Appendix E MSND/MSNP Information Technology Appropriate Use and Security Policy

Overview

This document outlines the appropriate use of Information Technology (IT) assets and the security requirements of IT asset users, as mandated by the Guide to Judiciary Policy.

Guidance

Policies and procedures must be developed for appropriate use of judiciary computer systems. Employees are responsible for the proper use of, and security measures for, government computers and the automated systems and records at their disposal, in accordance with the Guide, Vol. 11, § 440, Custody of Government Personal Property. Users must read this document in its entirety and acknowledge that they understand and will abide by MSND/MSNP appropriate use requirements and the MSND/MSNP Information Technology Appropriate Use and Security Agreement.

MSND/MSNP IT security policies are available to users, reviewed at least annually, and updated as necessary, in accordance with the Guide, Vol. 15, § 310.20.10 (a).

Definition of IT Assets

The IT assets covered by this policy are defined in the Guide, Vol. 15, § 310.10.10, IT Assets as including:

- Networks and their infrastructure (e.g., servers, switches, cables, firewalls):
    - the judiciary's wide-area networks (WAN) (e.g., the Data Communications Network (DCN), Public Access to Court Electronic Records (PACER-Net), and Defender Services (DWAN));
    - judiciary local area networks (LANs);
    - judiciary-provided private and public wireless networks;
    - courtroom IT systems; and
    - phone systems.
- Devices and equipment owned by the judiciary that do not connect to judiciary systems or networks (e.g., information systems used in support of WITSEC).
- Devices and equipment forming or connected to judiciary systems:
    - judiciary-owned workstation computers and peripherals (e.g., printers, copiers, phones, fax machines);
    - judiciary-owned portable computers and other mobile devices (e.g., laptops, tablets, smart phones, cell phones);
    - digital media (including internal and external hard drives, USB drives, CDs, DVDs, and tapes); and
    - supporting systems (e.g., power supply, HVAC systems in IT closets and facilities, communications connections).
- Software residing on judiciary systems, whether judiciary-developed (e.g., CM/ECF) or commercial (e.g., MS Word, Office 365, Outlook).
- Judiciary applications that are maintained on privately owned computers and mobile devices.
- Data and information:
    - data and information maintained on judiciary systems and devices, including information available to the public on judiciary systems (e.g., CM/ECF, the judiciary's websites, public kiosks);

- judiciary data and information on third-party systems by judiciary contract or other formal agreement (e.g., backup sites, alternate sites);
- judiciary data and information on the privately owned devices of users; and
- sensitive judiciary information, such as payroll records, contract files, etc.

Annual Awareness Training

All judiciary employees must be properly trained initially upon employment and thereafter annually on local and national information security policies in accordance with the Guide, Vol. 15 § 340 IT Security Training and Awareness, and the Guide, Vol. 11 § 650 (b), Appropriate Records and Documentation.

Appropriate Business Use

Concerning appropriate business use of MSND/MSNP IT assets, users must:

- Understand that government-owned equipment is for the use of judiciary employees in their performance of official government business, in accordance with the Guide, Vol. 15 § 525.20 (a).
- Adhere to the Code of Conduct for Judicial Employees when using judiciary computer systems, in accordance with the Guide, Vol. 15 § 525.40 (c).
- Upon logging on to court systems, and before being allowed access to any system and/or network resources, be required to consent to monitoring of my use by accepting the language in this banner, in accordance with the Guide, Vol. 15, § 515.30, Banner Notice:

United States District Court and Probation Office – Northern District of Mississippi

NOTICE TO USERS

This is a restricted government system for official judiciary business only. All activities on this system for any purpose, and all access attempts, may be recorded and monitored or reviewed by persons authorized by the federal judiciary for improper use, protection of system security, performance of maintenance, and appropriate management by the judiciary of its systems. By using this system or any connected system, users expressly consent to system monitoring and to official access to data reviewed and created by them on the system. Any evidence of unlawful activity, including unauthorized access attempts, may be reported to law enforcement officials.

Appropriate Personal Use

Personal use of government-owned equipment is defined as "activity conducted by judges and judiciary employees for purposes other than official government business and that is not deemed inappropriate personal use," in accordance with the Guide, Vol. 15 § 525.30, Definitions, when it occurs within the parameters below, where users understand:

- That as a Judiciary employee, they are permitted limited use of government-owned equipment for personal needs if such use does not interfere with official business and involves minimal additional expense to the government, in accordance with the Guide, Vol. 15 § 525.20 (b).
  Minimal additional expense is defined by the Guide, Vol. 15 § 525.30, Definitions as "personal use that will result in no more than normal wear and tear or the use of small amounts of electricity, ink, toner, or paper. Examples of such minimal additional expenses include:
  - making a limited number of photocopies,
  - using a computer printer to print a limited number of pages,
  - making occasional phone calls,
  - infrequently sending e-mail messages, and

- limited use of the internet".

An exception to this is personal cell phone use while traveling out of the country, as described in the MSND/MSNP Cybersecurity for International Travel Policy.

- That limited personal use of government-owned equipment should only occur during non-work time and that this privilege to use government-owned equipment for non-government purposes may be revoked or limited at any time by appropriate judiciary officials, in accordance with the Guide, Vol. 15 § 525.20 (c-d).

  Employee Non-Work Time is defined by the Guide, Vol. 15 § 525.30, Definitions, as "time when judges and judiciary employees are nototherwise expected to be addressing official business, such as:
  - off-duty hours before or after a workday,
  - lunch periods or other authorized breaks, and
  - weekends or holidays."
- That as a judiciary employee they may, for example, use government-owned equipment to review Thrift Savings Plan accounts, monitor medical, dependent care, or commuter benefit reimbursement accounts, seek employment, or communicate with volunteer charity organizations, in accordance with the Guide, Vol. 15 § 525.40 (a).
- That they must, at all times when using government-owned equipment for limited personal purposes, avoid giving the impression that they are acting in an official capacity. If there is a potential that such limited personal use could be interpreted to represent official business of the judiciary, they will use an adequate disclaimer, such as, "The contents of this message are personal and do not reflect any position of the judiciary or the [court unit]," in accordance with the Guide, Vol. 15 § 525.40 (b).

Inappropriate Use

Concerning inappropriate use of IT assets, users must not:

- Attempt to gain unauthorized access to other systems or data, in accordance with the Guide, Vol. 15 § 525.50 (b).
- Create, copy, transmit, or retransmit chain letters or other unauthorized mass mailings, regardless of subject matter, in accordance with the Guide, Vol. 15 § 525.50 (c).
- Use equipment for activities that are illegal, inappropriate, or offensive to fellow staff or the public, such as hate speech, or material that ridicules others on the basis of race, creed, religion, color, gender, disability, national origin, or sexual orientation, in accordance with the Guide, Vol. 15 § 525.50 (d).
- Create, download, view, store, copy, transmit, or retransmit sexually explicit or sexually oriented material, in accordance with the Guide, Vol. 15 § 525.50 (e).
- Create, download, view, store, copy, transmit, or retransmit material related to illegal gambling, illegal weapons, terrorist activities, and any other illegal or prohibited activities, in accordance with the Guide, Vol. 15 § 525.50 (f).
- Use equipment for commercial activities or in support of commercial activities or in support of outside employment or business activity, such as: consulting for pay, administering business transactions, or selling goods or services, in accordance with the Guide, Vol. 15 § 525.50 (g).
- Use equipment for fund-raising activity, endorsing any product or service, participating in any lobbying activity, or engaging in any partisan political activity, in accordance with the Guide, Vol. 15 § 525.50 (h).
- Post or provide judiciary information to external news groups, bulletin boards, or other public sites without authority, including any use that could create the perception that the communication was made in an official capacity as a judiciary employee, in accordance with the Guide, Vol. 15, § 525.50 (i).
- Use equipment in a manner that results in loss of productivity, interference with official duties, or greater than minimal additional expense to the government, in accordance with the Guide, Vol. 15 § 525.50 (j).

- Acquire, use, reproduce, transmit, or distribute without authorization any controlled information such as judiciary sensitive data, proprietary data subject to the intellectual property rights of others, such as copyright, trademark or other rights (beyond fair use), as well as computer software and data (e.g., export controlled software or data), in accordance with the Guide, Vol. 15 § 525.50 (k).
- Use judiciary-provided access to online investigative tools and databases containing personal information to gather information for non-work-related purposes, including attempting to research friends, neighbors, acquaintances, celebrities, other public figures, etc., in accordance with the Guide. Vol. 15 § 525.50 (l).
  Online investigative tools include LexisNexis and Westlaw public records or other databases that contain personal information (e.g., telephone, driver's license, auto registration and VIN numbers, home addresses, property ownership records, voting records).

Usage Policies by System

Email

Concerning the use of email systems, users must:

- Not use court provided email addresses for anything other than official government business. This includes making purchases (e.g., Amazon, eBay), using online services (e.g., social networking, blogging), and personal account access (e.g., banking, utilities). This could result in additional junk, spam, or phishing emails.
- Understand that sending sensitive judiciary information to or through personal web email accounts outside the judiciary network is discouraged because the email accounts do not afford sufficient security or privacy, in accordance with the Guide, Vol. 15 § 330.50 (b).

Instant Messaging

Concerning the use of instant messaging systems, users must:

- Only use the instant messenger (IM) applications provided by the court, in accordance with the Guide, Vol. 15 § 330.40 (a).

Internet & Social Media

Concerning internet and social media use, users must:

- Understand that internet access will be restricted consistent with the MSND/MSNP Information Technology Appropriate Use and Security Policy, in accordance with the Guide, Vol. 11 § 660 (b).
- Use discretion and avoid accessing internet sites that may be inappropriate or reflect badly on the judiciary, in accordance with the Guide, Vol. 15 § 510.30 (b)(1).
- Not use applications that employ peer-to-peer file sharing, chat rooms, and instant messaging (other than provided by the court) for communicating outside the DCN, in accordance with the Guide, Vol. 15 § 330.40 (b). Court users must understand that these applications pose extraordinary security risks to the judiciary's information technology infrastructure and can be blocked at the internet gateways until the security risks posed by their use can be mitigated. Examples of peer-to-peer applications are BitTorrent, and Tor, among others.
- Understand that access to personal web e-mail accounts (e.g., AOL Mail, Gmail, Outlook, and Yahoo) from within the DCN is prohibited, in accordance with the Guide, Vol. 15 § 330.50 (a). Use of these accounts poses threats to the judiciary's IT infrastructure because web email messages and their attachments bypass the existing network antivirus protections in place at the internet gateways and on the courts' email servers.
- Not identify themselves or others as court employees when using non-court messaging services (instant messaging, social networks, blogging, etc.). Their actions on these networks/services may be viewed as

official business by other users. If there is a potential that such limited, appropriate, personal use could be interpreted to represent official business of the judiciary, an adequate disclaimer must be used, such as, "The contents of this message are personal and do not reflect any position of the judiciary or the [court unit]," in accordance with the Guide, Vol. 15 § 525.40 (b).

- Not post or provide judiciary information to external news groups, bulletin boards, or other public sites without authority, including any use that could create the perception that the communication was made in an official capacity as a judiciary employee, in accordance with the Guide, Vol. 15 § 525.50 (i).
- Understand that as a court employee, they have a responsibility to prevent personal information about judges and staff and sensitive court unit data from appearing on public sites, in accordance with the Guide, Vol. 15 § 510.30 (c).
- Not install or use the TikTok application on a court-owned device.
- Read and agree to follow the MSND/MSNP Social Media and Social Networking Policy.

Voice Mail

Concerning the use of the judiciary voice mail system, users must:

- Carefully safeguard their voice mail PIN, in accordance with the Guide, Vol. 15 § 330.80 (h).
- Protect their voice mail from unauthorized access (e.g., to be used to make fraudulent calls or to obtain sensitive judiciary information), in accordance with the Guide, Vol. 15 § 330.80, Voice Mail System Security.
- Not leave voice mail messages containing sensitive information (e.g., credit card numbers, procurement decisions), in accordance with the Guide, Vol. 15 § 330.80 (g).

DCN Network (Wired and Wireless)

Concerning the use of the DCN network, users must:

- Not use the network in a way that could cause congestion, delay, or disruption of service to any government system, including, but not limited to, use of electronic greeting cards, video, sound, or other large file attachments, "push" technology on the internet, streaming recreational video, and other continuous data stream uses, in accordance with the Guide, Vol. 15 § 525.50(a).
- Not connect any personal software or equipment to court-provided equipment without the approval of the CUE, in accordance with the Guide, Vol. 15 § 530.20.10.
- Not connect any personal Wi-Fi equipment to the wired private judiciary network.

Software

Concerning software on judiciary IT assets, users must:

- Understand that they are not allowed to install personally owned software on court-issued desktops and laptops. If they need software installed, they will obtain written approval from their judicial officer or CUE; contact IT staff for installation; provide the software and license information to IT staff for a security risk review; and obtain approval by the IT Security Officer. Installation of the software will be performed by the IT staff, in accordance with the Guide, Vol. 15 § 535.30 (d).
- Allow IT staff to perform routine security-related maintenance, including the installation and continued updates of client software, antivirus software, firewall products, operating system patches, third-party software patches, and firmware updates, in accordance with the Guide, Vol. 15 § 330.60.60 (b).

VPN (Remote Access)

Concerning use of the remote access VPN, users must:

- Understand that VPN and Remote Access technologies are provided to secure access to judiciary networks from remote locations and to extend the judiciary network beyond the wired courthouse and

judiciary office locations. They will only use these technologies to perform approved work-related activities or job duties on judiciary computers, in accordance with the Guide, Vol. 15 § 330.60.10, Purpose of Remote Access, and the Guide, Vol. 15 § 330.60.50 (b).

- Understand that antivirus software with current malware definitions is mandatory on all computers that access judiciary networks, in accordance with the Guide, Vol. 15 § 330.25, Antivirus Software.
- Understand that if they do not maintain adequate security safeguards, remote access privileges may be suspended or terminated, in accordance with the Guide, Vol. 15 § 330.60.80 (c).
- Understand that personally-owned devices are not to be used to access (via VPN, Remote Access, or WiFi) judiciary networks.
- Understand the court is not liable for damage to personal or real property, any operating or service costs, or repair, when using personal equipment for conducting court business.

Mobile Devices

Concerning the use of judiciary mobile devices, users must:

- Understand that personally-acquired applications may be installed on government owned mobile devices (iPad or iPhone), if such personally-acquired applications do not detrimentally impact the performance or security of the court-owned device. They understand they will not be reimbursed for any personally-acquired applications, unless preauthorized for official use, in accordance with the Guide, Vol. 15 § 570 (e).
- Understand that any installed personally-owned applications on court devices may be removed during updates, applying security settings, or by unit device management policies. Ownership rights to these applications are abandoned upon return or disposal of the court-issued device, in accordance with the Guide, Vol. 15 § 570 (e-f).
- Not use Peer-to-Peer applications while the mobile device is connected to the DCN (via VPN), in accordance with the Guide, Vol. 15 § 330.40, Ban on Peer-to-Peer File Sharing, Chat Rooms, Instant Messaging. Examples of peer-to-peer applications are BitTorrent and Tor, among others.
- Understand the IT Department will not support personally-owned devices.

Password Policy

Concerning the use of passwords on judiciary networks, users must:

- Understand that as a user of judiciary information systems, they are responsible for creating, protecting, and securely managing passwords, in accordance with the Guide, Vol. 15 § 390 (a).
- Understand that their password will be changed periodically per system requirements (on applicable systems), in accordance with the Guide, Vol. 15 § 390 (c)(1).
- Carefully safeguard their passwords. They will not share their passwords or give them to family members or friends, in accordance with the Guide, Vol. 15 § 330.60.60 (c).
- Understand that the IT Department may need to know their password for support or maintenance reasons. If this occurs, the user should immediately change the shared password.
- Use password-protected screensavers that automatically activate after a period of inactivity to prevent unauthorized system access to their computer, in accordance with the Guide, Vol. 11 § 660 (f).

Data Protection

Concerning the protection of judiciary data, users must:

- Protect non-public judiciary information from unauthorized access or disclosure. Such information includes, but is not limited to, chambers work product, warrants, sealed cases, budget and accounting

material, personnel data (e.g., personal information about judiciary personnel, payroll, etc.), and source selection information in accordance with the Guide, Vol. 15 § 310.10.20 (a), and the Guide, Vol. 11 § 660 (g).
- Ensure that important data is stored on network drives and not on desktop or laptop hard drives, so that the data is properly backed up.

Physical Protection

Concerning physical protection of judiciary IT assets, users must:

- Physically protect and secure equipment, devices, media, and printed output against loss, theft, and misuse, in accordance with the Guide, Vol. 11 § 650 (b)(5) and from observation by unauthorized individuals, in accordance with the Guide, Vol. 15 § 310.10.30 (b)(1).
- Keep court-issued laptop and/or mobile devices in a secure location when traveling and when not in use. They will not check a court-issued technology device when traveling by commercial carrier, in accordance with the MSND/MSNP Cybersecurity for International Travel Policy.
- Not modify equipment (physically or functionally) without approval from the IT Department, including loading personal software or making configuration changes, in accordance with the Guide, Vol. 15 § 525.35 (b).
- Physically protect equipment from damage by food, liquids, cleaning products, hygiene products, dirt, dust, magnets, extreme temperatures, prolonged exposure to sunlight, or pets.
- Return, in good condition, all equipment checked out to them, including removable media (such as USB flash drives, external hard drives, etc.), to the court when these devices are either no longer needed or at the end of their employment in accordance with the applicable Form AO 566 (Property Pass) or Form AO 563 (Property Caretaker Receipt).

International Travel

Concerning international travel with IT assets, users must:

- Understand that Government Furnished Equipment (GFE) may not be taken outside the United States, unless provided specifically for that purpose by the IT Department.
- Read and agree to adhere to the MSND/MSNP Cybersecurity for International Travel Policy, MSND/MSNP International Travel Plan, and MSND/MSNP Basic Traveler Responsibilities.

Security Incident Procedure

A security incident is defined as "any real or suspected adverse event impacting the security of judiciary IT assets. These include, but are not limited to: attempts to gain unauthorized access to a system or its data; unauthorized disclosure of non-public judiciary data; unwanted disruption or denial of service; unauthorized use of a system for processing, accessing, modifying, or destroying data; and changes to system hardware, firmware, software, or access control characteristics without the owner's consent," in accordance with the Guide, Vol. 15 § 320.20 (a).

The **IT Security Officer** is the designated contact at each judicial district responsible for implementing security policies and procedures within the court, addressing security threats directed against IT assets within the court unit system boundary, and reporting all critical and serious incidents to the Judiciary Security Operations Center (SOC), in accordance with the Guide, Vol. 15 § 310.20.05 (b), and the Guide, Vol. 15 § 320.20 (d).

IT Security Officer:	Roy Geoghegan
Email:	Roy_Geoghegan@msnd.uscourts.gov

Office: (662)281-3034

Cell: (662)816-1287

Users understand that is it their responsibility to IMMEDIATELY contact the IT Security Officer and their supervisor for any of the following reasons:

- Any suspected security incident, in accordance with the Guide, Vol. 11 § 650 (b)(4).
- Any suspected or actual compromise of a password, in accordance with the Guide, Vol. 15 § 390 (d).
- Any suspected voice mail fraud or voice mail PIN compromise, in accordance with the Guide, Vol. 15 § 330.80 (h)(4).
- Any suspected attempt at unauthorized access, or if they suspect they are the target of an attempted exploitation.
- Any suspected disclosures of restricted information or data.
- Any loss of court-issued equipment. They understand that if court-issued equipment has been lost, they are responsible for providing a written statement of the details surrounding the loss to the IT Security Officer and their supervisor.
- Any theft of court-issued equipment. They understand that if court issued equipment has been stolen from them, they are responsible for providing a police report and written statement of the details surrounding the incident to the IT Security Officer and their supervisor. For theft within the court, the ISO will notify the CUE.
- Any loss or theft of **personally-owned mobile devices** configured for use with court services (such as Duo Mobile, Workspace One, etc.). They understand that the IT Department will initiate a process to remotely delete all data or wipe the entire device.

References

Code of Conduct for Judicial Employees

Form AO 563 (Property Caretaker Receipt)

Form AO 566 (Property Pass)

Guide to Judiciary Policy

- Vol. 11, § 440, Custody of Government Personal Property
- Vol. 11 § 650 (b), Appropriate Records and Documentation
- Vol. 11 § 650 (b)(4)
- Vol. 11 § 650 (b)(5)
- Vol. 11 § 660 (b)
- Vol. 11 § 660 (f)
- Vol. 11 § 660 (g)
- Vol. 15, § 310.10.10, IT Assets
- Vol. 15 § 310.10.20 (a)
- Vol. 15 § 310.10.30 (b)(1)
- Vol. 15 § 310.20.05 (b)
- Vol. 15, § 310.20.10 (a)
- Vol. 15 § 320.20 (a)
- Vol. 15 § 320.20 (d)
- Vol. 15 § 330.25, Antivirus Software
- Vol. 15 § 330.40, Ban on Peer-to-Peer File Sharing, Chat Rooms, Instant Messaging

- Vol. 15 § 330.40 (a)
- Vol. 15 § 330.40 (b)
- Vol. 15 § 330.50 (a)
- Vol. 15 § 330.50 (b)
- Vol. 15 § 330.60.10, Purpose of Remote Access
- Vol. 15 § 330.60.50 (b)
- Vol. 15 § 330.60.60 (b)
- Vol. 15 § 330.60.60 (c)
- Vol. 15 § 330.60.80 (c)
- Vol. 15 § 330.70.15
- Vol. 15 § 330.80, Voice Mail System Security
- Vol. 15 § 330.80 (g)
- Vol. 15 § 330.80 (h)
- Vol. 15 § 330.80 (h)(4)
- Vol. 15 § 340 IT Security Training and Awareness
- Vol. 15 § 390 (a)
- Vol. 15 § 390 (c)(1)
- Vol. 15 § 390 (d)
- Vol. 15 § 510.30 (b)(1)
- Vol. 15 § 510.30 (c)
- Vol. 15, § 515.30, Banner Notice
- Vol. 15 § 525.20 (b)
- Vol. 15 § 525.20 (c-d)
- Vol. 15 § 525.30, Definitions
- Vol. 15 § 525.35 (b)
- Vol. 15 § 525.40 (a)
- Vol. 15 § 525.40 (b)
- Vol. 15 § 525.40 (c)
- Vol. 15 § 525.50(a)
- Vol. 15 § 525.50 (b)
- Vol. 15 § 525.50 (c)
- Vol. 15 § 525.50 (d)
- Vol. 15 § 525.50 (e)
- Vol. 15 § 525.50 (f)
- Vol. 15 § 525.50 (g)
- Vol. 15 § 525.50 (h)
- Vol. 15, § 525.50 (i)
- Vol. 15 § 525.50 (j)
- Vol. 15 § 525.50 (k)
- Vol. 15 § 525.50 (l)
- Vol. 15 § 530.20.10
- Vol. 15 § 535.30 (d)
- Vol. 15 § 570 (e)
- Vol. 15 § 570 (e-f)

MSND/MSNP Backup, Storage, and Recovery Policy

MSND/MSNP Basic Traveler Responsibilities

MSND/MSNP Contingency Planning and Disaster Recovery Policy

MSND/MSNP Cybersecurity for International Travel Policy

MSND/MSNP Incident Response Plan

MSND/MSNP Information Technology Access Control Policy

MSND/MSNP Information Technology Appropriate Use and Security Agreement

MSND/MSNP Information Technology Awareness and Training Plan

MSND/MSNP Information Technology Configuration Management Policy

MSND/MSNP Information Technology Exception Policy

MSND/MSNP Information Technology Maintenance Policy

MSND/MSNP International Travel Plan

MSND/MSNP Log Management Policy

MSND/MSNP Media Sanitization and Information Disposal Policy

MSND/MSNP Network Management Plan

MSND/MSNP Password Policy

MSND/MSNP Physical Security Policy

MSND/MSNP Remote Access Policy

MSND/MSNP Social Media and Social Networking Policy

MSND/MSNP Wireless Technology Policy

Appendix F MSND/MSNP Information Technology Appropriate Use and Security Agreement

By signing this agreement:

- I acknowledge that I have read the MSND/MSNP Information Technology Appropriate Use and Security Policy. I agree to appropriately use government IT assets and abide by the policy's provisions. I also acknowledge that I understand my security responsibilities as a user of government IT assets, in accordance with the Guide to Judiciary Policy, Vol. 15 § 330.60.70, and the Guide, Vol. 15 § 510.10 (b).
- I understand that unauthorized or improper use of government IT assets may result in loss of the privilege, limitation of the privilege, disciplinary or adverse actions, criminal penalties, and/or civil penalties, including financial responsibility for the costs of improper use, in accordance with the Guide, Vol. 15 § 525.60, and the Guide, Vol. 15 § 510.20 (c).
- I understand that use of government assets is monitored and may be reported to the employee's court unit upon request. This monitoring includes but is not limited to internet usage, email usage, etc., in accordance with the Guide, Vol. 15 § 510.20 (d).

References

Guide to Judiciary Policy

- Vol. 15 § 330.60.70
- Vol. 15 § 510.10 (b)
- Vol. 15 § 510.20 (c)
- Vol. 15 § 510.20 (d)
- Vol. 15 § 525.60

MSND/MSNP Information Technology Appropriate Use and Security Policy

_____ _____

Date Signature of Employee

_____

Printed Name of Employee