SESSION 13

Computer Network Security for Courts

The article titled "*Legacy Systems, Cost Savings, Yes…But the Risk?*"[1] talks about the need to have updated hardware and software technologies and the repercussions which could be faced owing to the facts that the parameters of technological developments have not been met.

"*How to Leverage Networks to Boost Security*"[2] mentions about the several practices which can be implemented for ensuring network security like standardizing network infrastructure, adopting change management practices, compliance awareness.

Third document added in the session is "*Computer Security Policies for the Users in the United States District Court*"[3] enumerates upon the computer security practices to be adhered by the different members of the Court for maintaining the security.

[1] http://courttechbulletin.blogspot.in/2015/07/legacy-systems-cost-savings-yes-but-risk.html
[2] http://gcn.com/articles/2015/07/29/networks-as-security.aspx
[3] https://www.ilnd.uscourts.gov/clerksoffice/CLERKS_OFFICE/lca/pdf/localnet.pdf

LEGACY SYSTEMS, COST SAVINGS, YES… BUT THE RISK?[1]

30 July, 2015, James E. McMillan

Many courts use very old computer software and hardware systems. They save a lot of money doing that; but there are dangers that we discuss below.

I saw an interesting article last week in Government Computer News, July 2015 by author Brian Robinson titled: "What's worse: Living with legacy systems or replacing them". His article was precipitated by the recent hack of the US Government's Office of Personnel Management where millions of employees had their private information stolen. The fact was that those software systems were still running 20 year old COBOL code. And that in turn means that these systems were never designed to either be connected to the Internet or, be secure in that environment. In addition in another article from Ars Technica I learned that even encryption wouldn't have worked because first the systems are too old to support it and additionally that the hackers had gained valid system credentials likely via social engineering.

How many court systems have computer software in that same state? Does your CMS operating system and database support encryption if you wanted to use them? For sensitive juvenile, victim, and financial records such as garnishment orders encryption is a must.

So what is the risk / reward model for maintaining the old systems? If one is in business the risk can be potentially quantified as lost sales and like recent breaches at major retailers, loss of customer trust, and government fines.

For courts there are definitely risks. First, there is the ability or inability to maintain an older system. If one uses outdated languages or operating systems there may not be anyone who can fix something that breaks. Second, as noted above the system may be insecure. And therefore the data stored therein may be accessible. Third, the hardware that the old software runs on may become increasingly hard to obtain. I remember one court who had to buy their printer equipment on eBay because the notice document printing was hard coded for only that type of printer into their ancient system. And fourth there is a serious risk of losing the court's data because storage drives fail and even tape backups can become unusable.

The Department of Homeland Security posted an excellent web page on older systems risks with an assessment list for you to use at:

[1] http://courttechbulletin.blogspot.in/2015/07/legacy-systems-cost-savings-yes-but-risk.html?utm_source=feedburner&utm_medium=email&utm_campaign=Feed:+CourtTechnologyBulletin+(Court+Technology+Bulletin)

https://buildsecurityin.us-cert.gov/articles/best-practices/legacy-systems/assessing-security-risk-in-legacy-systems

So what is your Plan B? Can you replicate your old system on a newer "virtual machine"? At least it is running on newer hardware that can be maintained and replaced?

Is it to go to paper? Obviously this only helps with immediate work and not with the ability to operate as efficiently as with your system? And if your plan is to go to paper, have you tested it to see if this or any other approach works?

Or would you have to close your court? For how long? And can the problem be fixed at all?

It is probably time to think about these things and do your risk assessment?

HOW TO LEVERAGE NETWORKS TO BOOST SECURITY[2]

29 July, 2015, Joel Dolisy[3]

The breach at the Office of Personnel Management has put security top of mind for nearly every government IT manager.

Many agencies are already practicing excellent cyber hygiene; others are still in implementation phases. Regardless of where you are in the process, it is critical to understand that security is not a one-product solution, and it requires constant attention. Having a solid security posture requires a broad range of products, processes and procedures.

Networks, for example, are a critical piece of the security picture; agencies must identify and react to vulnerabilities and threats in real time. By optimizing network performance, you can implement automated, proactive security strategies that will increase network stability and have a profound impact on the efficiency and effectiveness of the overall security of the agency.

How can agencies leverage their networks to enhance security? Below are several practices you can begin to implement today, as well as some areas of caution.

Standardization. Standardizing network infrastructure is an often-overlooked method of enhancing network performance and security.

---

[2] http://gcn.com/articles/2015/07/29/networks-as-security.aspx

[3] Joel Dolisy is CIO at IT management software provider SolarWinds, based in Austin, Texas.

Start by reviewing all network devices and ensure consistency across the board. Next, make sure you've got multiple, well-defined networks. Greater segmentation will provide two benefits: greater security, as access will not necessarily be granted across each unique segment, and greater ability to standardize, as segments can mimic one another to provide enhanced control.

Standardization also allows you to bring new team members up to speed quickly on specifications and provides tighter control when rolling out new implementations and designs. And, finally, standardization reduces configuration errors and automates deployment.

Change management. Good change management practices go a long way toward enhanced security. For example, change management software – specifically, software that requires a minimum of two unique approvals before changes can be implemented – prevents unauthorized changes at any time of day or night, including 2:00 a.m. when an intruder might assume nobody is watching.

In addition, make sure you fully understand the effect changes will have across the infrastructure before granting approval. Analyze and understand, for example, the consequences on the network as a whole in terms of capacity, performance, risk, cost and more.

Configuration database. Once infrastructure is standardized and sound change-management practices are in place, it's important to have a configuration database for backups, disaster recovery, etc. If you have a device failure, being able to recover quickly can be critical; implementing a software setup that can do this automatically can dramatically reduce security risks.

Another security advantage of a configuration database is the ability to scan for security-policy compliance. With all configurations in one location, that otherwise cumbersome task can be far less time consuming and far more efficient.

Compliance awareness. Compliance is one of any agency's primary security concerns – and trying to comply with security technical information guides from the Defense Information Systems Agency, the Federal Information Security Management Act and more can be a complicated business.

That said, increased awareness and, in turn, increased security does not have to be difficult. Consider using a tool that automates vulnerability scanning and FISMA/DISA STIG compliance assessments. Even better? A tool that also automatically sends alerts of new risks by

tying into the National Institute of Standards and Technology vulnerability database, then checking that information against your own configuration database.

Areas of caution

Most security holes are related to inattention to infrastructure. In other words, inaction can be a dangerous choice. Some examples are:

Old inventory. Older network devices inherently have outdated security. Update as often as possible to ensure the newest security features are in place. In fact, invest in a solution that will inventory network devices and include end-of-life and end-of-support information. This also helps forecast costs for new devices before they quit or become a security liability.

Not patching. Patching and patch management is critical to security. Plus, the cost of getting a new software version is often higher than the cost of patching. Choose an automated patching tool to be sure you're staying on top of this important task.

Unrestricted bring-your-own-device policies. Some agencies have broad BYOD rules, some do not. Having no rules or having rules so strict that workers will try to circumvent them both invite breaches. The solution? Allow BYOD, but with restrictions. Separate the unsecure mobile devices on the network and closely monitor bandwidth usage so you can make changes on the fly as necessary.

While there is an increasing focus on enhancing agencies' security posture, there is no quick-and-easy solution. That said, tuning network security through best practices will not only enhance performance, but will also go a long way toward reducing risks and vulnerabilities.

COMPUTER SECURITY POLICIES
FOR USERS IN THE
UNITED STATES DISTRICT COURT
for the Northern District of Illinois

Introduction

This guide is to acquaint users with computer security practices that should be followed by members of the Court. Users are the first and best line of protection from compromise of data on Court systems. This plan has been adopted by the AO under IRM Bulletin 98-9 and James Metcalfe has been appointed as Computer Security Coordinator.

The United States Courts have experienced a dramatic increase in the use of computer resources to provide and process information. These new technologies are increasing our computer security risks.

User education and user policies are two critical components of risk management. Personal computer users often do not recognize possible risks and they may not be aware of measures that would minimize these risks. The following policies have been established in order to avoid and address security risks, ultimately protecting the Judiciary-wide Data Communications Network (DCN) and Northern District of Illinois networks and equipment.

These policies were written to provide users with a description of the security practices required by this Court. The information contained in this publication is intended to:

raise awareness of computer security,
define the responsibilities of the user,
assist users in recognizing potential problems, and
provide guidance to the end user if a compromise in security is suspected.

Every Court employee will be required to sign the User Agreement (at the back of this handbook) signifying their intention to adhere to these policies. If a need arises to create an exemption to a part of these policies, that user must obtain the approval of their supervising judicial officer or department manager and the Computer Systems Department (CSD). If the exclusion is approved by both parties, any installation or setup procedures will be handled or supervised by the CSD.

Overview of the Policies

Users are responsible for the appropriate use of their Court supplied PCs and for actions taken with regard to work created on personal or Court supplied home computers.

The DCN, Court networks, and other computer resources are designed to be used for official

Court business. Care must be taken to guard against unauthorized computer access to Judiciary information and to make proper use of the District's computer resources.

Access to the Internet will be provided where needed for Court business. Each user and each user's manager will need to exercise individual responsibility and judgment to ensure acceptable and appropriate use of Internet services as described in the Policy on Internet/Intranet Usage.

Users are expected to conduct themselves professionally and refrain from transmitting documents or electronic mail which contains indecent or obscene materials, profanity, or any form of discrimination or sexism.

The Judiciary's network bridges together administrative offices as well as all of the appellant, district and bankruptcy courts and some of their divisional and remote offices. This network is called the Data Communications Network or DCN. When you use Lotus Notes to send e-mail outside of our district or when you use the Internet/Intranet, you are using the DCN.

Four separate, yet related, sets of policies are contained in this document:

Security
Internet/Intranet Usage
Electronic Mail
Hardware and Software Installation

Finally, a user agreement follows at the end of the document which itemizes the major components of the policies. To affirm acceptance and compliance of the policies, all court staff must sign the user agreement.

Policy on Security

Physical Security

Protecting Your Office Computer

Computers need protection from physical hazards to avoid damage to the computer or loss of data. Users should protect equipment such as the computer unit, monitor, keyboard, scanner, mouse and printer by taking the following measures:

Do not place liquids on or around the PC or keyboard and avoid dropping crumbs or any foreign materials on the keyboard, mouse, or scanner.

Do not place non-removable stickers on the PC, monitor, keyboard, mouse, or scanner.

Avoid excessive heat.

Protect the PC and keyboard from dirt and dust particularly when construction or other dust-producing activities occur.

Do not place magnets (name tags, paperclip holders, etc.) on your computer equipment.

Avoid plugging heaters and other appliances into outlets that share the same circuit as computer because some appliances may overload the circuit causing the computer to lose power or incur damage.

Avoid areas susceptible to water damage.

Securing Notebook Computers

Due to their compact size, notebook computers are particularly susceptible to theft. Take measures to ensure that the notebook is either within sight or stored in a secure location. When traveling by car, place the notebook computer in a secure location such as the trunk of your car and avoid exposure to high heat. X-raying the notebook computer, for instance, upon entering the courthouse or traveling by air, will not damage the computer.

Keeping a Record of Borrowed Computer Equipment

If a laptop, CD or other computer property is borrowed by a user, that user is responsible for making sure that the CSD has written down the borrower's name along with the date and equipment identification. The borrower will ensure that borrowed or assigned computer equipment is physically secure at all times and that it is transported and used in the proper environmental setting. Further, the borrower will help to ensure that the CSD or any other lender of Court equipment has recorded the fact that the equipment was borrowed and will be returned promptly. If a user borrows equipment without CSD knowledge, that person could forfeit their right to borrow equipment for a specified amount of time to be determined by CSD.

Handling of Diskettes

All disks which contain Court information should be treated as sensitive. Disks should be protected from dust, food, and extreme temperatures. Leaving disks in direct sunlight will likely damage them. Also, it is important that they be stored in a secure location that is away from magnetic fields, such as telephones, electrical appliances, and motors, to insure the integrity of data. When entering the courthouse or other locations which employ security precautions, it is recommended that users exercise caution when running floppy disks through the x-ray machine.

Software Security

General Policy

Users may not attempt to gain access to network or local data for which they are not specifically authorized, nor attempt to break into or "hack" any network or computer system. Unauthorized access to information which is not related to an employee's assigned duties may result in disciplinary action.

Notify management and the CSD to report any contact with individuals in which illegal or unauthorized access is sought to sensitive information or when a user becomes concerned that a person may be the target of actual or attempted exploitation.

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 of applicable security features or procedures. Such monitoring may result in the acquisition, recording, and analysis of all data being communicated, transmitted, or processed in these systems by the user. If monitoring reveals possible evidence of criminal activity, such evidence may be forwarded to law enforcement personnel. The CSD, the Seventh Circuit Executive's Office and/or the Administrative Office of the U.S. Courts may be involved in such monitoring.

Data Backups

Network Backups: The network servers are backed up each evening. If a file is inadvertently deleted from a network drive by the user, the CSD may be able to recover the document. In those instances, contact the CSD for assistance in determining if the document is salvageable.

Networked Workstations: Local computer drives are not regularly backed up. Users whose PCs are part of a network should not save important information on the local hard drive (C: drive), as these drives may "crash" or be swapped out and replaced periodically in order to provide users with updated applications. The CSD is not responsible for network users' data files that are stored on a local drive. The user's network home directory (F:\) or group directory (G:\) is the proper location for permanent storage for all files from networked PCs.

Standalone Workstations: The only situation where data should be stored on the C: drive is for PCs or notebooks that are not connected to a network server. Users are then responsible for backing up the data stored on the local drive of their computers (usually the C: drive). It's highly recommended that each user copy changed local-drive data files to the network or a floppy each day, as well as perform full backups periodically. Please contact the CSD for assistance.

Laptops/Notebooks: Data integrity for non-networked laptops which have been assigned to specific users should be handled in the same manner as the above section, "Standalone Workstations." Users are not responsible for performing full backups on laptops checked out from a laptop "pool." However, any files created on the borrowed laptop should be copied to the network or a diskette and erased from the laptop before returning it to the laptop pool.

Software: Even though we have automatic network backups and most software products

provide safeguards such as automatic backup copies of files, sometimes you just can't be too careful. Making temporary backup copies of files can be accomplished by copying files to a floppy disk, to the local hard drive or to a different folder on the network file server. The best decision depends upon the user's particular situation.

Storage of Backup Disks: Backup disks should be clearly labeled, indicating the date of backup, disk contents, and the method of backup. Diskettes should be placed in a diskette holder or container and stored in a secure location. That location should provide for easy access to facilitate data recovery but placed away from the primary workstation.

If you have questions concerning backups, please contact the CSD staff.

Network Access

The user is responsible for maintaining a reasonably secure workstation. It is very important that you close all applications before you log off and leave for the day. Log out when leaving the work area for extended periods.

Passwords

Protection of Passwords: Improper protection of passwords may allow individuals unauthorized access to the DCN or Court data. Your password is the key to the information you and others have stored on network drives. Passwords must be protected and must not be given to anyone other than your supervisor or the CSD personnel as required for business and support reasons. Passwords should never be provided to any outside party over the phone, by e-mail, or by any other means. Persons attempting to gain unauthorized access to our system may impersonate systems personnel, maintenance personnel, or even court officials and judicial officers.

Changing Passwords: Passwords are required to be changed every 40 days and also following any time you have provided your password to another user or to the CSD staff. In cases where you have your passwords or others' passwords written down for emergency use, they must be stored in a secure location such as a locked safe or locked desk drawer. Ensure that someone "hunting" around your work area could not find out your password. If you think your password has been compromised in any way, change the password immediately. If assistance is required, contact the CSD.

Privacy: Your user name and password are the keys to any system. Persons who try to enter unauthorized systems can be expected to do anything to gain admittance. They sometimes will call users claiming to be repair personnel and ask for your user name and password or talk to ex-employees. Again, never give your password to anyone, except as required by your supervisor or the CSD, and then only in conformance with these policies.

Password Selection: Use the following guidelines when selecting passwords:

Passwords must contain at least five characters.

Passwords cannot be reused.

Passwords should contain a combination of letters, numbers and special characters.

Passwords which include special characters or numbers are more difficult to guess or decrypt.

Passwords should never be easily guessed such as names spelled backwards, names of a pet or relative, hobbies, or birth month.

Passwords should never be related to someone's identity, history or environment.

Passwords should not be simple alphanumeric sets like “ABCDE” or “12345".

Passwords should not be shared, written down, posted in your work space or included in data files.

Viruses

A virus is an executable file that replicates itself and attaches to other executable programs or macros in an unsolicited manner. A virus may be invisible to the user and do no apparent damage beyond spreading to other diskettes or files across the network. However, a virus can also destroy data, damage data integrity, deny access to service, and spread problems to other computers on the network.

The Judiciary has licensed Norton Anti-Virus for use on all computers including laptops/notebooks. It will scan files automatically, so once installed, there is no user action required to perform the virus scanning. The CSD personnel must be contacted at the first suspicion of a virus.

Users should be able to identify the possible signs of a virus and identify what steps to take if a virus is suspected.

Possible Signs of a Virus:

New filenames appear
Disk space mysteriously disappears
Files are corrupted
New dates appear
Files grow (without explanation)
Files are lost

Disk is unusable
Strange or unexpected messages appear on the monitor
Hard disk crashes
Memory capacity decreases

None of the above symptoms is conclusive of a virus but they are some ways that a virus will exhibit itself.

What to do if you suspect a virus:

Stay calm.

Write down the error message or description of the problem and what you were doing when you realized something was amiss.

Stop using the potentially infected workstation and turn it off.

Contact the CSD immediately.

Once the virus is removed, stay alert for possible reinfection.

Scan any diskettes used for possible infections.

Techniques for Avoiding Viruses: Be wary of files obtained from an outside source. Ensure that all files are scanned for viruses after they are copied to your local or network hard drive from sources such as the Internet, a bulletin board, or a Lotus Notes attachment. All disks that leave the work area (e.g., for work at home) or are obtained from an outside source should be scanned before being used in the workplace.

Since all DOS/Windows formatted diskettes have a boot sector that could be infected with a virus, it is important to treat any newly obtained diskettes as potentially infected and scan them for viruses upon receipt. This even includes shrink-wrapped diskettes from major manufacturers because infected diskettes have sometimes been shipped to stores by the thousands from the production facility.

Besides scanning all newly obtained diskettes, you can take other defensive measures. Never leave a diskette in drive A when you turn off a PC and always check the drive to make sure no diskette is in the drive when powering up. A fairly common way of contracting a virus is by "booting" (starting up) from a diskette in your floppy drive. All diagnostic and other boot type disks should be write-protected before use.

Policy on Internet/Intranet Usage

This policy describes the acceptable use of the public Internet network and the DCN and Court

intranets.

Internet Access

General Policy

1. Use of the public Internet network accessed via computer gateways owned or operated on the behalf of the United States District Court for the Northern District of Illinois (“the Court”) imposes certain responsibilities and obligations on Court employees and officials ("users") and is subject to Court policies and local, state and federal laws. Acceptable use is always ethical and reflects honesty. It demonstrates respect for a) intellectual property, b) ownership of information, c) system security mechanisms, and d) an individual's right to freedom from harassment and unwarranted annoyance.

2. Internet usage provided by the Court may be subject to monitoring for security and/or network management reasons. Users of these services are therefore advised of this potential monitoring and agree to this practice. This monitoring may include the logging of which users access what Internet resources and "sites." Users should further be advised that many external Internet sites also log who accesses their resources and may make this information available to third parties.

3. By participating in the use of Internet systems provided by the Court, users agree to be subject to and abide by this policy for their use. Willful violation of the principles and provisions of this policy may result in disciplinary action.

Specific Provisions

1. Users will not utilize the Internet network for illegal, unlawful, or unethical purposes or to support or assist such purposes. Examples of this would be the transmission of violent, threatening, defrauding, obscene, or unlawful materials.

2. Users will not utilize the Internet network for the purpose of participating in sexually oriented chat groups, visiting sexually explicit sites, or exchanging sexually explicit photographs, email, or files.

3. Users will not utilize Internet network equipment for partisan political purposes or commercial gain.

4. Users will not utilize the Internet network, e-mail or messaging services to harass, intimidate or otherwise annoy another person.

5. Users will not utilize the Internet network to disrupt other users, services or equipment. Disruptions include, but are not limited to, distribution of unsolicited advertising, propagation of

computer viruses, monopolizing and overloading networks with excessive high volume traffic which substantially hinders others in their use of the network.

6. Occasional personal use of the public Internet system may be allowed and will be treated similarly to "local telephone calls" [1] and users will keep the use of the Internet system for personal or non-public purposes to an absolute minimum. Users will exercise discretion in such use and acknowledge that such use is monitored and traceable to the Court and to the individual user. Personal Internet usage will be brief, limited, and must not disrupt productivity.

7. Access to the Internet from any Northern District of Illinois site is restricted to the use of the provided DCN Internet gateways. IRM Bulletin 97-19 states: "At its September 1997 session, the Judicial Conference approved a judiciary-wide policy regarding access to the Internet from computers connected to the DCN. The policy requires access to the Internet be provided only through national gateway connections approved by the Administrative Office pursuant to procedures adopted by the Committee on Automation and Technology." Access to the Internet via any dial-up Internet Service Provider (such as America Online or AT&T) is prohibited.

8. Users will take precautions when receiving files via the Internet to protect Court computer systems from computer viruses. Files received from the Internet should be scanned for viruses using Court-approved virus scanning software as defined by Court policy.

9. Users *will not* download or run any executable programs without prior approval from someone in the CSD. This includes, but is not limited to, any file with a file extension of .COM, .EXE, .SCR or .ZIP that is received via the public Internet system, e-mail or other messaging service.

10. Users will refrain from monopolizing system equipment, overloading networks with excessive data, or wasting other resources.

11. Users will utilize the Internet network to access only files and data that are their own, that are publicly available, or to which they have authorized access.

Internet E-mail

---

[1] ***IV. General Policy:*** Federal employees are permitted limited use of government office equipment for personal needs if the use does not interfere with official business and involves minimal additional expense to the government. Government office equipment including information technology includes but is not limited to: personal computers and related peripheral equipment and software, telephones, Internet connectivity and access to Internet services, and E-mail. This limited personal use of government office equipment should take place during the employee's non-work time. This privilege to use government office equipment for non-government purposes may be revoked or limited at any time by department officials. The privilege does not extend to modifying such equipment, including loading personal software or making configuration changes. *From the Executive Branch Model Policy/Guidance on "Limited Personal Use" of Government Office Equipment Including Information Technology - Version 9, March 8, 1999*

The Internet is an unsecured network and, as such, information and e-mail on the Internet can be read and broadcast or published without the knowledge or consent of the author. Most sites maintain records of all users or entities accessing their resources. These records may be open to inspection and publication without the user's 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 user's court unit and the entire federal judiciary.

Internet e-mail traffic is subject to inspection by a variety of persons and mechanisms. Authorized personnel on any node between the origin and destination of a message may have to inspect message contents in order to dispatch stalled deliveries or resolve other failures. Users should not expect the messages they send or receive via the Internet to be private.

Internet e-mail limitations:

Occasionally an Internet user's e-mail-reading software (Lotus Notes) will not be able to handle attachments.

Delivery and delivery times are not guaranteed due to unpredictable intermediary systems and network outages, slowdowns, and polling intervals.

Some messages may not be delivered although the message was correctly addressed.

Receipt or non-receipt can only be confirmed through other positive means, not by inference or assumption. The Lotus Notes “Receipt Requested” feature may not be honored by systems on the Internet. Users should not rely on this feature for Internet e-mail.

Delivery and response times on the Internet, as well as the DCN, are determined by traffic and congestion on the network. Users should not rely on Internet e-mail for time-sensitive communications or guaranteed delivery. For example, sending large files such as digital images to a large number of recipients will delay other traffic and may overload the system causing failures. Users are encouraged to use discretion when forwarding large e-mail messages to group addresses or distribution lists.

Congestion on the network can be caused by the propagation of “chain letters” and “broadcasting” of lengthy messages to lists or individuals. These uses also place a burden on the shared data storage device of the e-mail post office.

Internet e-mail access grants users the ability to subscribe to a variety of e-mail newsgroups, listservers, and other sources of information. These services are a potentially valuable information tool for some e-mail users; but again, the potential for network congestion is high. Users should be cautioned on the widespread use of mailing lists and listservers. In general, low-volume business related lists will not be a problem.

Intranet Access

The Judiciary's Data Communications Network (DCN) maintains the intra-Judiciary network where the Judiciary's "Intranet" (J-Net) has web sites for many of the United States Court Districts. Users will find AO and general Judiciary resource information, as well as links to circuit, district, and unit web sites across the nation on the J-Net. The Intranet is protected from the Internet through fire walled gateway sites yet precautions should be taken when downloading files from anywhere to a PC/laptop.

Policy on Electronic Mail

The purpose of this policy is to provide a guide to proper practices with respect to electronic mail usage in the Northern District of Illinois. Electronic mail originated in any automated system application of the court is for official business purposes only.

Conduct

E-mail users are expected to conduct themselves in a professional manner and should refrain from using profanity and/or obscenities in any electronic communication. Keep in mind at all times that an e-mail is easily copied or forwarded to anyone without the sender's knowledge.

Electronic mail is not a forum for soliciting goods and services which are not directly related to official business. Personal use of the Internet, if allowed, should be treated as a "local telephone call" and users will keep usage to an absolute minimum. Users are reminded that personal Internet usage will be brief, limited, and must not disrupt productivity. Refer to the section entitled "Policy on Internet/Intranet Usage" for further guidance about Internet electronic mail.

Attached files

Large file attachments should be used with discretion. Also note that the maximum allowable size for file attachments during business hours is limited. Any file from an outside source (i.e., AO, Internet, another Court) which is attached to an e-mail message must be scanned for viruses before being used.

Maintenance

It is the user's responsibility to delete and archive old e-mail messages and empty their trash and message log folders on a regular basis. The number of e-mail messages located in the in-box, trash, and message log should not be excessive. Instructions for archiving and deleting e-mail messages can be obtained from the Lotus Notes training guide, by looking in the Lotus Notes on-line help facility, or by contacting the CSD.

Security

Each user is responsible for the security of his/her e-mail account, which means that Lotus Notes logins and one's messages must not be available to unauthorized users at any time.

When leaving the work area, Lotus Notes should be left minimized with the password-protect option. Employees are not to read other employees' e-mail without prior permission.

Protect your passwords by changing them frequently. Do not share or repeatedly use the same passwords. A person who gains access to your e-mail account will be able to read all of your e-mail and may send messages to others in your name.

Policy on Hardware and Software Installation

Users' Hardware on U.S. Courts' PCs/Laptops/Printers

Contact the CSD for all hardware requests, needs, and installation. Personal hardware (e.g., an external CD ROM drive) may not be installed without consulting the CSD. Users may bring in amplified speakers or headphones to use with those PCs that have sound cards if desired. If there is a need for personal hardware to be loaded on Court equipment, users must first obtain the approval of the employee's supervising judicial officer or department manager and the CSD. If it is approved, the installation will be handled by the CSD.

Users' Software on U.S. Courts' PC/Laptops

The CSD will maintain an inventory of software installed on all unit computers. All computers are subject to inspection and scanning at any time to ensure that only authorized software is installed.

Privately-Owned Software

Installation of employee-owned software, including screen savers, on court PCs is generally prohibited. If there is a need for personal software to be loaded on Court equipment, users must first obtain the approval of the employee's supervising judicial officer or department manager and the CSD. If it is approved, the software installation will be supervised by the CSD. However, static background images, or "wallpaper," are not software and are permissible. Only court-procured, licensed copies of software should be installed, maintained, and utilized on court-owned computer equipment. Some of the reasons for this position are:

1. The installation of personal software not procured and installed by the District exposes our computer resources to the threat of computer viruses.

2. Installing employee-owned software on court PCs may be in violation of software copyright and licensing agreements. The use of software in violation of licensing agreements exposes our

organization to possible compensatory damages as well as punitive action.

3. Since we have no practical experience supporting these programs, the effect that employee-owned software may have upon systems components such as network hardware, operating systems, and PCs is unknown. This makes the task of troubleshooting and supporting authorized systems software and components more difficult and hampers our ability to provide timely, quality support.

Copyrighted Software

Copyrighted software must not be reproduced except as permitted by the terms and conditions of the contract under which it was purchased. All applicable laws must be obeyed and the use of pirated software is prohibited. All copyrighted software is to be procured, installed and tested by systems personnel.

Demonstration Software

To avoid contract violations and to ensure that all software is obtained from legitimate sources, individual users are not authorized to accept demonstration software. Demonstration or trial software may only be obtained through normal procurement channels and any such procurement must be approved and facilitated by the CSD.

AO/Court-Developed Software

AO and court-developed software may be occasionally distributed directly to court employees by the AO. All AO and court-developed software must be scanned for viruses prior to installation. The CSD must be contacted prior to installing such software and/or to assist in the installation.

Public Domain Software

Public domain software refers to programs that are not copyrighted and may be distributed at no cost. Public domain software must be approved by the CSD and the employee's supervising judicial officer or department manager. If it is approved, the software media will be virus scanned and the installation will be supervised by the CSD.

Shareware

Shareware is copyrighted software so there will not be a time when it is acceptable for a user to install a shareware program on a Court PC or laptop.

U.S. Courts' Hardware on User-Owned Personal Computers/Laptops

In rare cases, installation of a piece of hardware, such as a printer or modem, may be approved by one's supervising judicial officer or department manager for specific work-related purposes. If this need arises, users must first obtain their supervising judicial officer or department manager's approval and that of the CSD. When a piece of equipment is borrowed, information about the borrowed item and the borrower will be recorded by the CSD.

U.S. Courts' Software on User-Owned Personal Computers/Laptops

Some of our U.S. Courts' software licensing agreements will, on a rare occasion, allow for use on an employee's home computer. The use of software in violation of licensing agreements exposes our organization to possible compensatory damages as well as punitive action. Installation and support of allowable U.S. Courts' owned software on home PCs and laptops are the responsibility of the user.

Computer Policies User Agreement

To ensure that you are aware of your security responsibilities and to certify that you have received the most recent policies and procedures, you will be required to sign the user agreement that appears at the end of this document. Contact your supervisor, the Personnel Officer, or the CSD if you have questions about any part of the policies. The security of our computer systems requires the vigilance and commitment of each and every network user.

If a need arises to create an exemption to a part of these policies, that user must first obtain the approval of the supervising judicial officer or department manager and the CSD. If the exclusion is approved by both parties, any installation or setup procedures will be handled or supervised by the CSD.

United States District Court
for the Northern District of Illinois

Computer Policies User Agreement

As a user of computers, peripherals and networks of the United States District Court for the Northern District of Illinois, I acknowledge my responsibility to conform to the requirements and conditions established by this document. By participating in the use of the DCN and Northern District of Illinois networks ("Networks") and personal computer equipment provided by the Court, I agree to be subject to and abide by this policy for my use. I understand that willful violation of the principles and provisions of this policy may result in disciplinary action.

Security

1. I acknowledge that the DCN, Court networks and other computer resources are designed to be used for official Court business.

2. I will protect computer equipment (such as the computer unit, monitor, keyboard, scanner, mouse, and printer) by taking the measures outlined in the sections "Protecting Your Office Computer" and "Handling of Diskettes" in the Policy on Security.

3. I will ensure that borrowed or assigned computer equipment is physically secure and that it is transported and used in the proper environmental setting. Further, I will help to ensure that the CSD or any other lender of Court equipment has recorded the fact that I borrowed the equipment and I will return borrowed equipment promptly.

4. I will not attempt to gain access to network or local data for which I am not specifically authorized. I will not attempt to break into or "hack" any network or computer system.

5. I acknowledge my responsibility to immediately report to management and the CSD 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.

6. 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. 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 understand that the CSD, the Seventh Circuit Executive's Office and/or the Administrative Office of the U.S. Courts may be involved in such monitoring. I expressly consent to such monitoring.

7. I understand that I am responsible for keeping secure any documents or files I create that I do not

store on a network server.

8. I understand that I am responsible for maintaining a reasonably secure network workstation as stated in "Protecting Your Office Computer."

9. I will change my various passwords frequently and will not share my password with others. I will choose passwords that are difficult to guess.

10. I will ensure that virus-checking software is running at all times and will report to the CSD any suspicion of a virus.

Internet/Intranet

1. I acknowledge that acceptable use of the public Internet network accessed on behalf of the U.S. District Court for the Northern District of Illinois is always ethical, reflects honesty, and shows restraint in the consumption of shared computing resources. It demonstrates respect for intellectual property, ownership of information, system security mechanisms, and an individual's right to freedom from harassment and unwarranted annoyance.

2. For security and/or network management reasons, I understand and agree to be subject to the monitoring of my use of internet services provided by the Court. This monitoring may include the logging of which users access what Internet resources and "sites." Users are further advised that many external Internet sites also log who accesses their resources and may make this information available to third parties. I will utilize the Internet network to access only files and data that are mine, which are publicly available, or to which I have authorized access.

3. I will not utilize the Internet for illegal, unlawful, or unethical purposes or to support or assist such purposes. Examples of this would be the transmission of violent, threatening, defrauding, obscene, or unlawful materials.

4. I will not use the Internet to participate in sexually-oriented chat groups, visit sexually explicit sites, or exchange sexually explicit photographs, email, or files.

5. I will not utilize the Internet equipment for partisan political purposes or commercial gain.

6. I will not utilize the Internet, e-mail or messaging services to harass, intimidate or otherwise annoy another person.

7. I will not utilize the Internet to disrupt other users, services or equipment. Disruptions include but are not limited to distribution of unsolicited advertising, propagation of computer viruses, and sustained high volume network traffic which substantially hinders others in their use of the network.

8. Occasional personal use of the public Internet system may be permitted and will be treated similarly

to “local telephone calls”. I will keep the use of the Internet system for personal purposes, if permitted, to an absolute minimum. Users will exercise discretion in such use and acknowledge that such use is monitored and traceable to the Court and to the individual user. Personal Internet usage will be brief, limited, and must not disrupt productivity.

9. Access to the Internet from any Northern District of Illinois site is restricted to the use of the provided DCN Internet gateways. Access to the Internet via any dial-up Internet Service Provider (such as America Online or AT&T) is prohibited.

10. I will take precautions when receiving files via the Internet to protect Court computer systems from computer viruses. Files received from the Internet should be scanned for viruses using Court-approved virus scanning software as defined by Court policy.

11. Keeping in mind that Internet e-mail is easily copied or forwarded to anyone in the world without the original sender's knowledge, I will conduct myself in a professional manner by refraining from using profanity, obscenities, or other distasteful language in any electronic communication.

12. I will not use electronic mail to solicit goods and services which are not directly related to official business.

Electronic Mail

1. I understand that it is my responsibility to avoid having an excessive amount of messages saved in Lotus Notes.

2. I understand that employees are not to read other employees' e-mail without prior permission, and that unauthorized access to information which is not related to an employee’s assigned duties may result in disciplinary action.

3. I will minimize Lotus Notes with a password-protect option enabled when leaving my work area.

4. I understand that electronic mail is not always confidential. I also accept that authorized personnel on any node between the origin and destination of a message may have to inspect message contents in order to dispatch stalled deliveries or resolve other failures.

Hardware and Software Installation

1. 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 will not take any actions which will jeopardize the security of the system after my departure. Any loss to court owned computer equipment is the responsibility of the employee and any insurance refunds will become the property of the court.

2. I will obey all software copyright laws.

3. I will not install any software of any kind on any U.S. Court owned computer and will refer all needs for software procurement and installation to the CSD. I understand that I am prohibited from downloading or installing executable software from any source onto the Network or local drive without prior authorization from management and the CSD. I recognize that I must ensure that any files or software I am authorized to receive have been subjected to approved virus protection measures. Finally, I understand the term "software" refers to executables such as AO distributed utilities, games, screen savers, business applications, shareware, freeware, and demonstration copies of programs.

4. Excluding speakers and headphones where permitted by a supervising judicial officer or department manager and the CSD, I will not install any personal hardware on any U.S. Court owned computers.

5. I understand that support of allowable U. S. Court owned software on home PCs and laptops is the responsibility of the user.

United States District Court
for the Northern District of Illinois

Computer Policies User Agreement

I acknowledge my responsibility to conform, to the best of my ability, to the requirements set forth in this agreement. Failure to comply may result in denial of access to the Network and Court automation equipment and, if necessary, such violations will be reported to the proper authorities. I understand that violation of the Court's policy on Internet/Intranet use may lead to disciplinary action, including termination. I understand the subject matter discussed in "Policies Relating to Computer Users" and I agree to abide by that document.

I understand that failure to sign this acknowledgment will result in denial of access to the DCN, U.S. District Court for the Northern District of Illinois networks and automation resources.

Name (printed): _____

Employee's Signature: _____

Date: _____