

UNITED STATES DISTRICT COURT
Middle District of Pennsylvania
IT Department



Appropriate Use and Security Policy and Agreement

Contents

Revision Log.....	4
Overview	5
Guidance	5
A. IT Security Policies and Plans	5
B. Court IT Security.....	5
1. Audits.....	5
2. IT Security Officer (ITSO)	6
C. General Computer Usage Security Policy Information.....	6
Applicability to Interns.....	7
D. Policy on IT Security for All Users.....	7
1. Physical Security.....	7
2. Securing Laptop Computers and Cell Phones	8
3. Software Security - General Policy	8
4. Data Backups	9
5. Network Management, Security, and Access	9
6. Passwords.....	9
7. Virus and Malware Avoidance	10
8. Incident Response Plan	11
9. IT User Security Training	11
10. Local User and Administrative (Privileged) Accounts.....	11
11. Remote Access and Desktop Support.....	12
E. Policy on Internet Usage	13
1. Internet Access.....	13
F. Policy on E-mail and Messaging	15
1. Conduct.....	15
2. Attached Files.....	16
3. Maintenance	16
4. Security	16
5. Web E-mail is Prohibited	16

G. Policy on Hardware and Software Installation	17
1. Personal Hardware is Prohibited	17
2. Software on Courts owned PC, Laptops and Smart Phones	17
3. Copyrighted Software.....	17
4. AO/Court-Developed Software assets.....	17
5. U.S. Courts' Software on User-Owned Personal Computers/Laptops	17
6. Maintenance	17
H. Policy on Social Media	18
1. Use of Social Media	18
2. Principles.....	19
3. Responsibility	19
4. Relevant Technologies	19
5. Rules	20
6. Productivity Impact While in Work Status	22
7. Terms of Service.....	22
8. Off-Limits Materials	22
9. Disciplinary Actions	23
I. Computer Policies User Agreement.....	23
J. Windows Service/Admin Account.	24
Policy Review	24
Exceptions	24
Policy Authorization	24

Revision Log

Date	Description	Editor
Dec. 2019	Initial Policy	AL
March, 2020	Updated, signed, and adopted	AL
Feb. 2021	Removed reference to Symantec Anti-Virus	AL
Feb.2022	Changed Systems to IT	AL

Overview

This document outlines the United States District Court for the Middle District of Pennsylvania (PAMD) appropriate use of Information Technology (IT) assets and the security requirements for users and IT Department staff, as mandated by the Guide to Judiciary Policy, Volume 11: Internal Control - Chapter 6: Information Systems and Security and Volume 15: Information Technology.

<http://jnet.ao.dcn/policy-guidance/guide-judiciary-policy/volume-11-internal-control/ch-6-information-systems-and-security>

<http://jnet.ao.dcn/policy-guidance/guide-judiciary-policy/volume-15-information-technology>

Guidance

In accordance with the Guide to Judiciary Policy, policies and procedures must be developed for the appropriate use of judiciary computer systems. (Volume 15, § 310.20.10.) http://jnet.ao.dcn/policy-guidance/guide-judiciary-policy/volume-15-information-technology/ch-3-security#310_20_20. Employees, including IT staff, are responsible for the proper use of, and security measures for, government computers and the automated systems and data. (Volume 11 § 640 (c).)

<http://jnet.ao.dcn/policy-guidance/guide-judiciary-policy/volume-11-internal-control/ch-6-information-systems-and-security#640> . PAMD has a set of policies to fulfill these requirements, which includes this document.

A. IT Security Policies and Plans

The following IT security policies and plans are in effect at PAMD and are reviewed by the Clerk of Court or designee, IT Director, and IT Security Officer at least annually or as needed.

1. Access Control Policy
2. Appropriate Use and Security Policy Agreement
3. Security Awareness Training Policy and Plan

4. Backup Storage Recovery Plan
5. Configuration Management Policy and Plan
6. Contingency Planning and Disaster Recovery Policy
7. Incidence Response Policy and Plan
8. Log Management Policy
9. IT Maintenance Policy and Plan
10. Media Sanitation and Information Disposal Policy
11. Network Management Policy and Plan
12. Password Policy
13. Patch Management Policy and Plan
14. Witness Protection Policy
15. IT Exception Policy
16. Remote Access Policy
17. Wireless Technology Access Policy
18. Systems Security Policy and Plan
19. International Travel Policy

B. Court IT Security Officer

1. **Audits** - *Guide to Judiciary Policy, Vol. 11, Ch. 6* provides Internal Control procedures for Information Systems and Security. The procedures provide what reviews are to be done, their frequency, and the position responsible for oversight of these reviews. Internal Control audits are performed annually at a time designated by the Clerk of Court.

Guide to Judiciary Policy, Vol. 15, § 310.20.20 provides details for the Judiciary IT Security Scorecard. The Scorecard will be completed and submitted each year by December 31 by the IT Director or ITSO.

2. **IT Security Officer (ITSO)** - The Court IT Security Officer is designated in *InfoWeb* and by a written memorandum from the Chief Judge. The ITSO has the primary day-to-day responsibilities for coordinating and facilitating information

security issues within the court, creating IT security policies, plans and ensuring their enforcement. The ITSO is a senior position within the Court and therefore has the full authority to take all actions necessary to stop an immediate or emerging threat to the Court's data, systems, and networks. Further, the ITSO has the authority to direct IT Department employees to assist with the protection of the Court's IT infrastructure. Because of the importance of IT security within the court. Although the ITSO position falls within the IT Department, the ITSO reports to the IT Director, Chief Deputy Clerk, Clerk of Court, and Chief Judge on matters of Court IT security.

C. General Computer Usage Security Policy Information

This portion of the Appropriate Use and Security Policy is to acquaint users with computer related security practices that shall be followed by all employees of the Court. Court users are the best defense against malware infections, loss of court data and property, and maintaining an overall high level of IT security posture in the workplace.

User education and user policies are two critical components of overall risk management. The following policies have been established to decrease security risks, ultimately protecting the Court, the employee, the Judiciary-wide Data Communications Network (DCN), PAMD's data, systems, and networks assets. The information contained in this guide is intended to:

- Raise awareness of computer security;
- Define the responsibilities of users;
- Assist users in recognizing potential problems; and
- Provide guidance if a compromise in security is suspected

Every Court employee will be required to sign the Computer Policies User Agreement (*at the end of this policy*) signifying their agreement to adhere to this

and referenced policies. In rare circumstances, if the need arises to create an exception to policy, then the user must first obtain the Clerk's or Management written approval using the Exception to IT Security Policy procedure.

This policy does not create any right to use government-owned equipment other than official government business, nor for inappropriate personal use. Judiciary employees are specifically prohibited from using government-owned equipment in the furtherance of a private business. Nor does the privilege extend to modifying such equipment, including loading personal software or making configuration changes.

Unauthorized use and/or access to information, files, or data not related to an employee's assigned duties may result in disciplinary action and possible termination. Using judiciary-provided access to online investigative tools and databases containing personal information to gather information for non-work-related purposes is prohibited, including attempting to research friends, neighbors, acquaintances, celebrities, other public figures, etc. Online investigative tools include LexisNexis and Westlaw public records or other databases that may contain personal information (e.g., telephone, driver's license, auto registration and VIN numbers, home addresses, property ownership records, voting records).

Access to the internet will be provided in the office for Court business. Each user and each user's manager will need to exercise individual responsibility and sound judgment to ensure the acceptable and appropriate use of internet services as described in the [*Policy on Internet Usage*](#) found in the document. All internet access is monitored to ensure that nefarious sites are not accessed.

Users are expected to conduct themselves professionally and should not save, download, and/or transmit any documents or e-mail which contains confidential,

indecent, or obscene materials, profanity, or any form of discrimination or sexism.

Regarding social media, the Code of Conduct for Judicial Employees applies to all online activities. See the *Policy on Social Media* found in this document.

Applicability to Interns:

The security policies found herein also apply to interns (law students selected by the District Judges to work in Chambers for a short period of time). Interns will be expected to abide by all PAMD's IT Appropriate Use and Security requirements outlined in this policy. Each Intern will be required to agree to all policies and procedures by signing the *Computer Policies User Agreement* found at the end of this document and the Court's *Policy on Social Media Agreement* found in this document prior to being allowed access to the Court's Data, Systems, and Network. Any violation by the Intern may lead to immediate termination of the Intern's network access privilege with the Court. Interns will not be allowed to:

- Make any changes to any objects on the network, such as servers, printers, and shared folders;
- Make any changes to local computers or computer accounts;
- Make any changes to files located within the network shared folders, except for Chambers files permitted by the appointing District Judge;
- Make any changes to computer programs running on the local computer;
- Download non-work related programs, files, or content from the internet;
- Access dcn_gtwy (wireless access), JPORT, or the DCN using unapproved private SSL VPN providers;
- Copy any court owned or Judiciary owned computer programs, files, and intellectual properties;
- Access spaces other than those specifically designated in Chambers or Intern's area by the appointing District Judge or HR.

D. Policy on IT Security for All Users

1. Physical Security

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

- Do not place liquids on or around your computer or keyboard and avoid dropping crumbs or any foreign materials on the keyboard, mouse, or scanner.
- Do not place non-removable stickers (passwords on sticky notes) on your computer, monitor, keyboard, mouse, or scanner.
- Do not place magnets (name tags, paperclip holders, etc.) on your computer equipment. Avoid plugging heaters and other appliances into outlets that share the same circuit as the computer because some appliances may overload the circuit causing the computer to lose power or incur damage.

2. Securing Laptop Computers, Smartphones, and Cell Phones

Due to their compact size, laptop computers, tablets, smartphones, and cell phones are particularly susceptible to theft. Take measures to ensure that they are either within sight or kept secure.

Laptop computers are the primary computers for court staff. When transported for travel or telework purposes, users will ensure that their computer equipment is always physically secure and that it is transported and used in a proper environmental setting. The Property Custodian will require each employee to sign for their equipment as part of the permanent court inventory record.

Employees that have approved telework agreements can take their assigned

laptops to their residence or other locations to perform their work-related duties. It is important for all employees to understand that they are individually liable for government-owned equipment in their custody.

3. Software Security - General Policy

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

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

All Court data, systems, and networks are the property of the Judiciary and the U.S. Government. All internet, telecommunications, and computer information systems are subject to monitoring to ensure proper functioning, to protect against improper or unauthorized use or access, to verify the presence of applicable security features, and the enforcement of policies. Such monitoring may result in the acquisition, recording, and analysis of all data being communicated, transmitted, or processed in the user's systems. If monitoring reveals possible evidence of criminal activity, such evidence may be forwarded to law enforcement officials.

4. Data Backups


See PAMD's *Backup and Storage Policy and Plan* for more information.

Important: Local laptop computer drives are not backed up. Users should not save important data to their local (C drive) because hard drives may "crash"

or be swapped out periodically to provide users with updated applications. Important data should always be saved in the appropriate network folder (drive). The IT staff is not responsible for users' data files that are stored on a local drive. If you have questions concerning backups, please contact the IT Department (570) 207- 5620 PAMD_Helpdesk@pamd.uscourts.gov

5. Network Management, Security, and Access

The user is responsible for maintaining a reasonably secure workstation. It is very important to close all applications before you leave for the day. Your screen will automatically be locked after 15 minutes of inactivity. The exceptions to this policy are Bench laptops, Courtroom Deputy workstations, and Judge's login accounts. The reason for these exceptions is that these specific sessions cannot time out when courtroom proceedings are in process. IT staff closely monitors associated computers to ensure they are restarted after hearings.

A good practice is to always lock your computer ( + L) or (*Ctrl+Alt+Del*) when you are leaving your immediate work area.

Except for IT staff, by policy, employees are not allowed to access the DCN using their personal computers or devices unless explicitly approved in writing by the Clerk. The Clerk may approve such use by e-mail during prolonged emergencies or other events that make the courthouse inaccessible. General Teleworking is not an approved reason for accessing the DCN using personal computers. This is to maintain a high level of network security and reduce the risk of zero-day malware infection to the court's systems and data. Although not a routine practice, the IT staff may occasionally access the DCN with their personal computers for testing or troubleshooting IT issues. When this occurs, every administrator login is captured and reported by SPLUNK e-mail alerts to IT Department staff.

6. Passwords

See PAMD's *Password Policy* for more information.

Protection of Passwords: - Improper protection of passwords may allow unauthorized entities or individuals to access the DCN or Court's data.

Passwords must be protected and not be given to anyone. An exception to this policy would be if IT support staff needs it for technical support purposes.

When this happens, change your password immediately after the IT support staff has resolved your issue. Passwords should never be provided to any outside party over the phone, by e-mail, or by any other means. Persons attempting to gain unauthorized access to the Court's systems may impersonate IT support or maintenance personnel, or even Court officials and judicial officers. If a user believes his/her login credentials have been compromised, contact the IT Department Immediately (570)207-5620

PAMD_Helpdesk@pamd.uscourts.gov .

7. Virus and Malware Avoidance

Virus and malware outbreaks are typically caused by executable files that replicate and attach themselves to other programs or macros in a covert manner. At first, an infection may be invisible to the user, with no apparent damage (even though malware could be spreading to other disks or files across the network). However, malware can destroy data, damage data integrity, deny user access to services, encrypt disk volumes and individual files, compromise systems, spread problems to other computers on the network, and impact the overall health of the local Court and the entire Judiciary's Data Communications Network (DCN).

If you encounter or suspect what seems to be a virus or malware activity on your computer or laptop, write down the error message or description of the problem and what you were doing at the time when you realized something was amiss. Do the following:

- Stop using the potentially infected computer immediately and
(do not restart).
- Immediately Contact the IT Department (570) 207-5620
PAMD_Helpdesk@pamd.uscourts.gov. The IT Department staff is the Computer Incident Response Team (CIRT) for the Court. The IT Security Officer (ITSO) has the lead role for the CIRT. For more information on appropriate responses for IT security incidences, see the *Incident Response Plan in this policy*.
All Court personnel will receive annual IT security training that will address how to respond appropriately to IT security incidences.

Techniques for Avoiding Viruses, Malware, and Spam:

What's the difference between Spam and Phishing?

Spam: Unsolicited Bulk e-mail that tries to sell a product or service like pharmaceuticals, dating websites, or financial services.

Phishing: a fraudulent attempt to obtain sensitive information by leveraging e-mails sent to a large group of recipients. e-mails are designed to trick the user into sharing sensitive and personal information, opening file attachments, or clicking poisoned links.

e-mail and the internet are the primary sources for malware infections. Be wary of file attachments, web pages, and web links from unknown outside sources, especially those found in e-mails enticing you to click. Pay attention to the sender's e-mail address and any embedded URLs or links within the message body.

e-mails and attachments received via e-mail are scanned for known viruses and malware prior to arriving in your inbox. But there is no effective method to scan for nefarious internet links within e-mails or attachments. If an e-mail is from an unknown source, be suspicious. Look for any misspellings or catchy phrases like "Open Now," "This is very important," or "Shipment Status," beware! Good advice is to hover over any of the links to determine

the validity and report suspicious e-mails to the IT Department; never forward suspicious e-mails. Avoid any e-mail attachment with a file extension ending in .exe, .bat, .zip, .vbe, or any other extension you are not familiar with. As employees of the Court, you should be receiving common Adobe (.pdf) and Microsoft Office extensions (.doc, .docx, .xls, .xlsx, .pptx, etc.) attachments. But even those cannot be completely trusted as there could be embedded malware within the document itself using a macro or script. As computer users, we are the Court's primary line of defense or the weakest link against malware outbreaks.

*****THINK BEFORE YOU CLICK*****

Flash/Thumb drives:

Personal external hard drives are not allowed to be connected to any court system or computer. Employees are prohibited from bringing personally owned disks or thumb drives from home to work. All disks and thumb drives obtained from outside sources pertaining to court business (filers, law firms, and Judiciary) need to be scanned prior to being used in the workplace. This includes media received from Judiciary sources and from Judiciary sponsored events. By policy, disks and thumb drives obtained from outside sources will not be loaded onto PAMD's IT system assets, including laptops, PCs, and servers, without first being certified that they are virus-free by the IT Department staff. Media will be scanned using a virus/malware program (e.g., Trend Micro Apex One/Deep Security) to ensure that the media is not infected. The IT Department staff will log the scan activity and results. Infected media will be immediately destroyed by the IT Department staff and will not be returned to the user.

8. Incident Response Plan

See the PAMD's *Incident Response Plan* for more information.

The purpose of the IT Incident Response Plan is to have a process in place to

manage IT-related security incidents that include theft, intrusions, hostile probes, and malicious software outbreaks. These "attacks" may be directed against both information systems and other types of systems, for example, telephonic systems. The attacks, whether directed at governmental or non-governmental organizations, have emphasized organizations' increased vulnerability to intrusion and incidences involving automated systems. As we expand our reliance on computing technology, its vulnerabilities greatly increase. The Plan addresses all phases of IT incident response handling and what steps need to be taken during each phase.

9. IT User Security Training

See the PAMD's *Security Awareness Training Plan* for more information. All employees will be required to participate in annual refresher IT User Security Training. New employees will receive initial security training within the first several days of employment. New employees will be required to attend security training and sign the *Computer Policies User Agreement*. The IT Director will be responsible for providing the venue for the training (online, video, or in-person) and will document the attendees. All IT Department staff need to participate in additional IT Security Training provided by AO's SDSO Training Division.

10. Local User and Administrative (Privileged) Accounts

Local Computer Administrative Accounts: Ordinary users will not be granted local administrative account privileges on their computers. There is **NO** exception to this policy.

Domain Administrative Accounts: IT administrators will use their personal privileged accounts (Domain Admin) only when necessary to troubleshoot and resolve problems. Otherwise, IT personnel will use their local user non-privileged accounts. Some older hardware, such as switches, printers, and VMWare hosts do

not allow for the creation of more than one administrative account. In those cases, a single administrative account will be used.

11. Remote Access and Remote Desktop Support

See PAMD's *Remote Access Policy* for more information.

In accordance with the *Guide to Judiciary Policy*: <http://jnet.ao.dcn/policy-guidance/guide-judiciary-policy/volume-12-human-resources/ch-10-telework>,

PAMD participate in the telework program to ensure continuity of operations in the event of natural disasters, terrorist acts, pandemics, inclement weather, or any other event that would interrupt normal operations. In addition, Active, Senior Judges and Court Staff routinely work from their residence and remote travel locations. To support teleworking efforts, PAMD approves the use of *Secure Socket Layer Virtual Private Network* (SSL VPN) offered by the AO https://jport.uscourts.gov/dana-na/auth/url_default/welcome.cgi and a second form of authentication also offered by the AO called *DUO*. DUO is a two-factor authentication protocol that strengthens remote access security by requiring two methods (also referred to as factors) to verify users' identity. These factors can include something you know - like a username and password, plus something you have - like a smartphone app to approve authentication requests. The IT Department can assist in the installation, configuration of remote access software and apps for approved users. (570) 207-5620

PAMD_Helpdesk@pamd.uscourts.gov

E. Policy on Internet Usage

This policy describes the acceptable use of the Internet, DCN, and PAMD's Intranet (SharePoint).

1. Internet Access

a) **General Policy:**

Use of the internet via gateways owned or operated on behalf of the United States District Court for the Middle District of Pennsylvania (PAMD) imposes certain responsibilities and obligations on Court employees and is subject to Court policies and federal laws. Acceptable use is always ethical and reflects honesty. It demonstrates respect for intellectual property, ownership of information, and system security mechanisms.

Internet usage provided by the Court is monitored (logged) for security, potential user abuse, and network management optimization. Users of these services are therefore advised of monitoring and agree to this practice by default when logging onto court computers. Monitoring will include logging of sites and resources being accessed by users. Users should further be advised that the Security Operations Center (SOC) at the AO monitors internet usage. Many internet sites also log information on those accessing their sites and may make this information available to third parties.

To protect users from inadvertently being routed to an unacceptable or malware site, web proxy servers (called Websense or Forcepoint Web Security) have been installed within the Court's networks. When on the court's network, access to "blocked" websites and pages will be denied and indicated by a pop-up message in the browser.

Categories for "blocked" and "allowed" sites are recommended by the Clerk of Court, IT Director, and or ITSO approved by the Court's *IT Security Committee*.

By participating in the use of internet connection provided by the Court, users agree to abide by this policy. Willful violation of the principles and provisions of this policy may result in disciplinary action or other actions deemed appropriate by the senior management.

b) Specific Provisions

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

Users will not utilize court networks or equipment for partisan political purposes or commercial gain. Users will not utilize court networks, e-mail, or messaging services to harass, intimidate or otherwise annoy another person or employee.

Users will not utilize the internet to disrupt other users, services, or equipment. Disruptions include, but are not limited to, distribution of unsolicited advertising, propagation of computer viruses, monopolizing and overloading the network with excessive high-volume traffic which substantially hinders others users' ability in their use of the network. Examples are streaming media, internet radio, Hulu, Netflix, YouTube, Apple, and Amazon streaming services.

Occasional personal use of the internet is allowed and will be treated similarly to local telephone calls. Users will keep the use of the Court's internet access for personal purposes to an absolute minimum. Users shall exercise discretion in such use and acknowledge that such use is logged and traceable to the particular support office and individual user. Personal internet usage will be brief, limited, and must not disrupt productivity in any way.

Below are some examples of unacceptable workplace internet usage, but not limited to:

- Collaboration with outside non-court groups or individuals on school homework or social activities

- Watching lengthy non-court or non-work-related videos (e.g., sports, tv programs) unless approved by a supervisor
- Accessing sites to perpetrate any form of fraud, and/or software, film, or music piracy
- Accessing Facebook, TikTok, or other social media sites
- Accessing retail coupon sites
- Violating the rights of others by publishing or displaying any information that is defamatory, obscene, known to be inaccurate or false, profane, or threatening
- Postings to informational sites, such as Wikipedia and WikiLeaks
- Use of Twitter and other texting sites
- Conducting employment searches
- Any applications that employ peer-to-peer file sharing, chat rooms, and instant messaging (except for the Judiciary approved IM and Microsoft Teams) are prohibited for communicating on the DCN, including but not limited to (see *Guide to the Judiciary Policy Vol. 15, 330.40*):
- http://jnet.ao.dcn/policy-guidance/guide-judiciary-policy/volume-15-information-technology/ch-3-security#330_40
 - Skype – free version (this is not Microsoft’s Skype for Business)
 - Messenger (Facebook’s IM)
 - WhatsApp Messenger
 - WeChat
 - Line
 - Viber
 - Telegram Messenger
 - Kakaotalk
 - IMO
 - Snapchat
 - TikTok
 - BitTorrent
 - Morpheus
 - Interactive internet games
 - Google Talk

Judicial Conference approved a judiciary-wide policy regarding access to the internet from computers connected to the DCN. The policy requires access to the internet to be provided only through national gateway connections approved by the Administrative Office (AO) pursuant to procedures adopted by the Committee on Automation and Technology.

By policy, users are not allowed to download or receive files directly from the internet from untrusted outside DCN sources. Proposed Orders are excluded from this provision. Contact the IT Department xt.5620 for assistance. For required files from other than trusted sources, the IT Department will scan the file with the current virus scanner (e.g., Trend Micro Apex One/Deep Security). Examples of trusted sources are JNET, and updates from Microsoft, Adobe, Oracle, Westlaw, and LexisNexis. Court IT staff, because of their duties, will need to download files from the internet using mandated security precautions as defined herein.

Users will not run any executable programs found on the internet without prior approval (e-mail) from the IT Department staff, IT Director, or the IT Security Officer. This includes but is not limited to any file with a file extension of:

.COM, .EXE, .SCR or .ZIP that is received via the public internet system, e-mail, or other messaging services.

F. Policy on E-mail and Messaging

The purpose of this policy is to provide guidance for proper practices for judiciary e-mail and instant messaging (IM) usage. e-mail and IM originated in any automated system application of the Court should be for official business only.

1. Conduct

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

communication. Keep in mind that it can be easily copied or forwarded to anyone without the sender's knowledge.

e-mail and messaging are not a forum for soliciting goods and services which are not directly related to official business. Use of personal e-mail and messaging on your cell phone, if approved, is allowed when not connected to the DCN_GATEWAY and shall be treated as a “local telephone call.”

Personal webmail will not be accessed using court provided workstation (PC). Users are reminded that personal usage will be brief, limited, and must not disrupt productivity. Use of personal e-mail and messaging is prohibited on Court provided workstation (PC) in accordance with *paragraph 5* of this section.

2. File Attachments:

Large file attachments should be used with discretion. The maximum allowable size for file attachments during business hours is limited to 30 MB per e-mail due to the overall effect on the bandwidth availability for all users. If you have larger files, attempt to break them up using several e-mails. Large attachments will also slow down your court e-mail application. It is highly discouraged for users to e-mail pictures and other personal items to their court e-mail account due to possible virus, malware, and privacy concerns.

3. Maintenance

It is the user's responsibility to manage, delete and archive old messages and empty their Deleted Items folders on a regular basis. The total size of the mailbox which includes inbox, trash, drafts, sent items, and deleted items should not reach a limit that impairs and limits mail client normal function. For assistance in archiving, deleting, and general mailbox maintenance contact the IT Department. (570) 207-5620. PAMD_Helpdesk@pamd.uscourts.gov

4. Security

Each user is responsible for the security of his/her account, which means one's login/password and e-mails must not be available to unauthorized users at any time. A person who gains access to your account will be able to read all your communications and send messages to others in your name. Employees are not to read other employees' e-mails or messages without prior permission. Users are encouraged to lock their active sessions when leaving the office for a prolonged period of time, or lunch. To further secure unattended computing sessions, the IT Department has imposed a screen inactivity timeout of 15 minutes which automatically locks idle sessions. IT Department staff may, from time to time, be exposed to users' e-mail while performing/answering support calls.

5. Web E-mail

The use of web e-mail (for example AOL, Yahoo, Gmail, Hotmail, and others) on Court computers is not allowed due to the increased security threat that it poses to the Court and the Judiciary. Because web e-mail uses an internet browser for access, some of the computer's security processes are bypassed and users could unknowingly download viruses, malware, or click on a link that leads to malware sites. All malware is to be taken seriously, but some malware can destroy or encrypt the Court's data, such as ransomware.

G. Policy on Hardware and Software Installation

1. Personal Hardware

Contact the IT Department (570) 207-5620 PAMD_Helpdesk@pamd.uscourts.gov for all hardware requests needs and installation. Personal hardware (e.g., an external hard drive or thumb drives, monitors keyboards and mouse or other pointing devices) is prohibited. If the need arises for personal hardware to be

attached to Court equipment, users must first contact the IT Department for approval and installation.

2. Software on Courts' PC/Laptops and Smartphones

IT staff will maintain and monitor software installed on all Court computers and devices. All computers and devices are subject to inspection and scanning at any time to ensure that only authorized software is installed and is up to date. Only authorized software is permitted, which is defined as software necessary for court operations. Personal software and applications are prohibited.

3. Copyrighted Software

Copyrighted software must not be installed, 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 will be procured, installed, and tested by the IT Department staff.

4. AO and Court-Developed Software

AO and other Court-developed software may be occasionally distributed directly to Court employees by the AO. All AO and other Court-developed software must be scanned for viruses prior to installation. IT Department staff must perform the installation.

5. Courts' Software on personally owned Computer/Laptop

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

is the responsibility of the user. Contact the IT Department (570) 207-5620 PAMD_Helpdesk@pamd.uscourts.gov for more information.

6. Maintenance

The IT Department is responsible for routine and emergency maintenance of IT systems (servers, printers, switches, laptops, smartphones, etc.). Members are assigned maintenance roles and are trained to perform system maintenance activities. These activities include, at a minimum, troubleshooting, activities for patch management, virus detection and remediation, firmware updates, and IT equipment repair or replacement. Typically, maintenance activities will be performed during non-court working hours by the IT staff. Some maintenance activities will need to occur during the workday, but the goal is to minimize disruption to court operations.

H. Policy on Social Media

This policy applies to all Court employees, including Chambers staff. There are Five Canons by which all judicial employees must govern their actions when using social media. Although not intended to be an exhaustive list, the Canons make up the core of the Code of Conduct for Judicial Employees and the impact use of Social Media.

Online 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

<http://jnet.ao.dcn/policy-guidance/ethics-and-financial-disclosure/primer-ethics-getting-it-right>

Additional Requirements:

1. Use of Social Media

Social media, professional networking sites, rapid-fire communications, blog sites, and personal websites are all widespread communication technologies. The rules for use of this social media with respect to Court employment, however, are identical to the rules for use of other communication methods (such as writing or publishing, telephoning, or even conversation).

Employees must use good judgment and careful discretion about the material or information posted online.

As new avenues for social media arise where no policy or guidelines yet exist, employees should again use good judgment and take the most prudent action possible. Employees should consult with their manager or supervisor if uncertain.

2. Principles

The Court's reputation for impartiality and objectivity is crucial. The public must be able to trust the integrity of the Court. The public needs to be confident that the outside activities of our employees do not undermine the Court's impartiality or reputation and that the manner in which the Court's business is conducted is not influenced by any commercial, political, or personal interests.

You should not identify yourself as a Court employee of a specific Court, Appellate, or District, but rather by generic job title or position description. By identifying oneself as an employee of the United States Courts, a social networker becomes, to some extent, a representative of the Court, and everything posted has the potential to reflect upon the Court and its image. It is acknowledged that without identifying oneself as an employee of a specific Court, an employee may intentionally or unintentionally reveal information that will allow the inference of Court employment. If this occurs, the employee assumes the responsibility for representing the Court in a professional manner.

3. Responsibility

Any material, including photographs, presented online on a Court employee website, social media, e-mail, or blog that pertains to the Court by any poster is the responsibility of the Court employee, even if Court employment can only be indirectly inferred or deduced. Personal blogs should not identify Court employment even indirectly; if possible, use your first name only. Do not reference or cite other Court employees without their express consent, and even then, do not identify them as Court employees.

4. Relevant Technologies

This policy includes (but is not limited to) the following specific technologies:

- Classmates
- Digg
- Facebook
- Flickr
- TikTok
- LinkedIn
- Google+
- Pinterest
- Instagram
- Personal Websites
- Twitter
- Snapchat
- WhatsApp
- YouTube

5. Rules

Use of the Court e-mail address for social networking (for example, blogs, Facebook, Twitter) is not permitted. Use of an employee's Court e-mail address is subject to the same appropriate use policies pertaining to the use of the telephone, namely, limited personal use not interfering with the performance of work responsibilities. e-mail addresses should not be used for "chain" correspondence, solicitation of donations, or any business enterprise. Court personnel is 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.

Think before you post.

Internet postings---whether they are 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. Any commentary you post that could reveal an association with the Court must contain an explicit disclaimer that states: *"These are my personal views and not those of my*

employer.” Again, remember that even harmless remarks could be misconstrued by litigants unfamiliar with Court processes (such as pro se litigants).

- **DO NOT** list your place of employment or any other employment information.
- **DO NOT** identify the judge who employs you or the judicial division where you work.

Observe Security Protocol.

Online comments can jeopardize the safety of all Court personnel.

- **DO NOT** post pictures of the inside or outside of the courthouse, especially the judges’ chambers.
- **DO NOT** post pictures of Court events.
- **DO NOT** post pictures of judges or other personnel.
- **DO NOT** post information about the habits or routines of judges or other personnel.
- **DO NOT** discuss courthouse security measures or security personnel.
- **DO NOT** reveal details of judges’ schedules and travel; do not reveal details of your own travel schedule when traveling on official business.

Maintain Court’s confidentiality.

Confidentiality is critical.

- **DO NOT** discuss any of the Court’s internal procedures, whether they are confidential or not.
- **DO NOT** post anything about a case you or your co-workers are working on or have worked on.
- **DO NOT** comment on lawyers practicing in the Court.

- **DO NOT** post anything about the Court’s views on any legal issues. Do not post anything about pending or closed cases, regardless of whether the information is “public” or not.
- **DO NOT** post your personal views about the Court’s rulings or the rulings of other judges.
- **DO NOT** post any online comments containing confidential Court information, including information about court cases and decisions.

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 online activities do not interfere with your job or work commitments.

- **DO NOT** engage in online activities that detract from the dignity of the Court.
- **DO NOT** post online comments about issues before the court or likely to come before the Court.
- **DO NOT** post comments endorsing or criticizing political parties or candidates.
- **DO NOT** use the official court seal or any other official court symbol or identification.

In addition to the above security protocols, special care must be taken to ensure the safety of the Judge and Court staff as well as the integrity of the Court when performing travel to attend court proceedings or Conferences:

- **DO NOT** post pictures taken during travel with a judge.
- **DO NOT** post pictures immediately after the conclusion of a trip. Allow at least two days prior to posting pictures. Make sure that the locations of your pictures do not allow for someone to develop

knowledge of your travel routine (e.g., staying in the same hotel and eating in the same restaurants when you are on official travel supporting court operations). Do not post pictures to a social networking site that allows others to add comments if there is a potential to run afoul of Canon 1 should comments serve to demean the Court, a judge, or the work ethic of court employees in any way. The examples set forth above are not exhaustive. If you are in any doubt about whether your use of the Internet, e-mail, or social media may violate this policy, then do not do it.

Further, if any employee becomes aware of the social networking activity of other staff members that would be deemed distasteful or fail the good judgment test, please contact your supervisor.

6. Productivity Impact While in Work Status

The use of Court assets (computers, internet access, e-mail, etc.) is intended for purposes relevant to the responsibilities assigned to each employee. Social networking sites have not been deemed a requirement for any position, and office access to these services is prohibited per Judiciary policy. Access to social media sites while in the office or when teleworking while on the DCN using personal devices is prohibited because of the potential impact upon productivity. Security Operations Center (SOC) monitors the DCN and will report violators of this policy.

7. Terms of Service

Most social networking sites require that users when they sign up, agree to abide by a Terms of Service document. Court employees are responsible for reading, knowing, and complying with the terms of service of the sites they use.

8. Off-Limits Materials

This policy sets forth the following items which are deemed off-limits for social networking whether used at Court or after work on personal computers, irrespective of whether Court employment is identified:

- a) **Seal and Logos** - United States Court seals and logos may not be used in any manner.
- b) **Politically Sensitive Areas** - Employees may not be seen to support any political party or cause. Employees should never indicate a political allegiance on social networking sites, either through profile information or through joining political groups. Employees should not express views for or against any policy which is a matter of current political debate. Employees should not advocate any particular position on an issue of current public controversy or debate. If an employee is in doubt, they should refer immediately to their supervisor or manager.
- c) **The Hatch Act, 5 U.S.C. § 7324 et seq.**, regulates the participation of government employees, as defined in 5 U.S.C. § 7322(1), in certain types of partisan political activities. Although the Hatch Act is not applicable to the Judicial Branch, the Judicial Conference has adopted similar restrictions. Canon 5 of the Code of Conduct for Judicial Employees prohibits all active engagement in partisan political activities, including, but not limited to, public endorsement of a candidate or contribution to a political campaign. The Code of Conduct should be consulted for a thorough understanding of the specific prohibitions on political activity contained in Canon 5. In addition, Advisory Opinion No. 92 provides guidelines for political activities.
- d) **Confidential Information** - One of the most important obligations of employees is to ensure that non-public information learned during

employment is kept confidential. Confidential information is strictly forbidden for any discourse outside of the appropriate employees of the Court. Information published on the blog(s) must comply with the Court's confidentiality policies. This also applies to comments posted on other blogs, forums, and social networking sites. Confidential information is not to be discussed or referred to on such sites, even in private messages between site members who have authorized access to the information. Court employees should also refrain from discussing any of the Court's internal processes and procedures, whether they are of a non-confidential or confidential nature.

- e) **Online Recommendations** - Some sites, such as LinkedIn, allow members to "recommend" current or former co-workers. If an employee does this as a representative of the Court, it may give the appearance that the Court endorses the individual being recommended. This could create a liability situation if another entity hires the recommended person based on the recommendation. Accordingly, Court employees should not participate in employee recommendations for reasons of liability. All communication of this type should be referred to the Court's Human Resources Officer for verification.

9. Disciplinary Actions

Employees who participate in online communication deemed not to be in the best interest of the Court may be subject to disciplinary action, including dismissal. Inappropriate communication can include, but is not limited to:

- Confidential Court information or data leakage.
- Inaccurate, distasteful, or defamatory commentary about the Court.
- Behavior or communication encouraging behavior that is illegal, grossly unprofessional, or in bad taste in violation of the Code of Conduct.

This policy has been adapted from the AO's *Guide to Judiciary Policy, Volume 15, Chapter 3*, and the April 2010 edition of the *Resource Packet for Developing Guidelines on the Use of Social Media by Judicial Employees*.

<http://jnet.ao.dcn/policy-guidance/ethics-and-financial-disclosure/social-media-guidance-and-policies/social-media-resource-packet-code-conduct-committee-april-2010>

I. Computer Policies User Agreement

To ensure that you are aware of your security and online presence responsibilities and to certify that you have received the most recent policies, procedures, and provisions, you will be required to sign the user agreement that appears at the end of this section (Attachment 1). Contact your supervisor, IT Director, IT Security Officer, or the Clerk if you have questions about this policy. The security of our Court, the DCN, and related computer systems require vigilance and the commitment of each employee. If a need arises to create an exemption to one or more of these policies, you must first obtain the Clerk of Court's explicit approval (procedures for Exceptions to IT Security Policy can be found in PAMD's IT Policy Exception. Teleworkers (remote access) will be required to complete, and sign Telework forms to ensure they understand their responsibilities to maintain the highest level possible to protect the court's data, systems, and networks when working offsite. Certain users (typically senior staff) may have signed for an additional laptop used for travel and teleworking to keep at home. Users in this category will be required to bring the checked-out laptops to work at least quarterly (or more frequently when required by the IT Department), for anti-virus/malware, application, and patch updates, if applicable.

J. Windows Service Account

Many applications and agents require service accounts and are usually shared among multiple applications, servers, network hardware. Application functionality would not operate without the use of service accounts. Examples

of applications that require service accounts are IIS, SQL Server, SharePoint, and backup applications.

By policy, PAMD allows for the use of service accounts that must have access to assets to monitor, assess, and change settings when necessary across the domain. The alternative would be a vast untenable list of local admin accounts on servers and workstations for monitoring resources, the maintenance of which would be near impossible.

All service accounts are managed in the local Active Directory. SPLUNK provides real-time e-mail alerts to the IT Department staff when there is an attempt to run a service with wrong credentials.

Policy Review

The Clerk of Court or designee, Director of IT will review this policy annually or upon events that warrant an earlier review.

Exceptions

Exceptions to this policy will be documented as a component of the PAMD IT Security Policy Exceptions Request Form.

Policy Authorization

This policy is approved by the Clerk of Court/CUE



Date: 3-2-20

United States District Court for the Middle District of Pennsylvania

Computer Policies User Agreement

As a user of computers, data devices, peripherals, and networks of the United States District Court for the Middle District of Pennsylvania, I acknowledge my responsibility to conform to the requirements and conditions established by PAMD's *Court IT Appropriate Use Security Policy and User Agreement*. By using the Judiciary's Data Communications Network (DCN) and the United States District Court for the Middle District of Pennsylvania (PAMD) and any related IT equipment provided by the court, I agree to be subject to and abide by these policies. I understand that willful violation of the principles and provisions of this policy may result in applicable disciplinary action as well as denial of access to the network and the use of court IT equipment. I am also aware that such violations will be reported to the proper authorities if necessary.

I understand that I can be held personally liable for the loss or damage of government-furnished equipment in my custody if a board of survey finds that the loss or damage was due to my negligence.

When I am teleworking, I understand that there are potentially greater security risks. I will be required to use the Judiciary's approved Virtual Private Network (VPN) software Cisco AnyConnect and Pulse Secure and agree that I will not attempt to connect personal hardware or use external disks/thumb drives to upload/install personal software. I also understand that when using public Wi-Fi connections (e.g., hotel lobby, airport, or coffee shops) to access the judiciary's networks, I must first connect using approved SSL VPN clients provided with my court-issued laptop. This will provide an encrypted tunnel between the laptop and the Judiciary network. I am also aware that the judiciary is not responsible for operating or other costs (e.g., utilities) incurred when using government-owned IT equipment in a private residence for official purposes.

I understand that failure to sign this acknowledgment will result in denial of access to the Court's network and the use of any related automation resources assets.

[To sign submit your agreement, click here then send via email](#)