8.0 CERTIFICATION

I have read and I understand the Acceptable Computer Use Policy adopted by the Board of Judges on January 16, 2009.

_____ _____

Employee's/User's Signature Date

UNITED STATES DISTRICT COURT
for the
DISTRICT OF CONNECTICUT

ACCEPTABLE COMPUTER USE POLICY

SECURITY STATEMENT

Adopted by the Board of Judges on January 16, 2009

TABLE OF CONTENTS

UNITED STATES DISTRICT COURT
for the
DISTRICT OF CONNECTICUT

ACCEPTABLE COMPUTER USE POLICY

1.0 Overview
The United States District Court for the District of Connecticut ("Court") has published this Acceptable Computer Use Policy to provide guidelines that are consistent with the Court's established culture of openness, trust and integrity. The Court is committed to protecting its employees and the judiciary from illegal or damaging actions by computer users.

Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail (email), Internet browsing, Telnet, and FTP, are the property of the Court. These systems are to be used for official government purposes in serving the interests of the Court in the course of normal operations.

Effective security is a team effort involving the participation and support of every Court employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know and comply with these guidelines.

2.0 Purpose
The Court has adopted this policy for the authorized use of the Internet and computing resources. These rules are in place to protect the employee and the Court. Inappropriate use exposes the Court to risks including virus attacks, compromise of network systems and services, and legal problems.

3.0 Scope
These guidelines are not exhaustive. They apply to all Court employees, with such exceptions as may be authorized by the Board of Judges, and apply to others who are provided access to the Court's computing resources for the conduct of official government business.

4.0 Policy
4.1 General Use and Ownership
Court users of the Internet must adhere to the same code of ethics that governs all other aspects of judiciary activity. The Internet may only be used for authorized activities and must be used in a professional, lawful and ethical manner in accordance with the restrictions contained herein. Limited personal use of the Internet is authorized by the Court, provided that such use is kept to a minimum and does not interfere with job performance or the conduct of official business and does not compromise the mission or reputation of the Court.

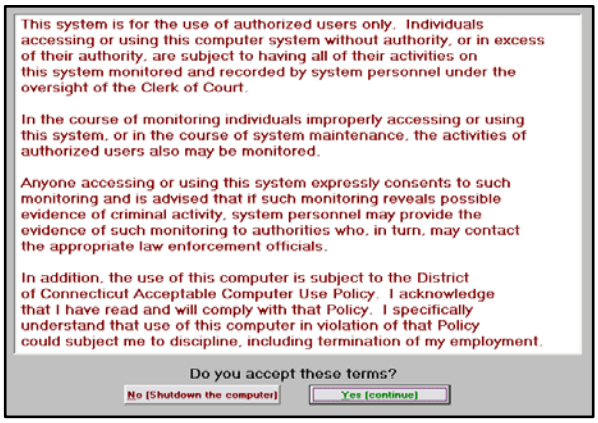
Responsibility

1. Use of the Internet via computer gateways owned or operated on behalf of the United States Courts imposes certain responsibilities and obligations on Court computer users and is subject to judiciary policies as well as local, state and federal laws. Court computer users must ensure that they use the Internet safely and productively, to avoid creating a bad image or compromising the interests of the judiciary in any way. To be acceptable, computer use must be ethical, reflect honesty and show restraint in the consumption of shared computer resources. Court computer users must demonstrate respect for intellectual property, ownership of information, system security mechanisms, and individuals' rights to freedom from harassment and unwarranted annoyance. Access to the Court's

computer systems (i.e., network, email, Internet) is a privilege, not a right. With this privilege comes great responsibility!

2. The Office of Information Technology (OIT) will install new software or upgrade software currently installed; such installations include but are not limited to commercial, locally developed, and freeware software. Court computer users shall not install any software on Court computers, but may request OIT to do so. Software can be installed as soon as compatibility with Court computers has been determined. Installations will be limited to software that supports the Court's mission. The Court reserves the right to refuse software that will severely affect other installed software or operating systems. All software that is in violation of any other Court policy shall also be refused. Additionally, the Court will remove software deemed inappropriate or damaging.

3. Personal use of Court computers shall be kept to a minimum. Employees are responsible for exercising good judgment regarding the reasonableness of personal use. Employees should be guided by departmental policies on personal use, and if there is any uncertainty, employees should consult their supervisor or manager.



4. Use of the Internet services provided by the Court is subject to monitoring for security and/or network management purposes. Court computer users are therefore advised of this monitoring and cannot use the Court's computers until they consent to this practice. Monitoring includes the logging of all resources and "sites" that are accessed. Users should further be advised that many external Internet sites also log who accesses their resources, and may make the information available to third parties. By participating in the use of Internet systems provided by the Court, users agree to abide by this policy as well as the Court unit's official policies on computer use and security. This policy hereby incorporates by reference the Code of Conduct for Judicial Employees which is applicable to all Internet activities. An employee's willful violation of the principles and provisions of this policy may result in disciplinary action, as stated in **Section 5.0** of this document.

4.2 Privacy and Security (see also Local Monitoring and Internet Blocking)

Access to the Internet is provided through the Judiciary's Data Communication Network (DCN). As part of the security system of the DCN's Internet gateway, a log is kept of all Internet activity passing through the DCN. The log is monitored at the gateway for improper use. If an individual accesses an Internet site or sends an electronic message through the DCN's Internet gateway, the fact that the activity originated from the United States Courts will be known by the receiving site or party. Accessing inappropriate Internet sites is not acceptable because it could be an embarrassment to the judiciary.

The Internet is not secure. Messages and information can be read or broadcast without the knowledge or consent of the author. Users should not, and cannot, assume that the messages they send or receive via the Internet will be private. Internet mail is also unreliable. Delivery and delivery times are not guaranteed due to unpredictable intermediary system and network outages, shutdowns, slowdowns and polling intervals. Users should not rely on Internet mail for time-sensitive communications or guaranteed delivery. Also, sometimes attachments to an email may not be readable by the receiving party. Note: The Lotus Notes "Receipt Requested" feature may not be honored by systems on the Internet. Users should not rely on this feature for Internet mail.

Various Guidelines:

1. System level passwords will be changed quarterly, user level passwords will be changed every six months.
2. All desktop computers, laptops, and workstations should be locked with a password-protected screen, that is activated by pressing Ctrl+Alt+Delete (at the same time) when the user is away from his/her computer.
3. Because information contained on portable computers is especially vulnerable, special care must be exercised.
4. Court computer users must use extreme caution when opening email attachments received from unknown senders, which may contain viruses, logic bombs, or Trojan horse code. When in doubt, users must consult OIT before opening email attachments.
5. To ensure compliance with this policy, each Court computer user is required to attend one (1) hour of Information Security (InfoSec) training annually. As InfoSec changes, it is important that each user is made aware of these new security topics in order to protect the user and the Court.

4.3 Unacceptable Use

Court computer users are specifically prohibited from using the Internet and/or computing resources for the following purposes:

1. Sending data, files, or mail over the Internet that contain any discriminatory or malicious statements;
2. Making unauthorized commitments or promises of any kind that might be perceived as binding the Government;
3. Sending confidential information over the Internet, unless it is for Official Court-related purposes. The Internet is not a secure means of transmission and can cause confidential information to be compromised should it be read by an unauthorized party;
4. Taking part in Internet discussion forums or blogs that are not associated with official government business;
5. Posting opinions on Internet forums or blogs that are personal in nature;
6. Using the network connection for commercial or political purposes or for private gain;
7. Using the network for illegal activities such as illegal gambling, illegal weapons, terrorist activities, and any other illegal or prohibited activities;
8. Intentionally accessing sites or downloading/ transmitting information that contains sexually explicit material, except when authorized as necessary to the user's job responsibilities.
9. Intentionally accessing, either locally or remotely, another employees files, data, email, or other electronic information unless explicitly authorized by a judge or the Court Unit Executive (CUE).
10. Accessing or viewing streaming media (audio or video) or Internet radio or television, except when authorized as necessary to the user's job responsibilities.

Confidential/Proprietary Information

Users may access only files, data, email, or other electronic information that are their own, that are publicly available, or to which they have authorized access. Improper use or distribution of information is prohibited. This includes copyright violations such as software or music piracy. Users will show respect for intellectual property and creativity by giving appropriate credit when files or portions of files are used in connection with the performance of official duties.

Downloading

Users should refrain from any use or practices that might jeopardize the judiciary's computer systems and data files when downloading files from the Internet. Only material and software that is authorized and properly licensed may be downloaded, and files must be checked for viruses. Large downloads, such as those required by Information Technology personnel in the performance of their duties, should be performed at non-peak times to avoid diminished network performance response time for other network users.

Email and Communications Activities

1. Caution should be exercised with regard to the volume and size of email being sent. In addition, attaching large files to email messages can drain the resources of the Court's email system. Placing a link to a file on the Internet/Intranet/Extranet within an email is a useful alternative when sending emails because it reduces the size of the email by directing the user to the file.
2. Internet mailing lists can produce a high volume of messages automatically, so this activity should be avoided.

Access by Court computer users to personal Internet email accounts (e.g., AOL, Gmail, Yahoo, etc.) from within our networks is generally prohibited. Use of these accounts poses threats to the judiciary's information technology infrastructure because most do not provide virus scanning of email and attachments. Court computer users may make minimal access to personal Internet email accounts only with the permission of a judge, CUE, or supervisor.

> *Judiciary personnel are reminded of the Judicial Conference policy, adopted at its September 2002 session, regarding Personal Use of Government Office Equipment (including Information Technology), which states that, unless further restricted by local court policy, judiciary employees are permitted limited use of government office equipment (including information technology) for personal needs if such use does not interfere with official business and involves minimal additional expense to the government. Sending and receiving a* ***limited*** *amount of personal email in your Lotus Notes court account is consistent with this personal use policy and is far preferable to accessing a personal Internet email account from a computer security point of view.*

The use of automatic email forwarding to personal Internet email accounts which can result in sensitive case or personal information being forwarded over network connections that are subject to interception by malicious outside Internet users must be avoided. A safer alternative is to keep up with email while away from the office by using Court-issued remote access via a virtual private network (VPN) connection back to the Court, to use J-Ran web-mail, or to use a Court-provided wireless email device (such as a Blackberry) to receive email, all of which provide secure email access to authorized off-DCN users.

Court computer users must avoid advertising their Court email address over the Internet. In particular, limit the recipients of your email messages to people and organizations you know. Users should not use the "Reply All" function when responding to messages sent to lists or people not known to them. This helps reduce the possibility that your Court email address will be captured by spammers, phishers, or other malicious Internet users.

The following Email and Communications Activities will ***always*** be considered unacceptable:

1. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
2. Unauthorized use, or forging, of email header information.
3. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
4. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
5. Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).
6. Intentionally accessing, either locally or remotely, another employee's email unless explicitly authorized by a judge or the Court Unit Executive (CUE).

System and Network Activities

The following activities are strictly prohibited, with no exceptions:

1. Introduction of malicious programs into the network or server (i.e., Viruses, Worms, Trojan horses, email bombs, and the like).
2. Revealing any Court computer user password (i.e., network, email, etc.) to others or allowing use of your account by others. This includes family and other household members when work is being done at home. Court computer users are responsible for all actions taken through their accounts.
3. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the user is not an intended recipient or logging into a server or account that the user is not expressly authorized to access, unless authorized as part of official duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information.
4. Executing any form of network monitoring that will intercept data not intended for the user's host, unless this activity is a part of the user's regular job duties.
5. Circumventing user authentication or security of any host, network or account.
6. Providing information about, or lists of, Court employees to parties outside the Court, unless authorized by a judge or CUE.
7. The DCN is an unclassified network. Court users agree to not introduce, store, pass, or process classified data over the network, unless it is for Official Court-related purposes.

Other Unacceptable Uses

The use of peer-to-peer file sharing, chat rooms, and instant messaging for communicating with persons or entities outside the judiciary's private data communications network is prohibited. File sharing (using programs such as Napster, Grokster, Morpheus, and certain interactive Internet games), chat rooms, outside instant messaging (such as AOL Instant Messenger) and Internet based telephonic or video programs such as Skype, are based on Internet technologies that circumvent the security protections provided by existing DCN. Accordingly, all such uses are prohibited.

4.4 Local Monitoring and Internet Blocking

For security and network maintenance purposes, authorized individuals acting on behalf of the Court will utilize software such as WebSense, SNORT, Wire Shark, Sniffer, Etheral and other tools used for blocking and monitoring Internet use at the local level.

The Court will audit networks and systems on a periodic basis to ensure compliance with this Policy. If the Court determines that a particular employee is abusing his/her computing privileges, the Court or the user's supervisor will limit/remove that user's privileges.

Email

Personal Web Based email accounts will be blocked except those identified by the Administrative Office (AO) which provide virus scanning of email and attachments, such as Yahoo (which may be used only for official business purposes). Any exceptions to this Policy must be reviewed and approved by the Board of Judges.

Streaming Media

To avoid decreases in network capacity and to minimize system downtime which can occur due to the use of bandwidth-intensive applications such as streaming media or Internet Radio, the following internet protocol activity will be blocked between 8:30 AM and 5:00 PM, Monday through Friday:

- Internet Radio and TV
- Streaming Media (Audio/Video)

Accessing the following site categories is ***always*** unacceptable:

- Adult/Sexually Explicit
- Chat Rooms and Instant Message
- Gambling
- Games (Internet or locally installed)
- Hacking
- Intolerance and Hate
- Illegal Drugs
- Peer-to-Peer file sharing networks
- Phishing & Fraud (identity theft)
- Spyware (live viruses)
- Tasteless & Offensive
- Violence

Judiciary employees may have a business purpose in accessing a blocked site, or an appropriate site may be blocked for some unknown reason. If this is the case, access rights may be restored, upon email request, following the approval of the respective judge or CUE. Such request must indicate the specific site that is blocked and the reason access is needed. Once approved, the email shall be forwarded to the IT Director of the Court unit for appropriate action.

5.0 Enforcement

The judges, CUEs, and supervisors are in a position to observe computer users daily. If a judge, CUE, or supervisor suspects that a Court computer user has committed a violation of this Policy an investigation will be conducted. The judge, CUE, or supervisor may authorize the IT Director to produce a report of any user's Internet activity. The report shall be limited to the Internet and computer use activities of the employee in question. Thereafter, the report may be used as the basis for disciplinary action. Any report produced shall be confidential and viewed only by those individuals designated by the judge, CUE, or supervisor. The user's immediate supervisor will be informed of any security violation. Following an investigation, the user's computer privileges can be restricted or removed at the discretion of the judge, CUE, supervisor, or IT Director.

Any employee who violates this policy will be subject to the full range of disciplinary actions, up to and including termination.

6.0 Definitions

Blogs - Internet sites where users can read and/or post information or opinions about a specific topic

Chat rooms - electronic forums where users can visit and exchange views and opinions about a variety of issues

Computing Resources – any form of computer hardware, software, or personal device (e.g.: Blackberry, PDA, etc.)

Data Communications Network (DCN) – Judiciary Wide Area Network (WAN)

Denial of Service (DoS) - an attack on a site or service that overwhelms a Web site's servers with requests or messages, thus preventing users making legitimate requests

Extranet - a Web site for selected users, rather than for the general public. An extranet uses the Internet as its transmission system but requires a password to gain entrance

File Transfer Protocol (FTP) - allows a user to copy or send files (HTML-documents, graphic images, spreadsheets) from one computer to another via the Internet

Forged routing information - the process of selecting paths in a network along which to send network traffic has been compromised to mask/hide specific routing information

InfoSec – an abbreviation for Information Security

Instant Messaging - the act of instantly communicating between two or more people over a network such as the Internet

Intellectual Property - Creative ideas and expressions of the human mind that have commercial value and receive the legal protection of a property right

Internet – stands for: ***Inter***connected ***Net***works

Internet Gateway - a device that provides access to the Internet from another network. This is usually dedicated to a router

Intranet - Inter-connected network within one organization that uses Web technologies for the sharing of information internally, not world wide

Logging - The process of storing information about events that occur on the firewall or network

Logic bombs - a program that will execute a pre-programmed routine (frequently destructive) when a designated condition is met, such as a date

Malicious programs - Software capable of performing an unauthorized process on an information system

Network Sniffing - The practice of monitoring or eavesdropping on electronic transmissions

Operating Systems - provide an interface between the user or application program and the computer hardware (i.e., Windows XP (Home/Professional))

Packet spoofing - An attempt to gain access to a system by posing as an authorized user

Peer-to-Peer file sharing - an application that runs on a personal computer and shares files with other users across the internet

Phisher – one who engages in a type of deception designed to steal a user's valuable personal data, such as credit card numbers, passwords, account data, or other sensitive data

Pinged floods - a simple denial-of-service attack where the attacker overwhelms the victim with ICMP Echo Request (ping) packets

Security breach - External act that bypasses or contravenes security policies, practices, or procedures. A similar internal act is called security violation

Shared computer resources - this technique uses desktop computer processing power of multiple machines that would otherwise be wasted at night, during lunch, or even in the scattered seconds throughout the day when the computer is waiting for user input or slow devices

Spammer - someone who sends unwanted email (often in bulk)

Storage Media - The physical device itself (i.e., hard drive), onto which data is recorded. Magnetic tape, optical discs, floppy disks are all storage media

Streaming Media - Technical term for digital audio or video transmissions via the Internet

Telnet - the main Internet protocol for creating a connection to a remote server

Trojan Horse Code - This is a program that disguises itself as another program. Similar to a virus, these programs are hidden and cause unwanted effects

Virtual Private Network (VPN) - These systems use encryption and other security mechanisms to ensure that only authorized users can access the network and the data cannot be intercepted

Virus - a piece of code that is secretly introduced into a computer system in order to corrupt it or destroy data

Web Browser - Software to navigate the Internet (e.g., Microsoft Internet Explorer/Mozilla Firefox)

Worm - a self-replicating computer program

7.0 Revision History

This policy may be amended at any time by the Board of Judges.

Adopted by the Board of Judges on January 16, 2009