END USER IT SECURITY POLICY

INTRODUCTION AND PURPOSE

The United States District Court for the District of Maryland and the United States Bankruptcy Court for the District of Maryland (referred to collectively as the "court") provide each employee with information technology assets, access, and other resources required for performance of the employee's duties. Each court employee must follow all guidelines contained in this policy in order to protect the confidentiality, integrity, and availability of information residing on, processed on, or transmitted by the court's information technology assets, access, and other resources. Court employees must also follow each guideline outlined herein on the appropriate use and protection of government-owned information technology assets, access, and other resources.

SCOPE AND BACKGROUND

This policy applies to all judicial officers, chambers' staff, clerk's office staff, contractors, vendors, and interns (referred to collectively as "employee" or "employees").

This policy summarizes the end user requirements contained in the following court IT policies:

- Access Control
- Appropriate Use of IT Systems
- Awareness and Training
- Backup and Storage
- Configuration Management
- Contingency Planning and Disaster Recovery
- Incident Response
- Log Management
- Maintenance
- Media Sanitization and Information Disposal
- Network Management
- Password Security
- Patch Management
- Physical IT Security
- Policy Exceptions
- Remote Access and International Travel
- Witness Protection
- WLAN Security

These policies, in turn, are based on the Guide to Judiciary Policy, Volume 15, Chapters 3 (IT Security) and 5 (Managing IT Resources) and the Guide to Implementing the Judiciary Information Security Framework.

APPROPRIATE USE

Government-owned information technology assets, access, and other resources are authorized for use in the performance of official court business. Appropriate personal use of government-owned assets, access, and other resources is permitted as long as it constitutes minimal additional expense and takes place only during time that does not interfere with work responsibilities.

In using government-owned information technology assets, access, and other resources for limited, personal purposes, users must, at all times, avoid giving the impression that they are acting in an official capacity. If it is possible that such a personal use could be interpreted as representing the court, then a disclaimer must be provided. An acceptable disclaimer may be "The contents of this message are those of the sender and do not reflect any position of the government or my court".

Inappropriate personal use of government-owned information technology assets, access, and other resources is prohibited. Inappropriate personal use includes, but is not limited to, the following:

- Using information technology assets, access, and other resources that could cause congestion, delay, or disruption of service to any government system.
- Attempting to gain unauthorized access to other systems.
- Creating, copying, transmitting, or retransmitting chain letters or other unauthorized mass mailings, regardless of subject matter.
- Using information technology assets, access, and other resources for activities that are illegal, inappropriate, or offensive to fellow staff or the public.
- Creating, downloading, viewing, storing, copying, transmitting, or retransmitting sexually explicit or sexually oriented material.
- Creating, downloading, viewing, storing, copying, transmitting, or retransmitting material related to gambling, illegal weapons, terrorist activities, and any other illegal or prohibited activities.
- Using information technology assets, access, and other resources for commercial activities, in support of commercial activities or in support of outside employment or business activity.
- Using information technology assets, access, and other resources for fund-raising activity, endorsing any product or service, participating in any lobbying activity, or engaging in any partisan political activity.
- Posting 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.
- Using information technology assets, access, and other resources in a manner that results in loss of productivity, interference with official duties, or greater than minimal additional expense to the government.
- Acquiring, using, reproducing, transmitting, or distributing non-public information or intellectual property of others.

EMAIL

Court issued email is a government-owned information technology asset. Thus, this policy applies when a court email address or court email system is used. Limited appropriate personal use of work email is permitted.

The judiciary retains emails of separating employees for a limited period of time. The Chief Judge or Clerk of Court must approve the transfer of any email when employees transfer to the Administrative Office of the U.S. Courts (the AO) or other court units.

Emails from a court email address and/or court email system are subject to disclosure. Any email can be forwarded, broadcasted or published without the knowledge or consent of the author. Further, for messages sent outside of the judiciary and partner-agencies, such as to the Department of Justice,

recipients utilize the internet - an unsecured network - and communications can be intercepted and reviewed without the sender's (or receiver's) consent and knowledge. Any such emails must be carefully crafted to exclude any non-public information.

Users should exercise discretion when sending or forwarding email messages to group addresses or distribution lists. Users must not send or forward inappropriate email messages to others either internal or external to the court.

Access to personal email accounts from within the Data Communication Network (DCN) is strongly discouraged. Use of these accounts poses a threat to the judiciary's IT infrastructure because web email messages and their attachments may bypass the existing network anti-virus protections in place at the internet gateways and on the court's email servers.

Sending non-public information to or through personal email accounts outside the judiciary network is similarly discouraged because the email accounts do not afford users sufficient security or privacy.

NETWORK AND INTERNET ACCESS

Network access, including the Internet, is a government-owned information technology asset. This policy applies when users are on the DCN, either directly or using a Virtual Private Network (VPN) technology.

Personal devices are prohibited on the court's WiFi network (DCN_GTWY).

Users must exercise caution when clicking on any unfamiliar links. The IT Help/Service Desk is available to evaluate the cybersecurity posture of any online resources.

Judicial officers or their designees, as part of their official job duties, may require occasional case-related access to inappropriate, offensive, and even possibly illegal Internet sites. Such access must take place outside of the judiciary's network, by using cellular devices, such as a laptop connected to a MiFi.

SOCIAL NETWORKING WEBSITES

In addition to this policy, users should also refer to the Judiciary's Social Media Resource Packet. Social networking sites such as Facebook, TikTok and Twitter make it easy to share thoughts, ideas, pictures, videos and other information with a wide audience. Employees should not discuss any of the court's internal procedures or processes, whether confidential or not, on any external social networking site or otherwise with non-court employees. Employees must keep non-public information confidential, exercise discretion to avoid embarrassment to the court, and take precautions to avoid security risks for court personnel. Employees should not post pictures of the courthouse, inside or outside; pictures of court events; or pictures of the court's judicial officers.

Employees should carefully evaluate whether listing their employment with the judiciary on a social networking website poses a security risk, and employees may not identify themselves as working for any specific court unit or any specific judge. With the written permission of the Clerk, Chief Deputy Clerk or Judge, employees may state their association with the court unit or judge on professional networking sites only (e.g., LinkedIn).

SOFTWARE DOWNLOADS

Except on mobile devices, unauthorized software downloads or installations are prohibited. If a software

program is needed, users should contact the IT Help/Service Desk for assistance. Downloading of large files for personal use is prohibited, including music files or movie files. Network activity is monitored for large downloads.

INSTANT MESSAGING, CHAT ROOMS, AND PEER-TO-PEER FILE SHARING

Employees may only use the instant messaging (IM) features on the DCN if they are provided in applications that function entirely within the DCN (e.g., the judiciary's version of Microsoft Teams).

Applications that employ peer-to-peer file sharing, chat rooms, and instant messaging for communicating outside the DCN pose extraordinary IT security risks and their use is prohibited.

SAFETY WHILE DRIVING

The use of court provided wireless devices and all work-related communications using a wireless device while driving is prohibited unless a hands-free device or system is used. Employees must use a hands-free microphone while driving or allow voice mail on their mobile phone pick up calls when it is unsafe to answer. Texting while driving is strictly prohibited.

SAFEKEEPING OF GOVERNMENT-OWNED ASSETS

Government-owned information technology assets issued to employees must be signed out and in, following the procedures described in the court unit's Asset Management policy.

Employees are responsible for safekeeping the government-owned information technology assets from theft and damage. Employees should never leave assets unlocked or in unsecure areas.

If a government-owned information technology asset is lost or stolen, the Clerk of Court or Chief Deputy Clerk must be notified immediately. The IT Service Desk/Help Desk must be contacted immediately to have the device remotely disabled.

If a personally owned device that contains any court data, including emails, is lost or stolen, the Clerk of Court or Chief Deputy Clerk must also be notified immediately.

Employees should keep their work area clean, avoid eating or drinking nearby, and refrain from connecting other equipment such as portable heaters or fans into the same surge protector as the computer and/or peripherals.

BACKUPS AND DATA STORAGE

Employees are responsible for storing important data on shared drives, so it can be backed up, and not on local devices (e.g., laptops, physical and virtual desktops, or iPads). Critical data, including shared drives, is backed up at least daily, and in some cases numerous times a day. Backups are retained according to the judiciary's Records Disposition Schedules.

The judiciary's OneDrive should not be used to permanently store court documents. It can be used for access from multiple devices for convenience and for collaboration with colleagues but should be considered a temporary repository.

While the collaboration features of OneDrive are robust, unless employees are extremely familiar with OneDrive's functionality, there is a significant risk of document loss or inadvertent sharing of data with

others in the judiciary. Employees are advised not to use OneDrive to work with non-public information, including but not limited to:

- Personal Identifiable Information (PII).
- Financial documents.
- Draft opinions.

Employees must read and acknowledge the OneDrive Guidance and User Agreement prior to using OneDrive.

Use of third-party cloud storage to store non-public information is prohibited.

PASSWORDS

Employees are required to change their initial passwords immediately following the first successful login and every 180 days thereafter. Systems and applications are configured to prohibit employees from recycling old password for 5 password changes, and from changing their password in less than 30 days from the previous time the password was changed. Passwords require a minimum of 8 characters and must comply with the following requirements:

- At least 4 letter combination.
- Must contain at least 1 upper case letter.
- Must contain at least 1 number.
- Must contain at least 1 symbol.
- No more than 3 repeated characters in a row.
- Cannot contain user account name.
- Cannot contain a part of user's display name.

Employees are prohibited from sharing usernames and passwords.

Saving or storing passwords for automatic processing is strongly discouraged. However, employees may use encrypted password-vault software if it stores passwords locally and not in the cloud.

LOCKING/TIMEOUTS

Sessions are locked or timed out after 15 minutes of inactivity preventing access until the employee reauthenticates to the session**.**

INCIDENT REPORTING

Each court desktop and laptop computer has antivirus/antimalware software installed. Employees should contact the IT Service Desk/Help Desk when reporting any suspected or confirmed IT security incident, including antivirus/antimalware alerts. When reporting an incident, employees should provide a description of the incident, its physical location (when applicable), the identity of the system affected, and the time the incident was first detected. If reporting on behalf of another, the identity and contact information for both the person reporting and the person affected should be provided.

Except as directed by the Chief Judge or Clerk of Court, employees will not contact any law enforcement agencies or the media regarding any security incident, whether suspected or actual. IT security incidents require a coordinated response to ensure the court presents an accurate and consistent message across all communication channels.

TRAINING AND EXERCISES

New employees are required to complete the security awareness training, including self-certification, within 24 hours from the time they are provided with access to the network. Mandatory security awareness refresher training, including self-certification, must be completed annually each October (the national cybersecurity awareness month).

Employees with access to the cash register or the credit card terminals must complete annual Payment Card Industry Data Security Standards (PCI DSS) training, including self-certification. The PCI DSS training ordinarily takes place in October in conjunction with the annual security awareness refresher training.

Additional security refresher training, including self-certification, may be required by information system changes or requested due to a security related incident. IT and administrative staff require additional training as germane to their job duties and responsibilities.

Practical exercises that simulate actual cyber-attacks and train users on appropriate actions and reporting of potential threats are conducted at least quarterly.

REMOTE ACCESS

Remote access is restricted to those employees with legitimate work-related needs. Remote access is limited to only the functionality required to perform approved job duties.

Remote access security-related maintenance is regularly performed by the employee with instruction from the IT staff, or, when appropriate, by the IT staff directly.

Remote access passwords and devices providing two-factor authentication must be carefully safeguarded.

Users should never allow anyone other than the authorized user to make use of remote access to the court's networks.

Employees must understand the risk associated with using public or shared computers and/or public WiFi and avoid such use whenever possible.

INTERNATIONAL TRAVEL

The best course of action is to not access the court's network, systems, and data while traveling internationally. If accessing the court's network, systems, and data is necessary, employees must take steps to reduce risk by:

- Traveling with loaner devices provided specifically for international travel.
- Using the minimum types of devices required.
- Restricting the capabilities of the travel devices to only those that must be used during the travel period.
- Loading the least amount of information (personal and official use) required to support the travel period.
- When reading and responding to email, VPN and two-factor authentication should be initiated first to ensure a secure path for email data.

The court's network, systems, and data must never be accessed from public or shared computers and/or unsecured public WiFi when traveling internationally. Secured public WiFi should only be used when dedicated connectivity, such as private WiFi or a dedicated MiFi, is not available.

INFORMATION DISPOSAL

Employees are responsible for shredding of printed non-public material. Employees must return all data storage media to IT for secure disposal.

PRIVACY ISSUES

All electronic documents and other communications created or stored using government-owned information technology assets, access, and other resources are the property of the court. The court may access documents or communications stored on its assets 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 government-owned information technology assets are private or confidential.

MONITORING

Use of court provided information technology access may be monitored. Employees consent to monitoring by using the government-owned information technology assets. Court IT personnel, when approved by the Chief Judge or Clerk of Court, may inspect the information technology activity logs for compliance with court policies and during IT security related investigations. Use of government-owned information technology assets is made with the understanding that such use is generally not secure, is not private, and is not anonymous.

VIOLATIONS

Violation of this policy may result in appropriate restrictions, loss of access and other adverse actions, up to and including termination of employment. The court may also notify law enforcement if it discovers evidence of any possible illegal activity. The privilege to use government-owned information technology assets for limited, personal purposes may be revoked or limited at any time with or without advance notice.

EXCEPTIONS

Exceptions to this policy can be granted by the Clerk of Court or the Chief Judge. Any exception will require written acceptance of the risk by the corresponding court unit.

POLICY REVIEW

This policy is reviewed annually. Employees may be required to re-sign the policy acknowledgement form after significant updates.

IT Committee: March 2021
Effective: May 2021

Reviewed: February 2021

END USER IT SECURITY POLICY
ACKNOWLEDGMENT FORM

I, _____ have read and understand the End User Information Technology Security Policy of the United States District Court for the District of Maryland and the United States Bankruptcy Court for the District of Maryland. I understand that use of the court's information technology assets is monitored, and my individual activity may be audited for inappropriate use. I agree to abide by this policy during my employment with the court. I understand that violation of this policy may subject me to disciplinary action.

_____
Signature

_____
Date