UNITED STATES DISTRICT COURT
MIDDLE DISTRICT OF PENNSYLVANIA

INFORMATION TECHNOLOGY USAGE AND SECURITY POLICY

Any employee who violates this policy will be subject to the full range of disciplinary actions, including termination. The Court also has the right to notify the appropriate authorities if evidence is discovered of any possible illegal activities. This privilege to use government equipment for non-governmental purposes may be revoked or limited at any time.

A. PURPOSE AND SCOPE

The United States District Court for the Middle District of Pennsylvania, United States Bankruptcy Court for the Middle District of Pennsylvania, and the United States Probation Office for the Middle District of Pennsylvania (hereinafter collectively referred to as "the Court") have adopted this policy concerning the use and security of Information Technology when employees are performing official duties. This policy applies to all Court employees.

B. DEFINITIONS

Employees

Includes all permanent and temporary employees, law clerks, students, externs, and interns.

Information Technology

Information Technology refers to, but is not limited to, all Court-provided electronic equipment, computers, hardware, software, tablets, laptops, cell phones, telephones, email, and internet access. It also includes employees' home computers when they are used to gain access remotely using the Court's Virtual Private Network ("VPN") via J-Port or other VPN software.

Intranet/DCN

The JNet and the internal web sites are intranets that are used within the federal judiciary, and operate within the Data Communications Network ("DCN") provided and supported by the Administrative Office of the U.S. Courts ("AO"). They are designed to provide a means for organizing and disseminating information for internal judiciary use. Employees 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.

Internet

Access to internet resources is provided to employees through the DCN. Internet access includes, but is not limited to, viewing web sites, sending and receiving email, transmitting or downloading files, running applications and making transactions via the DCN.

Remote Access/VPN/J-Port

Remote access to Court systems is achieved through an AO-provided virtual private network (VPN) connection through J-Port or other VPN software. VPN access is provided for the convenience of the Court, and must be used only for approved official business.

C. GENERAL RULES

This policy hereby incorporates by reference, the Code of Conduct for Judicial Employees, Judicial Conference of the U.S. Courts (*JCUSC*) Policy, and the Guide to Judiciary Policy (the *Guide*) which are applicable to all work using Information Technology. Specific sections of such policies include but are not limited to, the following"

The *Guide*, Vol. 15, Ch. 5, § 525 Personal Use of Government-Owned Office Equipment
The *Guide*, Vol. 15, Ch. 3, § 330.50 Personal Web Email Account Access Discouraged
The *Guide* (Vol. 15, Ch. 3, § 330.40 Prohibition of Peer-to-Peer File Sharing, Chat Rooms, and Instant Messaging (IM) states:
The *JCUSC* Committee on Codes of Conduct Judiciary's Social Media Resource Packet

Employees are expected to conduct themselves professionally and are prohibited from storing or transmitting obscene, profane, or indecent materials, or any form of discriminatory or illegal material.

D. EMAIL

Email messages sent to internet addresses should **not** be considered confidential. The internet is an unsecured network. As such, information and email on the internet can be read, broadcast, or published without the knowledge or consent of the author. At no time should an employee forward a "chain letter" email message or inappropriate email messages. Confidential work files, such as opinions, proposed orders and presentence investigations, must not be attached to or transmitted by email to or from a location outside the DCN, such as from an employee's personal email address.

Employees should not open suspicious/phishing emails and should be wary of messages with frequent misspellings or incorrect grammar. Report suspicious/phishing emails to the unit's IT department for investigation and implementation of proper security safeguards.

E. MONITORING AND BLOCKING

Use of internet services provided through the DCN is subject to monitoring for security and/or network management reasons. For example, many internet sites record who accesses their resources and visits their sites, and may make this information available to third parties without the knowledge or consent of the user. Employees using Information Technology are advised of this potential monitoring and consent to monitoring. This monitoring may include the logging of which users access what internet websites. Additionally, to protect the users of the internet from inadvertently being routed to an unacceptable site, blocking software and hardware have been installed on the Court's local network.

The following site categories will always be blocked unless otherwise approved:

- Adult/Sexually Explicit
- Chat Rooms and Instant Message
- Gambling

• Hacking
• Intolerance and Hate
• Illegal Drugs
• Peer-to-Peer file sharing networks
• Phishing & Fraud (identity theft)
• Spyware (live viruses)
• Streaming Entertainment Sites (HBO2GO, Hulu, Netflix, etc.)
• Tasteless & Offensive
• Violence

Employees may have an official purpose in accessing a blocked site, or an appropriate site may be blocked for some unknown reason. If this is the case, access rights may be restored, upon email request from an employee's unit executive or judicial officer to the unit's IT department. Such a request must indicate the specific site that is blocked and the reason access is needed.

F. UNACCEPTABLE USE OF INFORMATION TECHNOLOGY

Employees must adhere to the same code of ethics that governs all other aspects of employee activity. Accordingly, employees may not use Information Technology for prohibited activities that include, but are not limited to:

- Making unauthorized statements regarding Court policies or practices;
- Unauthorized transmissions of confidential information (such as that relating to sealed cases, ongoing investigations, litigation or procurement);
- Making unauthorized commitments or promises that might be perceived as binding the Court;
- Unauthorized use of subscription accounts or commercial services;
- Sending or displaying messages or pictures that are obscene or sexually explicit;
- Using Information Technology for activities that are illegal, inappropriate, or offensive to fellow employees or the public;
- Personal profit;
- Political, fund-raising or lobbying activities, or any illegal activities;
- Distributing information that includes copyright violations such as software piracy (the Court may incur a legal liability for unauthorized copying of files or software even if the copy is used for official business);
- The creation, copying, transmission or retransmission of chain letters or mass mailing regardless of the subject matter;
- Using unauthorized (outside the DCN) streaming technologies on the internet that continuously stream data through the network. Examples include, but are not limited to watching a video from Netflix, ABC.Com or listening to an internet radio station; and
- Using Information Technology as a platform or staging ground to gain unauthorized access to other systems.

G. INTELLECTUAL PROPERTY RIGHTS

Employees shall give intellectual property appropriate credit when files or portions of such files are used while carrying out official duties.

H. PRIVACY ISSUES

All electronic documents created or stored, and all communications using Information Technology, are the property of the Court. The Court may access documents or communications stored on its property or in its systems whenever warranted by business need or legal requirements; and it will periodically monitor its systems for accounting purposes, to assure proper use, and to prevent security violations. Employees should not expect that their communications using Information Technology are private or confidential.

I. USE OF SOCIAL MEDIA

Employees must refrain from discussing any of the Court's internal procedures or processes. Court personnel are expected to keep sensitive information confidential, exercise discretion to avoid embarrassment to the judiciary, and take precautions to avoid security risks. Judicial employees should carefully evaluate whether listing their place of employment on a social networking website poses a confidentiality and/or security risk. Do not post pictures of the courthouse, inside or outside; pictures of Court/training events; or pictures of the Court's judicial officers.

J. FILE TRANSFER

To prevent malware and viruses from being transmitted through the Court's email system and network, downloading of software and unapproved files is prohibited. If a software program is needed, please contact IT for assistance. Downloading of files for business purposes is permitted. An example would be downloading a PDF, MS Word, or WordPerfect file from another judiciary site. Downloading files for personal use is not permitted.

K. INSTANT MESSAGING AND PEER-TO-PEER FILE SHARING

The Instant Message (IM) feature available through the approved email program, which functions within the DCN, is the only acceptable IM software for use by employees.

L. SAFETY

Employees' use of Information Technology while driving is prohibited unless a hands-free device is used. Texting while driving is strictly prohibited. Employees are required to abide by applicable state and local laws.

M. PHYSICAL SECURITY

Employees are expected to take care of the Information Technology assigned to them. In this regard, employees should avoid eating or drinking nearby Information Technology; keep their

work area clean; refrain from plugging other equipment, such as portable heaters, into the same surge protector as the Information Technology.

N. OPERATIONAL SECURITY

Passwords

When the network, email and CM/ECF user accounts are set up, each employee is assigned a password. All passwords must be changed every 180 days. Passwords must be protected and must not be given to any outside party other than your supervisor or the IT staff as required for business and support reasons. Use the following guidelines when selecting passwords:

- Passwords must contain a combination of letters and numbers/symbols and must be at least 8 characters in length;
- The password cannot include your username;
- Do not use names spelled backwards, names of a pet or relative, hobbies, birth month;
- Passwords should never be related to someone's identity, history or environment;
- Randomly replace letters with numbers/symbols - “Icecream” becomes 1c3cr3@m; and
- Pick a sentence, i.e. your passphrase, and reduce it to first letters of each word - “It was a Dark and Stormy Night!" becomes IwaDaSN!

Locking, Logging off and Restarting Computers

The screen saver can be enabled so employees can lock down their computer when they are away from the computer by pressing The Windows key (⊞) + L to lock the computer. This method should be used whenever an employee leaves his/her work area or will later need remote access to his/her computer; otherwise, at the end of each workday, an employee shall log off.

Malware/Virus Prevention

All Court computers have malware/virus prevention software installed. Malware is short for "malicious software," and refers to software programs designed to damage or do other unwanted actions on a computer system. Common examples of malware include viruses, worms, Trojan horses, and spyware. Malware can cause security problems on a computer's system including deleting files or directory information or by gathering data. Malware infection may be invisible to the user and may cause no apparent damage beyond spreading to other media or files across the network. However, malware can destroy data, damage data integrity, deny access to service, and spread problems to other computers on the network.

The Court has licensed anti-virus software for use on all Windows computers including laptops and notebooks. This software will scan files automatically. No user action is required to perform the virus scanning. Employees can request a copy of the anti-virus software for home use at no cost by sending a message to IT.

Software

Software may only be installed on Court Information Technology by the unit's IT department.

If personal software is required, an employee must first obtain written prior approval from the unit executive or judicial officer before sending a request to the IT department. Employees may modify configuration preferences on Court-provided IT mobile devices and may install personally acquired applications as long as they are obtained through a private account with the AppStore, Google Play or similar service.

System access
Employees shall 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. If an individual seeks illegal or unauthorized access to sensitive information or if an employee has knowledge of an actual or attempted exploitation, he or she should notify the IT manager.

Portable Data Storage
Removable storage media, such as USB thumb drives, flash drives, etc. are **prohibited for use** within the Court's network, unless explicitly approved by the judicial officer or your unit executive. When permission is given, the portable storage device shall be password protected via encryption if it is used for sensitive data in order to prevent potential access should the device be lost or stolen. Contact IT for assistance to encrypt the storage media.

O. COURT-PROVIDED AND PERSONAL DEVICES

Only Court-provided devices are permitted access to the Court's wired and wireless network. Employees can use the webmail web site to access work email on a personal device by visiting https://login.microsoftonline.com. The IT staff will not install the court email program on personal devices unless the IT manager receives a request from the employee's unit executive or judicial officer. No employee may use the Court provided wireless system for video conference services such as FaceTime unless approved by the unit executive or a judicial officer.

Employees may not install personally owned hardware (e.g., an external CD ROM drive, monitors, CPUs) on office equipment. If there is a Court need for personal hardware to be loaded on office equipment, employees must first contact the IT manager. If it is approved, the installation will be handled by IT.

P. COMPUTING RESOURCES IN PRIVATE RESIDENCES

Upon determination by a judicial officer or the unit executive that Information Technology is available, and that its use is in the best interest of the Court, such resources may be provided under the following conditions:

All policies and procedures set forth in this document apply.

No internet connection can be provided at government expense for use with the equipment.

The employee is responsible for the equipment and must read, sign and comply with the provisions of the chargeable property receipt for the equipment.

The IT Department is responsible for maintaining an inventory of the equipment, repairing it, and seeing it is returned when the employee no longer needs it or leaves Court service.

The authorization to use the equipment must be reviewed annually.

While IT staff will install appropriate software and provide set up instructions, the employee is responsible for setting up, maintaining, and removing the equipment from his/her residence.

This policy may be amended at any time by the District IT Committee.

Judge's Signature

May 25, 2018

CERTIFICATION

To ensure that you are aware of your Information Technology usage and security responsibilities and to certify that you have received the most recent policies and procedures, you are required to consent to the Information Technology Usage and Security Policy using the link below. Contact your IT Manager if you have questions about any part of the policy. If a need arises to create an exemption to a part of this policy, please contact your judicial officer or your unit executive. If the exclusion is approved, installation or setup procedures will be handled by IT.

UNITED STATES COURT

MIDDLE DISTRICT OF PENNSYLVANIA

Information Technology Usage and Security Agreement

The security of our computer systems requires the vigilance and commitment of each and every network user. As a user of computers, peripherals and networks in the Middle District of Pennsylvania, I acknowledge my responsibility to follow the requirements and conditions established by the Information Technology Security Usage and Security Policy. 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, up to and including termination

To submit your agreement click here then send via email