United States District Court
for the
Eastern District of Kentucky
(KYED)

Computer User Handbook and Memorandum of Agreement

February 2018

Version 1.0

Prepared for the
United States District Court
for the Eastern District of Kentucky
101 Barr Street
Lexington, KY 40507

Contents

Revision Log

Date	Description	Editor
10/23/2019	Added Bethany Morgan as ISO	BMM
4/29/2020	Changed Lotus Notes to Outlook and updated	BMM
8/4/2020	Grammatical changes	LLW

INTRODUCTION

Information technology (IT) has significantly impacted the work of the United States courts. Although the benefits of these information systems are vast, the technology also increases exposure to malicious activity and potential loss of data within the courts.

Personal computer users need to be aware of measures that minimize the risks associated with IT. Minimization of risks includes proper procedures and practices to avoid a breach of public trust or embarrassment to the court and the judiciary. This handbook provides court employees a description of the security practices and policies required by the United States District Court, Eastern District of Kentucky. This publication will raise awareness of the need for 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.

All employees of the U.S. District Court, Eastern District of Kentucky, who use information technology systems during the course of their duties are required to adhere to the guidelines discussed in this document. In addition, staff members will be required to sign the "*Computer User Memorandum of Agreement*" contained in this handbook. These guidelines apply to employees in chambers and the Clerk's office, as well as interns, externs, and volunteers.

USE OF COMPUTER RESOURCES AND SERVICES

Technology resources are provided for official court business to be used to assist employees in the performance of assigned duties. Since no two employees will use these resources in exactly the same way, each user will have to exercise individual responsibility and judgment as to appropriate use within the guideline of "official business" in accordance with the *Code of Conduct for Judicial Employees*[1] and the description of court duties. While occasional and limited personal use is not categorically prohibited, such use should be kept to an acceptable level that does not interfere with assigned duties.

Fraudulent, harassing, indecent, profane, obscene, or unlawful material may not be sent by email or other form of electronic communication or displayed on or stored in any court-provided computer. Users encountering such materials should immediately report the incident to their judge or court unit executive. Non-government provided, unapproved, and personal equipment is prohibited to be physically wired or electronically connected to the court's private network, Data Communications Network (DCN), except through approved methods such as a court authorized VPN account.

SYSTEM MANAGEMENT

All court systems and Internet activity are inspected to protect against unauthorized uses and for maintenance purposes. During such inspection the activities of authorized users may be analyzed and/or recorded by system personnel. A person accessing and using this system expressly consents to system analysis. If analysis reveals possible evidence of criminal activity, such evidence may be provided to law enforcement personnel. If improper usage is found, disciplinary action may be initiated according to the Code of Conduct for Judicial Employees.

Documents created and maintained on judiciary-owned network systems are assumed to be created in the course of performance of official duties and may be official records. As part of the routine backup schedule, files located on these systems are duplicated daily. Should official need for access to an employee's files or electronic mail arise, it will be provided upon request by appropriate management authority.

[1] Code of Conduct for Judicial Employees - http://jnet.ao.dcn/Guide/Vol_2_Ethics_and_Judicial_Conduct/Part_A_Codes_of_Conduct/Ch_3_Judicial_Employees.html

PHYSICAL SECURITY

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, mouse, and printer by taking the following measures:

- 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.
- Protect the PC and keyboard from dirt and dust, particularly when construction or other dust producing activities occur.
- Make sure the surge protector is in place and in use.
- Avoid areas susceptible to water damage.
- Secure the workstation by locking the computer (Windows Key + L) when you are away from your desk for longer than 5 minutes.
- Log out of the network at the end of your day or if you will be away from your computer for an extended period of time (Logging off does not require powering the machine off).

Securing Portable Devices

For employees authorized to use court-owned portable devices such as notebook (laptop) computers, iPads, iPhones or other portable devices, special care must be taken. Portable computing devices, due to their compact size, are susceptible to theft, loss or damage. For these reasons, it is important to safeguard all portable devices in your possession. The focus should be on the data of the judicial; the safeguarding of the device is important but a secondary consideration.

Here are some tips on how they can be protected from damage, loss or theft:

- When traveling, keep the device on your person or place it in a secure location, such as the trunk of your car.
- In airports and other places, you may be required to have the device x-rayed. This process will NOT damage the device. However, be especially vigilant as this can be an opportunity for theft.
- Allow portable devices to adjust to room temperature before use. Using a device that has been out in extreme hot or cold temperatures could result in damage.
- Encrypt data stored on these “portable” devices.
- Consult the IT staff if you have any questions or concerns about the care and maintenance of a portable device.

With their cost, susceptibility to damage, loss and theft, and the expense involved in maintaining them, the availability of portable devices is limited. Employees who are assigned notebook computers, iPads, iPhones or other portable devices, must sign a receipt for the equipment. In the receipt the employee acknowledges that:

- It is for use in the conduct of official business.
- He/she is responsible for its proper use, care and reasonable protection from damage or loss.

Data Backups

Each employee has a file share on the court’s computer network to store data. The allocated network drive, currently referenced as the H\: drive (J:\ for Chambers), is backed up each evening. Other network drives are backed up according to a prescribed schedule. For this reason, **all work files should be saved on an allocated network drive**. If a file is inadvertently deleted from a network drive by the user, the IT staff may be able to recover the document. In those instances, contact the IT Help Desk immediately for assistance in determining if the document can be recovered.

Users are responsible for backing up the data stored on the local drive of their computer (usually the C: drive). It is strongly advised that work files **NOT** be kept on the local drive. If you require assistance making backups of data files on your local drive, contact the IT Help Desk.

Removable Storage Media

Removable or portable storage media include but not limited to, such devices as tablets, memory cards, USB flash (thumb

drives/flash drives) drives, external hard drives and optical disks (DVDs or CD-ROMs), smart phones, wearable technologies (smart watches), and external hard drives. It is recommended that sensitive or privileged information not be stored on such media since it can be easily lost or stolen.

If necessary, and with management approval, the following guidelines should be followed for using removable storage media:

- Store in a secure location such as a locked drawer, file cabinet, or safe.
- Use password protection or encryption for sensitive information stored on the media. The office of Information Technology can recommend encryption software.
- For backup purposes, maintain a copy of any important files on your network drive.
- Protect from damage such as strong magnetic fields, excessive moisture or dust buildup, food spillage and extreme temperatures.

Cloud Computing

Internet sites and computer services which allow a user to save files or electronic media via the Internet where the user does not always have a specific concept of where the data is actually maintained are often referred to as the "cloud." The "cloud" presents unique data access and security concerns which are inherent in the ambiguity of the storage location. The judiciary cannot guarantee the integrity of the information.

Storage of the judiciary data on a non-judiciary network, device, or Internet service is not permitted. Services such as DropBox, iCloud, and any other non-judiciary systems should not be used for court information.

Data Protection

Sensitive data, such as social security numbers, birth dates, phone numbers and addresses, accounting materials, benefit information, salary information, and confidential case information must be protected from discloser because loss of this data can lead to identity theft, personal inconvenience, public embarrassment or even bodily harm. This type of information should not be taken from a secure judiciary environment into a less secure home or off-site environment unless suitable precautions are taken to protect the data, and management approval.

PASSWORDS

Improper protection of passwords may allow unauthorized access to the network. Users must exercise care when selecting passwords. It is recommended that passwords be changed every 60 to 120 days. Your passwords are the key to the information you store on the network as well as access to user email and other court services and applications. Note: User password management is enforced by the national password policy.

Passwords must be protected and must not be given to anyone. If your password is provided to the IT staff for maintenance, it is highly recommended that the user changes the password when the work is completed.

Be aware that persons attempting to gain unauthorized access to our system may impersonate IT staff, maintenance personnel, or even judges. Unauthorized persons will try a variety of tactics to gain access to systems. Some tactics include; calling users claiming to be repair personnel and ask for usernames and passwords, going through the trash looking for discarded information, or talking to ex-employees. If you think your password has been compromised in any way, change the password immediately and notify the IT staff.

Users are required 3 of the following:

- Upper Characters (A-Z)
- Lowercase characters (a-z)
- Numbers (0-9)
- Special symbols: ! @ # $ % ^ & * ( ) _ + | ~ - = \ ` { } [ ] : " ; ' < > ? , / (NOTE: some characters may not be supported on all Judiciary systems).

- Password must be at least eight (8) characters long

When selecting passwords, best practices are:

- Original passwords given by the IT Staff should be changed.
- Passwords should be at least twelve characters in length.
- Passwords should not be reused.
- Passwords that contain a combination of letters, numbers and characters are more difficult to guess or decrypt. (Examples: Phrase; **I e**njoy **g**oing **to see mom a**nd **dad** > !3g2CM0m&D@d)
- Passwords should NOT be single meaningful words or be easily guessed, (names, names of a relative or friend, hobbies, birthday, or common password; i.e. qwerty, password, 12345, etc.)
- Passwords should not be shared, written down, told to unsolicited callers, posted in your workspace or included in data files.

DATA COMMUNICATIONS NETWORK (DCN) ACCESS

Court employees have access to the judiciary's private network known as the DCN. The DCN allows users to store information and access resources necessary for their job performance. An individual's network and court email accounts establish their identity on the DCN and what resources they are authorized to use.

INTERNET/INTRANET ACCESS

These guidelines apply to all Internet and Intranet (Internal Web) services accessed using computer resources of the judiciary (with the exception of the Public Wireless Access.) Employees who are authorized to use these services must make sure they use the Internet safely and productively, and not in any way that could compromise the interests of the judiciary. Once logged into the DCN, employees have access to the Intranet and Internet. As part of the Administrative Office's network security system at the Internet gateways, usage logs (bandwidth, service, and protocols) are maintained for all DCN traffic. In addition, access to certain types of sites are blocked within the policy established by the U.S. Judicial Conference.

Users that access an Internet site or send an electronic message through the DCN Internet gateway will be interpreted as originating from the United States Courts and will be known by the receiving site or party. Inappropriate usage could result in a breach of integrity of the DCN allowing unauthorized access, the theft of information or disruption to our private network through the introduction of computer viruses or other malicious attacks. The impact of these actions on the court could cause a breach in public trust of the judiciary.

All employees have access to the court Intranet which allows them to access resources and tools that are essential to court productivity, court documentation, management of employee documentation, and essential job activity. Access to these resources are limited to the employee's job assignment and must be treated as sensitive. Confidential employee information is maintained on management resources located on the Intranet and must be treated as such.

Users bear sole responsibility for any material they send, access, or display on the Internet or in Internet email. Acceptable use of the Internet:

- Access to the Internet must adhere to the same code of ethics that governs all other aspects of judiciary employee activity.
- Access to the Internet should be used primarily for official court business only.
- Employees are specifically prohibited from using the court provided Internet for the following purposes:
    - Sending information that contain discriminatory statements, including those that malign any race, creed, color, sex, or sexual preference.
    - Making unauthorized commitments or promises of any kind that might be perceived as binding the government.

- Sending information over the Internet that could reflect poorly on or cause a breach of public trust to the judiciary.
- Using the DCN to take part in Internet discussion forums that are not associated with official government business or posting personal opinions on Internet forums.
- Using the network connection for commercial purposes or private gain.
- Using the network for illegal activities.
- Using the network for political activities.
- Improper use or distribution of information is also prohibited. This includes copyright violations such as software piracy. The judiciary may incur a legal liability for unauthorized copying of files or software even if the copy is used for official business.

- Show respect for intellectual property and creativity by giving appropriate credit when files or portions of files are used while carrying out official duties.
- Don't disclose confidential or sensitive information without authorization.
- Refrain from any practices which might jeopardize the judiciary's computer systems and data files.

E-MAIL POLICY

Users are reminded that email is official correspondence and should follow any office policies or practices that apply to other forms of work-related written communications. Keep in mind, at all times that an email is easily copied or forwarded to anyone without the sender's knowledge.

Electronic Mail

Employees may use the court provided email account to send and receive e-mail from outside the judiciary provided they follow the provisions outlined below:

- It is unacceptable to send e-mails that contain discriminatory statements, including those that malign any race, creed, color, gender, or sexual preference.
- It is unacceptable to send information through email that could reflect poorly on or cause embarrassment to the judiciary.
- It is prohibited to use email for illegal activities.
- It is prohibited to use email for political activities.
- It is advised not to forward emails from outside sources that could have harmful content.

When emails are sent within the judiciary, they remain inside the DCN. In accordance with the Guide to Judiciary Policy Ch3: IT Security[2] sending sensitive judiciary information to or through a personal web email accounts outside the judiciary network is highly discouraged. The email accounts do not offer the sufficient security or privacy. There are limitations with e-mail when sending messages and attachments outside the judiciary. Messages sent outside of the judiciary are not secure. These could potentially be read or broadcast without the knowledge or consent of the author. Users should not expect the messages that are sent or received via the Internet to be private. E-mail can also be unreliable. Delivery and delivery times are not guaranteed due to unpredictable intermediary system outside the control of the judiciary. Consequently, users should not rely on email for time-sensitive communications or guaranteed delivery outside the judiciary. 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. Outlooks "Receipt Requested" feature will not work for messages going outside the judiciary.

Large messages, messages with large attached files, or messages sent to large numbers of recipients are discouraged. Distributing software, graphics, or images via e-mail causes congestion and places a burden on the email storage and delivery systems. To protect the flow of e-mail, the judiciary has imposed a 5 MB limit on Outlook and Internet email messages. This means that if the total size of a message and any attachments exceeds 5 MB, the message will not be

[2] Guide to Judiciary Policy Ch 3: IT Security **§ 330.50:** http://jnet.ao.dcn/policy-guidance/guide-judiciary-policy/volume-15-information-technology/ch-3-security#330_50

delivered. Users will receive automatic notification that their message was too large to be delivered. If there are work-related needs to transmit such messages, contact the IT Help Desk.

Access to Internet email grants users the ability to subscribe to a variety of Internet services which will automatically deliver information to the user. Users should refrain from entering their court address on websites. This can generate an enormous amount of email traffic junk mail, spam, and potentially inappropriate email. Because all this information enters the Outlook mail system, it can have a significant impact on the flow of e-mail throughout the circuit. Subscriptions should be kept to an acceptable minimum and only be for job related or court assigned duties.

Conduct

Email users are expected to conduct themselves in a professional manner. The email system is for business use only and should not be used as a forum for soliciting personal goods and services, promoting charities or other discussions of personal viewpoints or other personal matters. The level of civility and decorum befitting the judiciary should be observed at all times.

Maintenance

Keep the number of stored e-mail messages to a minimum to save network space and to help with system maintenance. It is the user's responsibility to delete old e-mail messages and empty their trash folder on a regular basis. Contact the IT Help Desk for assistance in learning how to manage your email.

Security

A person who gains access to your e-mail account will be able to read your e-mail and may send messages to others in your name. Each user is responsible for the security of his/her e-mail account. To ensure your email will not be available to unauthorized users when you are away from your desk, lock your computer (Windows icon + L) when stepping away, or log off your computer before you leave at the end of the day.

SOCIAL MEDIA GUIDELINES

Social media consists of numerous web applications that are used by many of us on a daily basis. Organizations and individuals connect and communicate through social networking Internet sites and disseminate information through Facebook, Twitter, Instagram, YouTube and numerous others. Some users seem less concerned about privacy and confidentiality as they navigate social media sites. Numerous news stories illustrate the privacy and confidentiality concerns generated by the expansion of social media Internet usage: employment opportunities lost because of Facebook profiles, scandals caused by YouTube or Flickr postings, and judicial proceedings compromised by jurors' Twitter postings.

The challenges and risks of social media environments are particularly critical for government employees who work in the courts where discretion and confidentiality are imperative. Sensitive information should be kept confidential and discretion should be exercised to avoid a breach of public trust to the Court and take precautions to avoid unnecessary security risks for all court personnel.

It is recommended that the following guidelines are used when participating in social media services and/or social networking:

1. **Think before you post.** Content on social media web sites (whether it be text, photos, videos, or audio) remains accessible long after forgotten by the user. Keep in mind that nothing is "private" on the Internet despite 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 the newspaper.

2. **Speak for yourself, not the court.** On social networking sites, many individuals list their occupations and/or places of employment. Considering the sensitive nature of the work that we do, court employees should carefully evaluate whether the listing of their place of employment on a social networking website poses a security risk. Also, remember that you are a representative of the Court and should conduct yourself in a way to avoid bringing embarrassment upon yourself and the Court. All judicial employees are required follow the

principles, values, standards and rules of behavior set out in the *Code of Conduct for Judicial Employees*[3] to ensure fairness, impartiality and competence in the performance of duties. In the age of Facebook, YouTube and Twitter, many employees often do not consider the implications of the materials they post. Users often believe that postings are private because of a social networking website's privacy features or that their comments are untraceable because they were made under a screen name, but this information may not be private and could cause damage to your reputation and the court's if it becomes public. Also, it is best to avoid commenting about any case.

3. **Keep secrets secret.** Employees are responsible to abide by all of the court's confidentiality and disclosure provisions. Court employees handle confidential, sensitive information, and the restrictions that employees normally observe in the performance of their day-to-day duties should also apply to their use of social media. Just as court employees are prohibited from disclosing sensitive, non-public information to the media and general public in person or over the phone, the same applies to social media. Court employees should refrain from disclosing any of the Court's internal processes and procedures regardless if they are of a non-confidential or confidential nature.

4. **Be mindful of security concerns.** Court employees must always use good discretion and avoid participating in activities that would compromise the security of the courthouse and personnel. Employees are prohibited in posting pictures of the courthouse (inside or outside), posting pictures of court events and posting pictures or schedules of the Court's judicial officers.

REMOTE ACCESS

Employees, with the approval of their judges or court unit executives, have access to court-provided IT services when they are not in the office through a Virtual Private Network (VPN). VPN accounts are limited to those users who have a legitimate job-related need for remote access. Remote access to the case management system may be granted by the court unit executive. If approved, the IT staff will provide the necessary access.

Use of case data is restricted solely to the approved user and the confidentiality of all non-public information must be maintained.

Since the VPN permits access to the judiciary's private data network (DCN), users must follow all of the policies and guidelines set down in this handbook. In addition, VPN users must take extra precautions to protect the security of the network by adhering to the following requirements:

- An individual's VPN account must not be shared, even with another court employee.
- Users must maintain proper security over their account information. This is particularly important when the VPN is accessed from a home computer or one shared by others.
- Users must keep the remote computer current with all software and hardware updates and have anti-virus/anti-spyware protection installed and up-to-date.
- If connected to the VPN at home through a wireless connection, it must be configured with proper encryption technology.
- Users must disconnect from the VPN when the service is no longer required or the PC is idle.
- The IT staff can assist with any questions relating to the VPN and how to secure the remote computer used for access.

SOFTWARE

[3] Code of Conduct for Judicial Employees - http://jnet.ao.dcn/Guide/Vol_2_Ethics_and_Judicial_Conduct/Part_A_Codes_of_Conduct/Ch_3_Judicial_Employees.html

All software must be installed either directly by the court IT staff or with their knowledge and assistance. This is to ensure that any software used by employees on court-owned equipment is compatible with existing computer systems and court resources; properly installed, maintained, used and upgraded; free of any computer virus; and properly licensed. Software installed on court-owned equipment that does not comply with these guidelines may be removed by IT staff. Employees who do not follow the policies and procedures set forth may be held liable for violations of copyright laws and may result in disciplinary action, up to and including termination.

There are situations where software may be installed with or without the user's knowledge that allows for functioning court approved applications. Contact the IT staff for further information.

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.

Demonstration Copies of Copyrighted 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 and tested in consultation with the Clerk of Court and the Director of Information Technology.

Shareware

Shareware allows a user to try out software before paying a license fee. Since it is similar to demonstration software the same policies apply to its testing, purchase, and installation as described above.

Publically Distributed Software

Public domain software refers to programs that are not copyrighted and may be distributed at no cost. While the use of public domain software is discouraged, it may be used with the prior approval of a judge (or Clerk of Court) and the Director of Information Technology. Judges and court unit executives are advised to contact the IT Help Desk prior to approval to ensure that the software will not conflict with other installed applications. All public domain software must be scanned for viruses prior to installation.

Court-Developed Software

Software developed by the Administrative Office or by a local court unit may be distributed directly to court employees by IT staff or the AO. All such software must be scanned for viruses prior to installation. The court IT staff should be contacted before installation.

Peer-to-Peer File Sharing Software

Peer-to-Peer (P2P) (i.e. Spotify) computing or networking is a distributed program that partitions tasks or workloads between peers. Peers make a portion of their resources, such as processing power, disk storage or network bandwidth, directly available to other network participants, without the need for central coordination by servers or stable hosts.

Access to files and applications in P2P are granted based on job description. P2P software can jeopardize the integrity of the DCN as well as the privacy of the user. This type of software can also put a user computer at risk of spyware, malware, and Trojan Horses. P2P software is prohibited and should ***NOT*** be installed on any user computer. The Court provides means for file storage and sharing that is setup securely by the IT Staff for the use of the court's users.

Privately-Owned Software

In general, employees are prohibited from using personally-owned software on Government equipment. If the judge or court unit executive deems it in the best interest of the court to allow personally-owned software to be installed on court-owned equipment:

- Authorization should be granted in writing by the judge or court unit executive showing justification.
- Prior to installation, the employee will provide the Director of Information Technology with the software license and give assurance, in writing, that copyright infringement will not occur from installation on court owned equipment.

- The Director of Information Technology (or Office of Information Technology) will maintain a record of the installation of this software including a copy of the license and a signed statement by the employee indicating there are no copyright infringement issues.
- It is possible that, after installation, this software could be erased, or otherwise made unusable in the course of regular maintenance or upgrades by IT staff. To ensure that the software is not totally lost, the employee is responsible for keeping a proper backup copy in accordance with the license agreement.
- The employee is responsible for notifying the Director of Information Technology when the software is no longer needed so that it can be properly removed from the equipment.
- Employees not following these procedures may be held personally liable for violations of copyright laws and may be subject to the applicable penalties.

MALWARE

Malware[4] (malicious software) is software inserted into a system, usually covertly over the Internet or email, with the intent of compromising the confidentiality, integrity or availability of a user's data, application or operating system or otherwise annoying or disrupting the user. Malware includes computer viruses, worms, trojan horses, spyware and adware. Malware may be invisible to the user and may not show apparent damage beyond spreading to other portable storage media or files across the network. Malware can destroy or corrupt data, deny access to services, and spread to other computers across the network.

Contact the IT Help Desk at the first indication (or suspicion) of malware. Possible signs of malware include:

- Personal computer is sluggish or locks up
- New file names appear
- Files are corrupted
- Unexpected or strange messages appear
- New dates appear
- Files grow
- Disk is unusable
- Memory capacity decrease

The judiciary uses licensed anti-virus programs for use on all government provided workstations and laptops. In addition, this software is licensed and available for installation on employees' personally owned computers both for use with judiciary business from home and for personal use. Contact the IT Help Desk to request a copy of this software for installation on your home computer.

When antivirus software is installed on a workstation, the files and system requests are continuously scanned as data is read and written to the local or network drives. This occurs in the background and most users are not aware that it is happening. An auto-protect feature is also included in this software. This feature eliminates the need to scan individual disks, additional drives, and USB drives. If an infected file is read from an external drive, the user is alerted of the risk. Contact the IT Help Desk immediately for directions.

The antivirus software is upgraded periodically by the IT staff in order to take advantage of new security features provided by the vendor. Antivirus, malware, and spyware signature updates are completed automatically (Computers must be powered on to receive the updates; users do not have to be logged in to the network). Users should report failing software or issues with the software to the IT Help Desk upon discovery.

New strains of malware appear daily on the Internet and are not always caught by even the most up-to-date program. The following guidelines will assist you in avoiding malware on your computer.

[4] Malware definition - http://en.wikipedia.org/wiki/Malware

- Scan files for malware before they are copied to/from any data storage media.
- Make certain that all executable files (programs) have been scanned and approved before using.
- Protect your data by saving it to the network drive.
- Never attempt to start a computer with portable media inserted.
- Do not open email attachments from an unknown source or from whom you were not expecting email.
- Do not follow any Internet links unless you are absolutely sure they are safe.
- Stay clear of disreputable websites.

COMPUTER SECURITY AWARENESS

Users are the first and best line of protection from compromise of data to judiciary systems. Most breaches of computer security are attributable to computer users. This means that computer security rests in the hands of the users of computer systems. You are essential to providing security to the data and the machine entrusted to you.

New technologies are increasing computer security risks. Networks, telecommuting, mobile communications and portable computers mean that important, sensitive data are more exposed to risk. Each of the previous sections of this handbook describe the critical areas you need to address to improve computer security. It is the responsibility of each employee of the U.S. District Court, Eastern District of Kentucky, to put the standards described in this handbook into action to protect the sensitive and mission critical information of the court.

To ensure all employees keep current as technology continues to change, the IT staff from time-to-time will provide computer security awareness training to better educate and prepare users on current threats. To ensure that employees are aware of their security responsibilities, and to certify they have received the most recent policies and procedures, staff will be required to sign the Computer User Memorandum of Agreement. A copy of the Agreement appears at the end of this Handbook.

The security of our systems requires the vigilance and commitment of each and every system user - We are all gatekeepers.