INFORMATION TECHNOLOGY POLICY

INTRODUCTION AND PURPOSE:
The Court provides each employee with a computer, other electronic equipment, software, e-mail and Internet access to be used in the performance of their duties. By accepting employment with the Court, employees agree to follow certain guidelines when using a work computer or laptop. Additionally, the Systems department will assist employees so they can use their computers more effectively.

SCOPE:
This policy applies to employees of the Court (all permanent and temporary staff including contractors, law clerks, students, consultants and interns) using government-provided computers. The policy further applies to home computers when they are used to gain access remotely using the Virtual Private Network (VPN) or JPort as they become part of the Judiciary's network.

DEFINITIONS:
Internet
Access to Internet resources is provided to Court personnel through the Judiciary's network or DCN (Data Communications Network) using web browsers such as Mozilla FireFox and Microsoft Internet Explorer. Internet access includes viewing Web sites, sending and receiving electronic mail, transmitting or downloading files, running applications and making transactions via the government-provided network.

Intranet/DCN
The J-Net and the Court's internal web site are Intranets that are used within the federal Judiciary, and operate within the DCN. They are designed to provide a means for organizing and disseminating information for internal judiciary use. The J-Net provides information to anyone in the Judiciary in the same way computers provide information on the Internet.

GENERAL RULES: (Also refer to the Judiciary's Policy on Personal Use of Government Office Equipment – http://jnet.ao.dcn/Property_Management/Personal_Use_Policy.html).

Government-provided computers, other electronic equipment and the DCN should be used for official Court business. Employees are subject to the guidelines noted below. Limited personal use of the Court-provided computers and the Internet is permitted as long as it does not interfere with an employee's duties and responsibilities. This limited personal use should take place during the employee's non-work time and should not include prohibited activities mentioned in "Unacceptable Use". Since the Judiciary pays one flat fee for all Internet access, there is no additional cost for personal use of the Internet. Employees are expected to conduct themselves

professionally and to refrain from storing or transmitting obscene, profane, or indecent materials, or any form of discriminatory material.

E-MAIL:
Unlike e-mail messages sent to other Court employees using Lotus Notes, messages sent to Internet addresses should **not** be considered private. The Internet is an unsecured network. As such, information and e-mail on the Internet is a public record and subject to public record regulations with respect to inspection and disclosure. It can be read, broadcast, or published without the knowledge or consent of the author. Users are encouraged to use discretion when forwarding large e-mail messages to group addresses or distribution lists. At no time should an employee forward a "chain letter" e-mail message or inappropriate e-mail messages to others either internal or external to the Court.

Further, the AO's IT Security Policy [2006-1] -Discouraging Personal Web E-Mail, also applies. It states:

> Access to personal Internet web e-mail accounts from within the judiciary's private data communications networks is strongly discouraged. Use of these accounts poses threats to the judiciary's information technology infrastructure. If you do use an Internet e-mail account, message attachments will be scanned for viruses and therefore some messages may be blocked without prior notification.

SOCIAL NETWORKING WEBSITES: (Also refer to the Judiciary's Social Media Resource Packet
http://jnet.ao.dcn/Ethics/Social_Media_Guidance_and_Policies/Social_Media_Resource_packet.html)

Social networking sites such as FaceBook, YouTube and Twitter make it easy to share thoughts, ideas, pictures and other information with a wide audience. Court employees should refrain from discussing any of the Court's internal procedures or processes, whether confidential or not. Court personnel are expected to keep sensitive information confidential, exercise discretion to avoid embarrassment to the Court, and take precautions to avoid security risks for Court personnel. Court employees should carefully evaluate whether listing their place of employment on a social networking website poses a security risk. Do not post pictures of the courthouse, inside or outside; pictures of Court events; or pictures of the Court's judicial officers.

FILE TRANSFER:
To prevent computer viruses from being transmitted through the Court's e-mail system and network, downloading of software and certain files is prohibited. If a software program is needed, please contact the Help Desk for assistance. Downloading of files for Court business purposes is permitted. An example would be downloading a PDF, MS Word, or Word Perfect file from another Court site. Downloading files for personal use is not permitted. For example employees are not permitted to download music files (MP3), movie files (WMV), or other non-work related files.

INSTANT MESSAGING AND PEER-TO-PEER FILE SHARING:
The AO's IT Security Policy [2006-2] *Prohibition of Internet Peer-to-Peer File Sharing, Chat Rooms And Instant Messaging* states:

> The use of peer-to-peer file sharing (e.g. BearShare), chat rooms, and instant messaging (IM) for communicating with persons or entities outside the judiciary's private data communications network (DCN) is prohibited. These programs pose extraordinary security risks to the judiciary's information technology infrastructure. The AO will send a notice to Court systems security staff if any of these programs are used. SameTime use is permitted as it restricts IM to Judiciary users only.

SAFETY
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 is used. Use a hands-free microphone while driving or let your voice mail on your mobile phone pick up your calls when it's unsafe to answer. Texting while driving is strictly prohibited.

PHYSICAL SECURITY:
Employees are expected to take care of their computer. Avoid eating or drinking nearby; keep the work area clean; do not plug other equipment like portable heaters into the same surge protector as the computer. Laptops issued to employees must be signed out and back in. It is the employees' responsibility to guard the laptop from theft and damage.

OPERATIONAL SECURITY:
Backups
All files stored on network drives are backed up to tape each evening. Once a month, one of these tapes is set aside as a permanent record. Systems can retrieve a file from these backup tapes as requested. For Lotus Notes e-mail, Systems can restore an entire mail file (excluding items in the Trash folder) for a period up to the two previous weeks. Systems has configured the common software applications to save employee's work on a network drive. Please do not save files to the C drive as it is not backed up.

Passwords
When the network, Lotus Notes and CM/ECF user accounts are set up, each employee is assigned a password. All network passwords will be changed every 120 days. Never share user IDs or passwords with others.

Locking or Shutdown of Computers

The screen saver can be enabled so employees can lock down their computer when they are away from the computer by pressing Ctrl-Alt-Del and choosing lock computer. This method should be used if an employee needs remote access to their computer; otherwise, at the end of each workday, please shutdown the PC.

Virus control
All Court computers have virus control software installed. When a floppy disk or a USB flash memory disk is inserted in the computer, a virus scan will run. Contact the Help Desk immediately if a virus alert message appears on the computer screen.

Software
Like many other organizations, the Court prohibits the loading of any software other than that provided by the Court, on Court computers. This includes screen savers, software like the weather bug, games, and other personally-owned software. Systems is required to have the appropriate licenses for all software installed on Court computers so if an employee needs software installed, please contact the Help Desk.

Remote Access
Remote access to Court systems is provided using a VPN connection through JPort and then a connection to the employee's work computer. Most of the common software programs and an employee's data files used at the Court can be utilized. VPN access is provided via any internet access system (home, hotel, public library, etc.). Contact the Help Desk for the directions. Such remote access must be approved by a manager. It is provided for the convenience of the Court, and must be used only for approved Court business.

UNACCEPTABLE USE:
As with all work related matters, the Code of Conduct for Judicial employees must be considered. Accordingly employees may not use government provided computers or the Internet for prohibited activities that include but are not limited to:

- Making unauthorized statements regarding Court policies or practices
- Transmitting confidential information (such as that relating to ongoing investigations or litigation)
- Making unauthorized commitments or promises that might be perceived as binding the government
- Using subscription accounts or commercial services that are not expressly authorized
- Sending or displaying messages or pictures that are obscene or sexually explicit
- Using the Court-provided connection for activities that are illegal, inappropriate, or offensive to fellow employees or the public. Such activities include but are not limited to: hate speech or material that ridicules others on the basis of race, creed, religion, color, sex, disability, national origin, or sexual orientation
- Using the Court-provided connection for commercial purposes
- Using the Court-provided connection for political, fund-raising or lobbying activities, collective bargaining, or any illegal activities
- Improper use or distribution of information which includes copyright violations such as software piracy (The Court may incur a legal liability for unauthorized copying of files or software even if the copy is used for official business.)

- Personal use that could cause congestion, delay or disruption of service. For example sending electronic greeting cards or sending messages with large attachments can degrade performance of the entire network
- The creation, copying, transmission or retransmission of chain letters or mass mailing regardless of the subject matter
- Using unauthorized (outside the DCN) streaming technologies on the Internet that continuously stream data through the network. Examples would be watching a video from YouTube, ABC.Com or listening to an Internet radio station.
- Using government systems as a platform or staging ground to gain unauthorized access to other systems

PROPER REPRESENTATION:
It is the responsibility of employees to ensure that they are not giving the false impression that they are acting in an official capacity when they are using the computer and Internet for non-governmental purposes. If there is an expectation that such a personal use could be interpreted as representing the Court, then a disclaimer must be used. An acceptable disclaimer may be "The contents of this message are mine personally and do not reflect any position of the government or my Court".

INTELLECTUAL PROPERTY RIGHTS:
Employees should show respect for intellectual property and creativity by giving appropriate credit when files or portions of files are used while carrying out official duties.

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

MONITORING:
Use of Internet services provided through the DCN is subject to monitoring for security and/or network management reasons. When accessing the Internet, employees must adhere to the same code of conduct that governs all other aspects of judiciary employee activity. By using the government-provided computer and Internet connection, consent to monitoring is implied with or without cause. The Court reserves the right to monitor and/or audit the Internet activity logs for compliance with acceptable use policies, whether located on central computers or on individual PC's. Any use of government communication resources is made with the understanding that such use is generally not secure, is not private, and is not anonymous. For example, many Internet sites record who accesses their resources and visits their sites and may make this information available to third parties without the knowledge or consent of the user. The Systems

department will not view an individual's specific Internet activity unless requested by a judicial officer or a unit executive and approved by the Chief Judge.

VIOLATIONS:
Any violations of this policy will be subject to restriction or loss of access and other adverse action, up to and including termination of employment. The Court also has the right to notify the appropriate authorities if it discovers evidence of any possible illegal activities. This privilege to use Government equipment for non-governmental purposes may be revoked or limited at any time.

POLICY REVIEW:
This policy will be reviewed as necessary.

Reviewed
November 2010

INFORMATION TECHNOLOGY POLICY

ACKNOWLEDGMENT FORM

I, _____ have read and understand the Information Technology Policy of the United States District Court of Maryland. I understand that use of the system will be monitored by the IT department for security and network management reasons and my individual activity may be monitored for inappropriate use. I agree to abide by that policy during my employment with the Court. I understand that violation of this policy may subject me to disciplinary action.

_____
Signature

_____
Date