Information Systems Security Policy

Revised December 2016

Table of Contents

1.0 PURPOSE

This policy will provide guidance for the use of computing resources by court employees and judicial officers.

2.0 SCOPE

This policy applies to all court employees (including interns) and judicial officers who use the court's computing resources in the performance of their jobs. In addition, this policy also applies to all court security officers who use court computers.

3.0 INTRODUCTION

The Federal Judiciary uses computer systems to maintain and process information. Because of networks, remote access, mobile communications, portable computers, decentralized information systems, and links to the Internet, the Judiciary's computerized information is vulnerable to theft, malicious destruction, and unauthorized change.

To protect the court's local computing resources, and the Federal Judiciary's national Data Communications Network (DCN), operating guidelines have been implemented which provide the framework for computer security in the U.S. Bankruptcy Court for the Southern District of Florida (court). This handbook was written to advise users of the court's computing resources and the DCN operating guidelines and to provide users with a description of the security procedures required by this court. The Information Technology Manager is responsible for updating this manual as needed. The information contained in this publication will raise awareness of computer security, define the responsibilities of the user, assist the user in recognizing potential problems, and provide guidance to the user if a compromise in security is suspected. All users of the court's computing resources and the DCN are required to adhere to the security guidelines and procedures discussed in this policy.

Users of the DCN and court computing resources are hereby notified that all telecommunications and information systems are monitored to protect against unauthorized use and for maintenance purposes. During such monitoring, the activities of authorized users may be monitored. Documents created and maintained on this system, including email messages, are assumed to be created and received during performance of official duties and may be official records. Should official need for access to an employee's files or email arise, it will be provided upon application of an appropriate official. Anyone accessing and using this system expressly consents to system monitoring and to official access to documents created and/or received by them. Any negligence, abuse or intentional malice in the use of systems hardware, software or computer information contained in the court's computer systems may result in the termination of the employee(s) responsible and restitution of any damages incurred as a result. The unauthorized sale or distribution of any data contained in the court's information systems is prohibited.

4.0 GENERAL USE OF COMPUTING RESOURCES

The DCN along with the court's computer networking and telecommunications resources are to be used for business approved by the court. The DCN is an unclassified network, and users are prohibited from storing, forwarding or processing any classified information on the DCN. In addition, users are expected to conduct themselves professionally and refrain from transmitting documents or emails that contain indecent or obscene materials, profanity, or any form of discrimination or sexism.

The use of home computers and private laptops or notebook computers in remote communication with the DCN must be approved by the Information Technology Department. In addition, special precautions for preventing the spread of computer viruses, as discussed in this handbook, must be employed.

5.0 PHYSICAL SECURITY

5.1 Computer Equipment Room

Computer equipment rooms will be kept locked at all times. Offices containing stored computer equipment at each court location must be locked after office hours. An inventory of computer equipment is maintained as set forth in the court's property management procedures.

5.2 Protecting Your 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, and printer by taking the following measures:

1. All desktop computers 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 remain logged in and active when unattended. Password protected screensavers are required for all court computers. Users are also encouraged to lock the PC using the ***CTRL-ALT-DEL*** keys and choosing the lock computer option. You may be held accountable for any negligence and/or unauthorized use, caused by access to your computer by unauthorized individuals.
5. People who do not belong in an area should be politely challenged and assisted. Any suspected unauthorized access should be reported to the Information Technology Department.
6. Do not place drinks (or any liquids) on or around the PC or keyboard, and avoid dropping crumbs or any foreign materials on the keyboard.

7. Protect the PC and keyboard from dirt and dust, particularly when construction or other dust producing activities occur.
8. Use a surge protector or other suitable power line filter.
9. Avoid areas susceptible to water damage.

5.3 Securing Mobile Devices

Due to their compact size, notebooks, laptops, tablets, and cell phones are particularly susceptible to theft. For that reason, it is important to secure court these issued mobile devices at all times. When leaving the office with a notebook, laptop or tablet, place the computer in a secure location, such as the trunk of your car, before departure.

5.4 Handling of Removable Storage

All removal storage that contains court information should be treated as sensitive. Disks, thumb drives and external drives should be stored in their protective jacket and protected from dust, food, and extreme temperatures. It is important that they be stored in a secure location away from magnetic fields, such as those created by electric motors, to insure the integrity of data.

6.0 DATA BACKUPS

The network drives, sometimes referred to as the S:, I:, and G:, are backed up each evening by the Information Technology Department. If a file is inadvertently deleted from a network drive by a user, Information Technology personnel may be able to recover the deleted data. For assistance in determining whether the document is retrievable contact the Information Technology Department.

Users are responsible for backing up the data stored on the local drive of their computer (usually the C: drive). It is highly recommended that each user backup any documents they may have stored on the C: drive to their network drive (S:). This will ensure that your documents are backed up on a nightly basis. Users are encouraged to contact the Information Technology Department to discuss backup options and password protection.

As part of the court's disaster recovery plan, the Information Technology Department will be responsible for backing up all server-based court systems to redundant storage devices. The Disaster Recovery Plan clearly identifies all aspects of data backup, recovery and rebuilding. Presently, there are two disaster recovery plans. One addresses the network systems and the other addresses the CM/ECF system. In addition, the court's Continuity of Operations Plan (COOP) identifies and lists all key applications and systems.

7.0 PASSWORDS

Improper protection of passwords may allow unauthorized access to the court's computing resources and the DCN. Users should exercise care when selecting passwords. In general, passwords are changed a minimum of every 90 days. Your user name and password are the keys to your system. Persons who try to enter systems that they are not authorized to enter can be expected to do anything to gain admittance. Persons attempting to gain unauthorized access to our system may impersonate Information Technology personnel. ***Passwords must be protected, and must not be given to anyone.*** If passwords need to be shared, they should never be provided to anyone over the phone, by email, or by any means other than personal delivery. If your password is provided to Information Technology personnel for a specific purpose, change your password as soon as Information Technology personnel have completed the work that required the use of your password. In cases where passwords are written down for emergency use (i.e., systems administrator passwords) they must be stored in a secure location such as a locked safe. If you think your password has been compromised in any way, change the password immediately. If assistance is required, contact the Information Technology Department. When selecting passwords, use the following guidelines:

What NOT to Use

- Do not use your login name in any form (as-is, reverse, capitalized, doubled, etc.)
- Do not use your spouse's or child's name
- Do not use other information easily obtained about you. This includes license plate numbers, telephone numbers, social security numbers, the brands of your automobile, the name of the street you live on, etc.
- Do not use a password of all digits, or all the same letter.
- Do not use a word contained in English or foreign language dictionaries, spelling lists, or other lists of words.

What to Use

- Your password must be 8 characters' alpha/numeric
- Do use a password with mixed-case alphabetic
- Do use a password with nonalphabetic characters, e.g., digits or punctuation
- Do use a password that is easy to remember, so that you do not have to write it down
- Do use a password that you can type quickly, without having to look at the keyboard. This makes it harder for someone to steal your password by watching over your shoulder.

Method to Choose Secure Passwords

- Choose a line or two from a song or poem, and use the first letter of each word. For example, "In Xanadu did Kubla Khan stately pleasure dome decree" becomes "IXdKKspdd".

- Alternate between one consonant and one or two vowels, up to eight characters. This provides nonsense words that are usually pronounceable, and thus easily remembered. Examples include “routboo,” “quadpop,” and so on.
- Choose two short words and concatenate them together with a punctuation character between them. For example: “dog;rain”, “book+mug”, “kid?goat”.

8.0 REMOTE ACCESS (VPN)

Court remote access computing resources may be used only by those individuals to whom they have been assigned. During system maintenance, Information Technology personnel may also gain access to or log the use of remote access 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, Information Technology personnel may provide the evidence of such monitoring to law enforcement officials.

Remote access to the DCN may be provided with the approval of the employee's supervisor or manager. The employee will then be required to sign and submit a Virtual Private Network (VPN) Policy Statement form (SYS-02). The form will be provided by Information Technology personnel along with the necessary hardware, software and instructions. Remote access users must meet certain job-related criteria and are required to follow the guidelines established by this policy. If a computer is equipped with software that allows a user to VPN in from outside the offices of the court (e.g., Laptop, COOP/Telework PC), password controls must be in place to prevent unauthorized access (refer to the password section of this document). All VPN users must log into the DCN using his/her (JENIE) username and password, and will be required to utilize a security protocol process called two-factor authentication. Two-factor authentication is an extra layer of security that not only requires a username and password, but also something that only the user should know or have immediately on hand (e.g., mobile app, physical key fob). The use of two-factor authentication makes it harder for potential intruders to gain access to the court's secured network.

8.1 COURT ISSUED COMPUTER HARDWARE FOR TELEWORK/COOP

The court has issued computers to staff that have requested and have been approved for telework and/or COOP purposes. Employees are required to have a safe and adequate place to work off-site, which is free from interruptions and provides the necessary level of security and protection for government property and confidentiality of data. The computer security policies contained in this manual, including internet access, apply to all employees and judicial officers who use court owned telework computers off-site. The employee is the only one authorized to use the court telework computers. In addition, the employee shall not download or install any software without the permission of the Information Technology Department. However, the employee may use the court telework computers for personal use as long as the computer security policies stated in this manual are followed.

9.0 REMOTE DESKTOP CONTROL

Information Technology personnel use remote desktop software to support and maintain the court's computers. In addition, certain employees are authorized to connect to their court PC using remote desktop software. Once connected, local control of the PC is disabled until the remote access connection is terminated. This software provides Information Technology personnel the ability to fully control any PC on the court's network. The current configuration of the software allows for direct peer-to-peer connections between a client and host PC. When the connection is established, the user is notified via a pop-up message that access to their PC is being requested. The user must click on ***accept connection*** in order to allow Information Technology personnel access to their PC. Once connected, information technology personnel will be able to view the entire screen of the remote PC in a window on their local PC screen and make any needed changes, updates and/or fixes.

10.0 INTERNET ACCESS

With the increased use of Internet services throughout the Judiciary, it is important that these tools are used properly and in the best interests of the government. Individual users must exercise responsible judgment. Under all circumstances, however, Internet access remains a privilege, rather than a right.

10.1 Overview of the Internet

The Internet is an informal collection of government, military, commercial and educational computer networks. Connection to the Internet offers users access to a wide spectrum of informational resources and the ability to communicate with other users on a global basis. The Internet audience is virtually unlimited. It is essential that users understand the limitations of the Internet. Because it is an unsecured network, any information contained on, and any communication sent or received via the Internet can be read, broadcast, and/or published without the knowledge or consent of the author. Most sites maintain records of all users and entities accessing their resources, which 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 to the user, the court, and the entire Federal Judiciary.

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 the Information Technology Department personnel.

10.2 Authorized Activities While on Duty

The following guidelines must be followed to ensure that employees use the Internet safely, productively, and in a way, that does not compromise the interests or integrity of the Judiciary. These guidelines apply to all Internet services,

including, but not limited to, email, web browsers, Telnet, and File Transfer Protocol (FTP).

The Judiciary provides the Internet connection to support and promote official government business and limited personal use. When accessing the Internet, employees must adhere to the same code of ethics that governs all other aspects of Judiciary employee activity. ***Examples of permitted Internet activities include work-related research, reading professional literature, and email relating directly to official duties.*** Official announcement of judicial policy or practice may be made only by offices or employees expressly authorized to perform that function.

10.3 Authorized Personal Use of the Internet:

1. Employees should keep the personal use of the Internet to a reasonable duration and only during personal time.
2. Personal use of the Internet should not adversely reflect on the court (e.g., no EEO violations, furthering of extremist organizations, dirty jokes, chain letters, racial, ethnic or gender slurs).
3. Unlawful or inappropriate use of the Internet is not permitted (e.g., no access to pornographic sites, no Privacy Act violations, no release of confidential, sensitive, classified, or FOIA (Freedom of Information Act)-exempt information, no copyright or licensing law violations).
4. Personal use of the Internet cannot result in any additional cost to the Judiciary (e.g., some Internet services charge a subscriber fee which employees may charge to their personal accounts).
5. Employees may conduct commercial transactions on the Internet at work during personal time, but not conduct a business or sell personal property or other effects through the Internet (e.g., limited retail purchasing through the Internet is acceptable, but conducting a consultant business while at work is not).
6. Personal use of the Internet may not interfere with the Court's mission.
7. The Internet should not be used to send emails containing religious messages, religious symbols, or religious greetings (users are identified as court employees and the government may not be involved in the establishment of religion).
8. For the same reason described above, employees should not use the Internet for political activities (e.g., using the Internet to further one's own or someone else's partisan or nonpartisan political campaign).
9. Employees may not claim to represent the views or position of the court, Judiciary, or the Government, and may not make unauthorized commitments or promises of any kind purporting to bind the court, Judiciary, or the Government.
10. If employees accidentally access a website that contains pornographic, sexually explicit, inappropriate or illegal materials, they must leave the site immediately and shall report this accidental access via email to the Information Technology Manager, with a copy sent to their manager.

10.4 Unauthorized Computing Resources Activities

Employees are expected to conduct themselves professionally in the workplace and to refrain from using the network for activities that are inappropriate. Employees

are specifically prohibited from using the Internet and email for the following purposes:

1. Sending, displaying, or downloading messages or pictures that are offensive, harassing or discriminatory, or that are of an obscene or sexually explicit nature.
2. Any use that could cause congestion, delay, or disruption of service to any government system or equipment, including streaming video, audio, or other large file attachments that can degrade the performance of the entire network (exception: any use that constitutes official government business, such as viewing streaming video from the AO's J-Net).
3. The use of peer-to-peer (P2P) file sharing (e.g., Napster, Grokster, Morpheus, Pirate Bay or other Bit Torrent web sites), Internet games, chat rooms and instant messaging are strictly prohibited in accordance with AO policies.
4. Downloading of software from any web site, without first obtaining approval from the Information Technology Department.
5. Making unauthorized statements regarding Judiciary policies or practices.
6. Transmitting confidential information (such as that relating to ongoing investigations, procurement, or litigation).
7. Making unauthorized commitments or promises that might be perceived as binding the government.
8. Posting an unauthorized home page or similar web site.
9. Using the network for illegal activities.
10. Using the network in a manner that could reflect poorly upon, or cause embarrassment to the Judiciary.

10.5 Privacy Expectations/Monitoring

Internet browsing and email transmissions are subject to inspection by a variety of persons and mechanisms, authorized and otherwise. Judiciary employees have neither a right nor an expectation of privacy while accessing the Internet and using email. The Clerk may request access to any electronic communications, and Internet activity may be monitored at any time for any purpose, including compliance with acceptable use policies. During such monitoring, the activities of authorized users may be monitored. Should official need for access to an employee's files or email arise, it will be provided upon application of an appropriate official. Anyone accessing and using this system expressly consents to system monitoring and to official access to documents created and/or received by them. Anyone using court-provided Internet services consents to the court's monitoring policy as stated in this manual.

10.6 Sanctions for Misuse

Violation of acceptable use policy will be sanctioned, including the imposition of criminal penalties, financial liability, and termination of employment. The court has a zero-tolerance policy with respect to the downloading, transmission and display of obscene or pornographic images and text. ***Any employee who violates this policy may be subject to the full range of disciplinary actions, up to and including termination.***

11.0 SOCIAL MEDIA POLICY

The Code of Conduct for Judicial Employees applies to all employees of the U.S. Bankruptcy Court for the Southern District of Florida. There are several Canons by which all judicial employees must govern their actions. The Canons that impact use of Social Media and on-line activities include:

Canon 1: A JUDICIAL EMPLOYEE SHOULD UPHOLD THE INTEGRITY AND INDEPENDENCE OF THE JUDICIARY AND OF THE JUDICIAL EMPLOYEE'S OFFICE

Canon 2: A JUDICIAL EMPLOYEE SHOULD AVOID IMPROPRIETY AND THE APPEARANCE OF IMPROPRIETY IN ALL ACTIVITIES

Canon 3: A JUDICIAL EMPLOYEE SHOULD ADHERE TO APPROPRIATE STANDARDS IN PERFORMING THE DUTIES OF THE OFFICE

Canon 4: IN ENGAGING IN OUTSIDE ACTIVITIES, A JUDICIAL EMPLOYEE SHOULD AVOID THE RISK OF CONFLICT WITH OFFICIAL DUTIES, SHOULD AVOID THE APPEARANCE OF IMPROPRIETY, AND SHOULD COMPLY WITH DISCLOSURE REQUIREMENTS

Canon 5: A JUDICIAL EMPLOYEE SHOULD REFRAIN FROM INAPPROPRIATE POLITICAL ACTIVITY

The challenges and risks of social media are particularly acute for government employees who work in positions where discretion and confidentiality are imperative. Court employees work in such an environment. Court personnel are expected to keep sensitive information confidential, exercise discretion to avoid embarrassment to the court, and take precautions to avoid unnecessary security risks for court personnel, including the judges they serve.

1. **Think before you post**. Internet postings---whether they be text, photos, videos, or audio---remain accessible long after they are forgotten by the user. Beyond that, remember that nothing is "private" on the Internet despite people's best efforts to keep things private. Do not post anything on the Internet that you would not want to read on the front page of your local paper.

    a. Do not list your place of employment or any other employment information.
    b. Do not identify the judge who employs you or the judicial district and division where you work.

2. **Observe security protocol**. On-line comments can jeopardize the safety of all court personnel.

    a. Do not post pictures of the inside or outside of the courthouse, especially the judges' chambers.
    b. Do not post pictures of court events.

c. Do not post pictures of judges or other personnel.
d. Do not post information about the habits or routines of judges or other personnel.
e. Do not discuss courthouse security measures or security personnel.
f. Do not reveal details of judges' schedules and travel; do not reveal details of your own travel schedule when traveling on official business.

3. **Maintain court's confidentiality.** Confidentiality is critical**.**

    a. Do not discuss any of the court's internal procedures, whether or not they are confidential.
    b. Do not post anything about a case you or your co-workers are working on or have worked on.
    c. Do not comment on lawyers practicing in the court.
    d. Do not post anything about the court's views on any legal issues.
    e. Do not post anything about pending or closed cases, regardless of whether the information is "public" or not.
    f. Do not post your personal views about the court's rulings or the rulings of other judges.
    g. Do not post any on-line comments containing confidential court information, including information about court cases and decisions.

4. **Speak for yourself, not your institution**. Remember that you are a representative of the court and should conduct yourself in a way that avoids bringing embarrassment upon yourself and/or the court. Court employees should abide by a simple rule: if you are not speaking to someone directly or over a secure landline, you must assume that anything you say or write is available for public consumption. Make sure your on-line activities do not interfere with your job or work commitments.

    a. Do not engage in on-line activities that detract from the dignity of the court.
    b. Do not post on-line comments about issues before the court or likely to come before the court.
    c. Do not post comments endorsing or criticizing political parties or candidates.
    d. Do not use the official court seal or any other official court symbol or identification**.**

5. **Enforcement**. Any employee who violates this policy may be subject to the full range of disciplinary actions, up to and including termination.

Finally, the examples set forth above are not exhaustive**.** If you are in any doubt about whether your use of the Internet, email, or social media may violate this policy, do not do it.

12.0 EMAIL POLICY

The court's internal email system is for official correspondence. However, the Clerk has authorized personal use of the court's internal email system during an employee's personal

time. When using the court's internal email system, users must conform to the same policies and procedures set forth in this handbook for Internet and Social Media. Keep in mind at all times that an email is easily copied or forwarded to anyone without the sender's knowledge. Documents created and maintained on this system, including email messages, are assumed to be created and received during performance of official duties and may be official records. Should official need for access to an employee's files or email arise, it will be provided upon application of an appropriate official. ***Anyone accessing and using this system expressly consents to system monitoring and to official access to documents created and/or received by them.*** The Clerk may request access to any electronic communications, and email activity may be monitored at any time for any purpose, including compliance with acceptable use policies. If such monitoring reveals possible evidence of criminal activity, court personnel may provide the evidence of such monitoring to law enforcement personnel for investigative purposes.

12.1 Conduct

Email users are expected to conduct themselves in a professional manner and should refrain from using profanity and/or obscenities in any electronic communication.

12.2 Internet Web Based Email

Because web e-mail messages and their attachments bypass the existing network anti-virus protections in place at the Internet gateways and on the court's servers, the retrieval of e-mail from personal Internet service provider accounts has been a primary source of computer virus, Malware and worm infection on the Judiciary's networks. Our centrally hosted e-mail is screened and protected through the national Internet gateways, but current technology provides no way to virus-scan personal e-mail or attachments accessed from the Internet-based e-mail providers before they are opened by the recipient. Accordingly, it is the official policy of the Judicial Conference that access by Judiciary personnel to personal Internet e-mail accounts, including but not limited to: AOL Mail, Gmail, Hotmail, and Yahoo!, from within the Judiciary's networks is discouraged. Court employees are discouraged from using Internet based email and are therefore permitted to send and receive personal e-mail using your court email account.
For those who find it necessary to access a personal Internet e-mail account from within the DCN, the following guidelines are suggested as ways to reduce the risk of introducing a virus, malware, worm, or other malicious software into the DCN:

1. Do not open any e-mail attachments unless you are sure they are safe. People naturally assume that the persons they are communicating with would not send them malicious e-mails, but the senders are typically not aware that they are sending viruses. Worse, spoofing programs frequently indicate that an e-mail message is from a known user, when it is initiated by a virus.
2. Do not open or follow any links in an e-mail unless you are sure they are safe. A common tactic of identity thieves and propagators of malicious software is to direct the recipient of an e-mail to a website which appears to belong to a real company or institution but which is a phony site constructed

for the purpose of identity theft or the spread of malicious software.

3. Use an Internet e-mail provider which provides virus scanning of e-mail and attachments, such as Google's Gmail, MSN's Hotmail, or Yahoo Mail.
4. Avoid advertising your e-mail name over the Internet. In particular, limit the recipients of your e-mail messages to people and organizations you know. Do not arbitrarily hit "Reply All" to messages with mail lists or people you do not know. This helps reduce the possibility that your personal or court e-mail name will be captured by spammers, phishers, or other malicious Internet users.
5. Avoid the use of automatic e-mail forwarding to personal Internet e-mail accounts. Automatic forwarding may result in sensitive case or personal information being forwarded over network connections that are subject to interception by malicious outside Internet users. Automatic forwarding can also result in the disruption of the court's e-mail service by flooding the server with messages.
6. Any file from an outside source which is attached to an email message must be scanned for viruses before being used. The court's anti-virus program will automatically perform this function. Users are reminded not to open any emails from unknown persons, specifically those emails with attachments.

12.3 Security

Each user is responsible for the security of their email account and should exit email when not preparing or reading messages. Protect your passwords by changing them frequently. Do not share or repeatedly use the same passwords. A person, who gains access to your PC, may gain access to your email account and will be able to read all your email, and may send messages to others in your name, or access prohibited Internet sites. You may be held accountable for any negligence and/or unauthorized use, caused by access to your computer by unauthorized individuals. To prevent this from occurring, ensure that your computer is logged off before you leave, or is protected by screen saver software that requires a password to reactivate to ensure that your PC will not be accessed by unauthorized users in your absence. In addition, you are required to completely shut down your computer before you leave work at the end of the work day. Employees who access their computers using remote desktop software are not required to shut down their computer. Instead they must lock the computer.

13.0 SOFTWARE

Any software purchased or acquired by the court will be inventoried and a record will be kept of all personnel with access to the software. Court personnel must adhere to all copyright statements.

13.1 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 Information Technology personnel.

13.2 Court Developed Software

Court developed software may be distributed directly to court employees by Information Technology personnel. All court developed software must be scanned for viruses prior to installation. Any application written for the court is the property of the court and copies may not be provided to anyone without the Clerk's knowledge. All newly created applications must be supported by adequate documentation.

13.3 Shareware/Freeware

Shareware and/or freeware software allows a user to try out software before voluntarily contributing a sum to purchase. Use of shareware/freeware must be approved in advance by Information Technology personnel and scanned for viruses prior to installation.

13.4 Privately Owned Software

Privately owned software cannot be used to process Judiciary information except when approved in advance by Information Technology personnel. Once approval has been obtained, the court will purchase a copy of the software for installation through normal procurement channels.

13.5 Systems Applications Manuals

There are several computer applications manuals and other materials documenting programs used in the court in the possession of Information Technology personnel. These manuals will remain in the court’s Information Technology department and will be allowed to circulate under the control of the Information Technology personnel who will maintain a record of the location of all circulating manuals. Computer manuals must be kept current as updates are received.

14.0 VIRUSES/MALWARE

A virus and malware are executable files that can replicate itself and attaches to other executable programs and/or macros in an unsolicited manner. A virus or malware may be invisible to the user. It may do no apparent damage, but may spread to other disks, files or systems across the network. A virus and malware can destroy data, damage data integrity, deny access to service, and spread problems to other computers across the network. Malware can block access to sites and take information off computers. The Judiciary has licensed anti-virus programs for use on all the Judiciary’s PCs, including laptops and computers used by employees at home. All PCs will have this software installed, and each employee will be trained to utilize the software to perform simple virus protection activities. Information Technology personnel must be contacted at the first

indication (or 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.

Signs of a Virus / Malware:

- Applications that do not work properly.
- Disks cannot be accessed.
- Printing doesn't work correctly.
- Pull-down menus are distorted.
- File size changes for no apparent reason.
- Date of last access does not match date of last use.
- An increase in the number of files, when nothing has been added.
- Uncommanded disk drive activity.
- Unusual error messages.
- System slows down, freezes or crashes.

Techniques for Avoiding Viruses / Malware:

- Install antivirus software and make sure updates are current.
- Scan your system regularly.
- Do not install new programs without first notifying Information Technology personnel.
- Do not visit unauthorized Web sites.
- Do not open e-mail attachments from unknown sources.
- Do not follow links in email that are not known.
- Do not use file-sharing software.
- Keep your Windows system files up to date with all the current security updates.
- Check with Information Technology personnel when error messages or warning windows pop up.

15.0 SECURITY TRAINING

Computer security training can increase the knowledge and awareness of the DCN community and protect the court's information systems. Computer security training will help to emphasize your role in computer security, explain what can be done to reduce the risks, and remind staff of the policies and procedures in place to protect the court's Information Systems. The court will provide computer security training on an annual basis. It is mandatory that each user attend.

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 Memorandum of Agreement that appears at the end of this Handbook.

The security of our computer systems requires the vigilance and commitment of each user. We thank you for your careful attention and dedication to this critical task.

USER MEMORANDUM OF AGREEMENT - SYS-01
U. S. Bankruptcy Court for the Southern District of Florida

As a user of the court's information systems, I acknowledge my responsibility to conform to the requirements and conditions established by this document.

1. The DCN is an unclassified network. I will not introduce, store, pass, or process classified data on the network.
2. I understand the policies outlined in this handbook, including authorized and unauthorized use of the Internet. I agree to abide by the policies set forth in this document.
3. I am responsible for all actions I take under my account. I will not attempt to "hack" the Judiciary network or any other network or computer on the DCN, or attempt to alter data, or to gain access to data for which I am not specifically authorized.
4. I will maintain the security of my workstation when connected to the court's network.
5. I will only use the DCN for approved business and authorized personal Internet use.
6. I will ensure that restricted information under my control is not publicly disclosed.
7. I will report immediately to my supervisor any attempt by an unauthorized person to obtain access to my computer.
8. I will not download or install executable software from any source onto my computer without prior authorization from my managers and/or the Information Technology Department. I will ensure that files or software I am authorized to receive have been subjected to approved virus protection measures.
9. I understand that all telecommunications and automated information systems are subject to monitoring to protect against unauthorized use and for maintenance purposes. During such monitoring, the activities of authorized users may be monitored. Documents created and maintained on this system, including email messages, are assumed to be created and received during performance of official duties and may be official records. Should official need for access to an employee's files or email arise, it will be provided upon application of an appropriate official. Anyone accessing and using this system expressly consents to system monitoring and to official access to documents created and/or received by them.
10. I have read and understand the issues outlined in the social media policy and I agree to abide by the policy.
11. I understand that I am responsible for all actions taken when participating in social media activities.

Employee's Name: _____

Employee's Signature: _____ Date: _____

Supervisor's Signature: _____ Date: _____