resources Acceptable Use and Security Handbook* is adopted, and employees of the Clerk, Probation and Pretrial Services shall be required to sign the User Memorandum of Agreement.

Signed this 12th day of September, 1997.

/s/
George P. Kazen
Chief United States District Judge

UNITED STATES COURTS

SOUTHERN DISTRICT OF TEXAS

Computing Resources Acceptable Use and Security Handbook

United States Courts

Southern District of Texas

Computing Resources Acceptable Use and Security

I. Introduction.

The networked computing environment provided to employees and officers of the United States Courts in the Southern District of Texas is intended to encourage the efficient use of court resources. To achieve this, the computers must provide consistently high-quality and cost-effective information and communication resources. The following policy should be followed carefully to ensure the safety and continued availability of these resources.

II. Purpose.

This Acceptable Use Policy will provide guidance for the use of computing resources by Court employees.

III. Scope.

This policy applies to all Court employees and officers who use the computing resources in the performance of their jobs.

IV. What Users Should Know.

There are several avenues through which the security and propriety of Court functions could be compromised through the use of computing resources. This Policy will address the procedures that must be used to protect against such a danger. Users should be aware of the ways in which problems could arise.

A. Desktop Terminals -- Every terminal or personal computer used for the work of the Courts can be used to compromise system integrity. An unattended work station can be used quickly to copy or destroy data or to damage a reputation.
This applies to laptop computers as well.

B. Software -- Computer programs and documents are often protected by copyright laws. Unauthorized installation of software may invoke civil or criminal penalties. In addition, certain programs may interfere with the normal operation of a computer or network, either through internal compatibility problems or through viruses.

C. Modems -- All computers equipped with modems offer a potential means by which unauthorized personnel could gain access to Court computing resources.

D. Network Connections -- Any personal computer connected to

a network is vulnerable to use by others with a connection to that network. In particular. shared resources such as common disk drives and database servers may be vulnerable. Communications over network connections, including email and file transfers, especially when transmitted to or from locations outside of the Southern District of Texas network, may be observed or copied without the knowledge of the person sending the email or initiating the file transfer. Any problems, such as computer viruses, introduced to a workstation connected to the network, could quickly affect every other computer connected to that network.

E. The Internet -- The Internet is an informal collection of government, military, commercial. and educational computer networks. It is essential that users understand some of the limitations of the Internet, the World Wide Web and the Internet e-mail system including security and delivery of an email message.

The Internet is an unsecured network. As such, information and email on the Internet can be read, broadcasted, or published without the knowledge or consent of the author. Users should be aware that cc:Mail is converted to email and may be sent via the Internet. Consequently, cc:Mail should be treated with the same precautions as email. Most sites maintain records of all users or entities accessing their resources. These records may be open to inspection and publication without the users knowledge or consent. If the activity of the user is other than official business, the publication of that activity could prove to be an embarrassment for the Court and the entire federal Judiciary.

Resources available on the Internet and World Wide Web should be carefully checked for reliability. In particular. software downloaded from the Internet could carry viruses or may have been distributed without the permission of the copyright owner.

V. Information Security.

There are three levels of security that should be observed when dealing with printed or electronic security within the Courts.

A. Public -- Some information is public by statute, and may be made available to the public providing that procedural guidelines particular to that information are followed. Examples of such information are unsealed case files and docketing information. Such information may be maintained unencrypted on Court computing resources provided that all original and official copies are

maintained safe from unauthorized changes.

B. Proprietary -- Some information is not public by statute, and should only be made available to the public under court order or by permission of an authorized supervisor. Such information includes internal procedure manuals. and certain financial information. This information should not be sent outside of the Court offices via email or file transfers, but may be maintained unencrypted on Court computing resources provided that all original and official copies are maintained safe from unauthorized changes.

C. Sealed -- Some information is protected by Court or statute from disclosure to any person other than employees and officers of the United States in the performance of their official duties. Examples include grand jury proceedings and probation and pretrial officer files. Such information should be maintained on Court computing resources only in encrypted form. Keys that allow decryption of such information should be available only to those who require such access in performance of official duties as allowed by statute or Court Order.

VI. Passwords.

Passwords and usernames will be used in a variety of ways on Court Computing Resources. Access to desktop and file server computers will be restricted by passwords. Decryption of **Sealed** information will also require a password or set of passwords.

A. Length and Composition -- All passwords shall be at least eight (8) characters long and shall include a combination of letters and other characters (punctuation marks and numbers). Names and actual words should not appear in passwords.

B. Security -- All persons using passwords should commit those passwords to memory. In no event should passwords be recorded on paper and left in an accessible place. Passwords are to be kept confidential and should not be shared with employees in the office or with individuals outside the office.

C. Creation and Maintenance -- In some agencies. passwords will be provided by the automation department. In others. employees will be allowed to choose passwords that conform to this Policy. In all cases, passwords must be changed at least once every three (3) months. Most court systems will require these regular changes through processes that track age of passwords. Passwords may not be reused. If an agency allows an employee to

choose a password for a Computing Resource, the chosen password must be different from passwords used for other Computing Resources.

VII. Acceptable Use and Security of Desktop Computing Resources.

These policies and procedures apply to laptop computers as well as desktop computers.

A. Preventing Unauthorized Access --

1. All desktop computers should require a password to initiate access.
2. All monitors should be protected from observation by unauthorized individuals.
3. Printers and printed output should be protected from observation by unauthorized individuals.
4. In no event shall a computer or terminal remain logged in and active when unattended.
5. All removable media should be protected from unauthorized access through safe storage.
6. People who do not belong in an area should be politely challenged and assisted. Any suspected unauthorized access should be reported to the automation department.

B. Protection From Viruses --

1. All Court desktop and laptop computers will run virus scanning software approved by the automation department.
2. No unauthorized software may be installed to Court Computing Resources. Automation department staff must always be notified before new software is installed.
3. All important files should be backed up regularly to tape, diskette or other removable media.
4. Any suspected virus infections must be reported to automation department staff immediately. Common symptoms of such infections include disappearing files, unaccountable file copies, unaccountable new files, changed or corrupted data, reduced disk space or memory, slow or frozen computer activity, strange messages, odd screen activity (screen color changes, balls bouncing about, characters dripping down screen, etc.), unexpected reboots, unexplained disk drive activity and changes in program lengths or time stamps.

C. Acceptable Use -- Desktop and laptop computers should only be used for activities within the scope of normal Court operations. The following activities shall be prohibited uses of Court desktop computing resources:

1. composing or printing unauthorized statements regarding agency policies or practices;
2. making unauthorized copies of copyrighted software,
3. installation of software without authorization from automation department staff.

D. Protection from Physical Damage and Theft -- Desktop and laptop computers are often quite fragile, and care should be taken to maintain these expensive resources in good working condition.

1. do not place food or drinks on or near keyboards, computers or monitors, and avoid dropping crumbs or other foreign substances onto them.
2. protect keyboards. computers and monitors from dirt and dust with a cover approved by automation department staff, particularly when construction, moving or similar dust-producing activities are taking place nearby;
3. use a surge protector, uninterruptable power supply or similar power line filter;
4. avoid areas susceptible to water damage;
5. keep magnets, such as those in speakers and telephones, away from computer monitors, diskettes, hard disks and backup tapes;
6. maintain laptop computers in secure locations whenever they are not in use.

E. Data Protection -- All network drives are backed up on a regular basis. Any important data stored on a desktop or laptop computer's hard drive (C: or D:) should also be regularly backed up to a network drive, a tape or a diskette. Any backup media that contain Proprietary or Sealed material as defined in V., above, must be maintained in a secure location. Any questions about how to make backups, should be directed to automation staff.

F. Access to Desktop Computers -- Desktop computers may be used only by those individuals to whom they have been assigned, or by the supervisors of those individuals. In the course of system maintenance, automation personnel may also gain access to desktop or laptop computers. Anyone using court computing resources expressly consents to such monitoring and is advised that if such monitoring reveals possible evidence of criminal activity, automation personnel may provide the evidence of such monitoring to law enforcement officials.

VIII. Acceptable Use and Security of Telephonic Computing Resources.

Certain employees and officers of the Court shall be supplied with modems with which to connect to resources outside of the

Court, or through which to gain access to Court Computing Resources from outside of the offices of the Court.

A. Preventing Unauthorized Access --

1. Except when specifically authorized by the automation department, no modem may be used to connect a computer within the Court offices to a computer network external to the Courts. In particular, dial-up network connections (establishing an Internet node using a protocol such as PPP or SLIP) to commercially operated Internet Services shall only be allowed by explicit permission of automation personnel.
2. If a computer is equipped with software that allows a user to dial in from outside the off-ices of the Court (e.g., PC Anywhere), password controls must be in place to prevent unauthorized access.
3. A computer equipped with software that allows a user to dial in from outside the offices of the Court (e.g., PC Anywhere) may not remain connected to court networks while that software is running.

B. Protection From Viruses -- No program or other file may be downloaded from a site outside of the Courts without explicit permission of automation personnel. Files downloaded from Court-operated bulletin board systems should be checked using virus-scanning software before execution.

C. Acceptable Use -- Modems should only be used for activities within the scope of normal Court operations. The following activities shall be prohibited uses of Court telephonic computing resources:

1. transmitting unauthorized statements regarding agency policies or practices;
2. transmitting unauthorized copies of copyrighted software.

D. Access to Telephonic Computer Resources -- Court telephonic computing resources may be used only by those individuals to whom they have been assigned, or by the supervisors of those individuals. In the course of system maintenance, automation personnel may also gain access to or log the use of telephonic computing resources. Anyone using court computing resources expressly consents to such monitoring and is advised that if such monitoring reveals possible evidence of criminal activity, automation personnel may provide the evidence of such monitoring to law enforcement officials.

IX. Acceptable Use and Security of Network Connections.

Most computers and terminals in the Courts are connected by some means to Court-operated computer networks.

A. Preventing Unauthorized Access -- As long as security procedures to prevent unauthorized access to desktop computing and modem resources (VII.A and VIII.A) are followed, network security concerns will primarily be about external access. Users should follow all procedures to protect passwords (VI). In addition, the following procedures will be followed:

   1. Web browsers must not be set to allow Java or similar programs to run automatically.
   2. "Cookie's" should not be accepted from web sites that might be insecure.

B. Protection From Viruses --

   1. All Court-operated networks will run virus scanning software approved by the automation department.
   2. Web browsers must not be set to allow Java. ActiveX or similar programs to run automatically.
   3. No program or other file may be downloaded from a site outside of the Courts without explicit permission of automation personnel. Files downloaded from Court-operated bulletin board systems should be checked using virus-scanning software before execution.

C. Acceptable Use -- All employees and officers are expected to use the Court's network connections in a professional manner that will reflect positively on them and on the Court. Networked computing resources should only be used for activity within the scope of normal Court operations. The following activities shall be prohibited uses of Court network connections:

   1. distribution of unauthorized statements regarding agency policies or practices;
   2. making unauthorized commitments or promises that might be perceived as binding on the Court or an agency thereof,
   3. transmitting confidential information, except as required for the performance of official duties;
   4. making or distributing unauthorized copies of copyrighted software;
   5. using the network connection for commercial purposes or private gain;
   6. playing games that consume network resources;
   7. using the network for illegal activities.

D. Access to Court Networks --Court networks are for the use of authorized users only. Individuals using court

network resources without authority, or in excess of their authority, are subject to having all of their email activities on these systems monitored and recorded by automation personnel. In the course of monitoring individuals improperly using this system, or in the course of system maintenance, the activities of authorized users may also be monitored. Anyone using this system expressly consents to such monitoring and is advised that if such monitoring reveals possible evidence of criminal activity, automation personnel may provide the evidence of such monitoring to law enforcement officials.

X. Internet Use

The Internet, including the World Wide Web, email, and other protocols, offers many useful resources to the Court. All installation of software for accessing the Internet must be approved by a supervisor in consultation with automation support personnel. The following policy shall govern use of these resources from Court resources.

A. Preventing Unauthorized Access -- The policy outlined above for desktop computing resources, modems and network connections shall apply to all use of the Internet. In addition, no unencrypted **Proprietary** or **Sealed** information, as defined in V, above, may be transmitted across the Internet via email or other transfer protocol.

B. Protection from Viruses -- The policies and procedures governing network connections as discussed in IX.B shall apply to Internet use.

C. Acceptable Use -- The Internet should only be used for activities within the scope of normal Court operations. The following activities shall be prohibited uses of the Internet from Court computing resources:

1. distributing unauthorized statements regarding agency policies or practices;
2. transmitting confidential information, except as required for the performance of official duties;
3. making unauthorized commitments or promises that might be perceived as binding on the government;
4. using subscription accounts or commercial services that are not expressly authorized,
5. hosting an unauthorized web site;
6. sending or displaying messages or pictures that are of an obscene or sexually explicit nature as defined in Miller v. California 4113 U.S. 15, 23 (1972) (material that "appeals to the prurient interest" (that is, is designed to produce sexual stimulation), is "patently offensive" to

"contemporary community standards," and lacks "serious literary, artistic, political, or scientific value.");

7. using the network connection for commercial purposes or private gain.
8. making or distributing unauthorized copies of copyrighted software, images or text;
9. using the network for illegal activities.

D. Access to the Internet -- Only those individuals who have received approval from supervisors may use court computing resources to gain access to the Internet. In the course of system maintenance, automation personnel will log the use of the Internet through court computing resources. Anyone using court computing resources expressly consents to such monitoring and is advised that if such monitoring reveals possible evidence of criminal activity, automation personnel may provide the evidence of such monitoring to law enforcement officials.

XI. Email

Court employees will have access to email for dissemination of information, communications among the courts and operations-related communications with the public. The following policies should guide use of email within the Court:

A. Records Maintenance -- While the Judiciary is not governed by the Freedom of Information Act, certain statutes and policies strictly govern the maintenance of records. Any official business conducted through email could be subject to these statutes and policies, as outlined in Information Resources Bulletin 97-14, May 19, 1997. Each Court unit will outline those email messages that must be maintained in accordance with statutes and established procedure, as well as the means by which such messages should be maintained. See your supervisor for those issues about which you should know.

B. Protection from Viruses -- Executable program files may be attached to email messages. No such file should be executed on Court computing resources except as authorized by automation staff.

C. Acceptable Use -- Email should not be considered a confidential medium for communication, particularly with the Internet. Employees and officers are expected to use email to communicate in a professional manner that will reflect positively on them and on the Court. The

following uses of email are prohibited:

1. distributing unauthorized statements regarding agency policies or practices;
2. transmitting confidential information, except as required for the performance of official duties;
3. using email for commercial purposes or private gain;
4. distributing unauthorized copies of copyrighted software, images or text.

D. Access to the Email -- Email is for authorized users only. Individuals using emai1 on court computing resources without authority, or in excess of their authority, are subject to having all of their email activities on these systems monitored and recorded by automation personnel. In the course of monitoring individuals improperly using this system, or in the course of system maintenance, the activities of authorized users may also be monitored. Anyone using this system expressly consents to such monitoring and is advised that if such monitoring reveals possible evidence of criminal activity, automation personnel may provide the evidence of such monitoring to law enforcement officials.

XII. Definitions.

Court Computing Resources -- Any computer or terminal belonging to an agency in the Court family shall be considered a Court Computing Resource. Additionally, all removable media, including tapes, diskettes and similar storage media, shall be considered Court Computing Resources. When used in the performance of official duties, computers and media owned by an employee or officer of the Court shall be considered Court Computing Resources subject to this Policy.

Encryption -- Encryption is the encoding of electronic data in such a way as to prevent its perusal or use by those who lack the necessary means of access, or "keys." Only encryption algorithms and programs approved by the automation departments of the Court shall be used on Court Computing Resources. Users of court computing resources may only use encryption in those instances and for those purposes expressly authorized by their supervisors.

Network -- A network is a connection between two or more computers. Networks can be established using telephone lines or specially designed wires and "hubs." Computers on a network can share resources. such as printers and hard drives, or transmit information

between one another in the form of email or file copies.

Terminal -- A device used to connect to another computer over a network connection. Usually, a terminal consists of a monitor and a keyboard, with a modem or network line attached. Technically, desktop computers can act as terminals, but usually a distinction is made between computers and terminals.

Virus -- The term "virus" is generically used to refer to any malicious computer program, but that classification is quite broad. Technically, viruses are codes that attach themselves to files and, when the files are opened, copy themselves onto other files. "Worms" are programs that copy themselves across networks without being attached to a file. "Phages" are viruses that modify other programs in unauthorized ways. "Mockingbirds" are programs that act like normal system processes in an effort to gain unauthorized information. A "logic bomb" is a code that causes an application or operating system to perform some action when conditions are met. Any of these classes of computer codes can compromise security, corrupt data or even destroy computer hardware. They can be transmitted on executable programs, word processor documents or other seemingly innocuous files. A user may not know that a virus is present until months or years after the infection takes place. Only up-to-date, sophisticated virus detection software can reliably cure and prevent infection by computer viruses.

United States District Court
for the Southern District of Texas
USER MEMORANDUM OF AGREEMENT

As a user of the Judiciary Communications Network, I acknowledge my responsibility to conform to the requirements and conditions established by this document.

1. I understand that failure to sign this acknowledgment will result in denial of access to the Judiciary Network.

2. I understand that the DCN is an unclassified network. I will not introduce, store, pass or process classified data on the network.

3 I understand the policies outlined in this Computer User Handbook and I agree to abide by the Handbook.

4. I understand that I am responsible for all actions taken under my account. I will not attempt to "hack" the judiciary network or any other network or computer on the DCN or attempt to gain access to data for which I am not specifically authorized.

5. I understand that I am responsible for maintaining the current level of security available on my workstation connected to the network.

6. I acknowledge my responsibility to use the Judiciary network ONLY for official government business.

7. I acknowledge my responsibility to ensure that restricted information is not publicly disclosed and to immediately report suspected violations of this regulation.

8. I acknowledge my responsibility to immediately report to the systems office any contact with individuals in which illegal or unauthorized access is sought to sensitive information or when I become concerned that I may be the target of actual or attempted exploitation.

9. I acknowledge my responsibility NOT to download or install executable software from **any** source onto the DCN without prior authorization from management and/or the systems office. I recognize that I must ensure that any files or software I am authorized to receive have been subjected to approved virus protection measures.

10. I understand that all-telecommunications and automated information systems are subject to monitoring to ensure proper functioning, to protect against improper or unauthorized use or access and to verify the presence or performance of applicable security features or procedures, and for like purposes. Such monitoring may result in the acquisition, recording, and analysis of all data being communicated, transmitted, processed or stored in these systems by the user. If monitoring reveals possible evidence of criminal activity, such evidence may be forwarded to law enforcement personnel. I expressly consent to such monitoring. I understand that the systems office is responsible for such monitoring.

11. I understand that I must ensure that all equipment is returned to the court in good condition at the end of my period of employment, and I promise not to take any actions which will jeopardize the security of the system after my departure.

12. I acknowledge my responsibility to conform to the requirements set forth in this agreement, and I will abide by all applicable policies. Failure to comply may result in denial of access to the DCN and that, if necessary, such violations will be reported to the proper authorities.

Name:_____ Court Unit:_____

Telephone Number:_____ Supervisor:_____

Employee's Signature:_____ Date:_____

Supervisor's Signature:_____ Date:_____

cc: Court Unit Systems Manager
Court Unit Personnel Record