Policy Manual

Technology

Chapter 7

Table of Contents

Technology

The national objectives of the judiciary IT Program as stated in the Guide to Judiciary Policy, Volume 15 are consistent with the local objectives of the Information Technology (IT) Unit for the United States Probation Office for the District of Connecticut.

As the office develops an overall system of goals and objectives, the IT Unit will tailor its unit goals to not only meet the Administrative Office's directives but the local needs as well.

1. DISTRIBUTION OF EQUIPMENT

Each position within the office is identified and the equipment that is needed is listed. It is the responsibility of the IT Unit to ensure that each individual on the staff receives the equipment allotted for his/her position.

If a situation arises where an individual requires additional computer equipment, a statement of requirements should be submitted to the IT Unit with a copy submitted to the individual's immediate supervisor.

The IT Unit will assess the request based on, but not limited to, the following:

- content of the statement of requirements
- office's goals & objectives
- availability of funds

Once a decision is made the individual will be notified and if the request is granted, the procurement process will begin.

2. USE OF EQUIPMENT - GENERAL

2.1 General

Employees may use government equipment and services for officially authorized purposes only. Limited personal use of government equipment and services by employees is an authorized use under the conditions set forth below. This policy provides users with a professional and supportive work environment while meeting expectations that federal tax dollars are spent wisely. The probation office recognizes that users are responsible individuals, capable of balancing the privilege of limited personal use with the expectations of fulfilling their job requirements. This policy does not supersede any applicable laws or regulations.

2.2 Personal Use Exception

Employees are permitted limited personal use of government office equipment and services provided that the use:

- does not interfere with official business;
- occurs only during non-work time (i.e.,when the employee is not otherwise expected to be addressing official business);
- involves minimal additional expense to the government; and
- is not illegal, disruptive, offensive, or otherwise inappropriate, as described below.

Minimal additional expense occurs when the federal government already provides equipment and services and the personal use results in no additional charge, minimal wear and tear, the use of limited amounts of consumables (i.e., electricity, ink, toner, paper, and/or supplies), and no more than minimal burdens of communications infrastructure and data storage capacity.

This privilege may be revoked or limited at any time and does not convey to employees an inherent right to use government property for personal purposes, nor does it permit modifying equipment, including loading personal software or making configuration changes. Supervisors may further restrict personal use based on the needs of the office or work performance.

2.3 Inappropriate Personal Use

Employees are expected to conduct themselves professionally in the workplace and to refrain from using government equipment and services for inappropriate activities. Inappropriate uses include those that:

- are illegal, offensive, or harassing to co-workers or the public; such as hate speech and material that ridicules others on the basis of race, color, religion, gender, sexual orientation, national origin, or disability;
- could cause congestion, delay, or disruption of service to any government system or technology (including video, sound, and other large file attachments and mass mailings);
- involve any illegal activity, including gambling or copy right violations;
- involve obscene, pornographic, sexually explicit or sexually oriented material;
- are for commercial purposes or in support of outside business or employment activity of the employee or a friend or relative;
- involve fund-raising, endorsements of products or services, lobbying, or any prohibited political activity.

2.4 Responsibilities – Users

Users should adhere to applicable rules, regulations, and standards of ethical conduct. Each user is responsible for

- practicing good judgment when accessing and using any government equipment and/or services;
- ensuring that any use of government property is for official business or is otherwise authorized and does not involve inappropriate activity;
- ensuring that communications reflect appropriate business ethics and practices and that any personal use does not convey the appearance that the user is acting in an official capacity;
- performing work assignments. Users should report to their supervisors the receipt of any harassing or threatening material in the workplace. After reading this policy, users should consult with their supervisors to resolve questions.

2.5 Responsibilities – Management

Management is responsible for

- ensuring that users are fully informed about usage policies;
- monitoring use;
- ensuring that appropriate approvals are obtained;
- informing higher level management of misuse;
- determining if materials, documents, messages and/or attachments constitute a federal record;
- assigning work.

2.6 Physical Security

The physical security of your assigned laptop is your personal responsibility, so please take all reasonable precautions. Be sensible and stay alert to the risks.

Keep your laptop in your possession and within sight whenever possible just as if it were your wallet, handbag or mobile phone. Be extra careful in public places such as airports, railway stations or restaurants. It takes thieves just a fraction of a second to steal an unattended laptop.

If you have to leave the laptop temporarily unattended in the office, meeting room or hotel room, even for a short while, secure the laptop in a locked cabinet or use a laptop security cable or similar device to attach it firmly to a desk or similar heavy furniture. These cable locks are not very secure but deter casual thieves. While on travel, room safes may be used, but be aware that hotel staff may have ready access to these safes. A laptop security cable secured to heavy furniture may also be used in a hotel room.

Lock the laptop away and out of sight when you are not using it, preferably in a strong cupboard, filing cabinet or safe. This applies at home, in the office or in a hotel. Never leave a laptop visibly unattended in a vehicle. If absolutely necessary, lock it out of sight in the trunk or glove box, but it is generally much safer to take it with you.

Carry and store the laptop in the supplied probation office padded laptop computer bag or strong briefcase to reduce the chance of accidental damage. An ordinary-looking briefcase is also less likely to attract thieves than an obvious laptop bag.

If it is lost or stolen, notify the police immediately. Procedures to follow are located in Chapter V - Internal Controls, Section H - Board of Survey.

At the end of the day, if laptops are left in the office, they must be secured in a locked cabinet before leaving for the day.

2.7 Penalties for Misuse

In accordance with the Guide to Judiciary Policy, users may be subject to penalties for inappropriate or unauthorized use of government office equipment and/or services. Penalties may include administrative action, ranging from counseling to removal from employment, criminal penalties, and financial liability, depending on the nature and severity of the misuse.

2.8 Guidelines for Use and Maintenance

The following provides a general outline of office practices designed to assist with the proper use and maintenance of government equipment and services. This information is not intended to be all-inclusive but to share useful information with employees.

2.8.1 Message Content

Originators (users) are responsible for the quality, tone, and content of their own written and telephonic communications, including e-mail and voice mail. Written documents, e-mail messages, and voice mail messages are a reflection of the originator (user) and may be forwarded to others without any explicit permission.

2.8.2 Care of Content

Users should use forethought when sending and forwarding written documents, email messages, and voice mail messages. Do not leave sensitive information on voicemail; limit the length and details of your message; and leave your phone number so the recipient can respond.

2.8.3 Correspondence Official Agency Record

Originators and forwarders should be aware that all written and digital communications leave a paper trail and may become official agency records.

2.8.4 Subject Line

Written documents and e-mail messages should have an informative subject line and should include a name and number for the recipients to call for more information.

2.8.5 Addressees/Recipients

Limit distribution of materials and messages, whether electronic or hard copy, to only the parties necessary to ensure a proper and efficient response.

2.8.6 Proofread

Originators should re-read all documents, materials, and messages for correct spelling, grammar, content, tone, and purpose before sending. Originators should take advantage of the tools provided in current systems, such as spell check, grammar checkers, and the thesaurus, as well as asking co-workers to read for clarity and tone.

2.8.7 Attachments

Exercise discretion when sending or forwarding large written documents, e-mail messages and/or attachments. Consider the purpose, cost, and storage available before copying, sending, forwarding, and/or printing. Transmitting and storing may be difficult when attachments include tables, graphics, colors, forms, or heavily formatted documents.

2.8.8 IDs - Log-On Identification and Tokens

Each user is given an individual log-on ID and/or token and is responsible for maintaining appropriate passwords. Users should not use the ID and/or token of another user to send messages or access voice mail unless specific permission is given. If it is necessary to send a data or voice message from the equipment of another user, the originator should add an explanatory note in the text or voice mail of the message. Also, users should not share another user's e-mail address without explicit permission of the owner of the e-mail address.

2.8.9 Maintenance

Users should make a timely effort to read, listen, and respond to e-mails, voice mails, and correspondence. When a user is absent from the office for an extended period of time, tools are available (such as e-mail rules and voice mail options) to inform others that the user is not able to respond immediately. Users should routinely review and purge e-mail/voice messages and logs, and hard copy files in accordance with federal records guidelines.

To assist in maintaining the entire e-mail system, users should not keep more than 1,200 total messages combined in the message log, trash, in-box, and all other active folders; and use archive options for reducing the number of stored files. For voice mail systems, limit the number of stored messages. For additional guidance and assistance about maintaining, archiving, and storing records contact the IT Unit.

2.8.10 Privacy

Authorized users should expect no privacy in the use of government equipment and/or services. Furthermore, any use of government equipment or services, for whatever purpose, is not secure, private, or anonymous; and almost any use may be monitored or recorded. Users accessing and using government electronic equipment and services, including personal computers, network drives, e-mail, Internet and Intranet service, expressly consent to monitoring of their usage and to access by appropriate officials to records created, received, or maintained by them.

Users should be aware that Internet sites capture the domain name of accounts accessing a specific site and maintain a record of the domain name. It could be embarrassing to a user and the judiciary if the domain name "uscourts.gov" were found on the access records of an inappropriate site.

3. WORKSTATIONS

3.1 Desktop Workstations

The probation office is committed to meeting the needs of the staff by providing alternative methods to complete work-related tasks. Desktop workstations are provided to employees as required.

Users must adhere to the following sections of the manual regarding the use of laptops:

- Use of Equipment – General
- Network Security
- Internet Access
- Use of Personal Software on Government Machines

Any unofficial use of the workstation not meeting the guidelines established in those sections will be reviewed by the Director of Information Technology and the chief probation officer. The employee may face disciplinary actions for any illegal or inappropriate uses of the laptop.

3.2 Configuration of Workstations

All workstations assigned generally will have a standard configuration. The workstations will be configured with the standard supported office applications such as:

- Microsoft Word
- Excel (spreadsheet)
- Lotus Notes E-Mail (electronic mail)
- Adobe Acrobat
- Co-Sign

- Web Browsers (Internet Explorer)
- Internet and DCN Access

Each workstation will be configured with Lotus Notes Client to provide e-mail access. Each workstation will include access capability to the office network and various Judiciary resources. This access will allow users to download and upload files to and from their user directories.

If an employee is using the workstation for a special project and requires access to special software, the employee must send an e-mail to the Director of Information Technology requesting the software and the reason why it is needed. A copy of the request should be sent to the individual's supervisor. The Director of Information Technology will research the request and the software will be installed if authorized.

At no time should an employee install any software or software patches on the office workstation unless instructed to by the IT Unit, i.e. all Microsoft patches should be applied.

3.3 Virus Scanning

It is the responsibility of the employee to scan all files for viruses before copying a file from a laptop to any machine connected to the probation office network. The use of the virus software will be addressed in the laptop training program. Any employee who fails to follow proper scanning procedures and introduces a virus into the network may be found negligent and may suffer disciplinary action as deemed appropriate by the Director of Information Technology.

Employees are also prohibited from changing the configuration of the workstation. Installation of software or reconfiguration of the workstation could result in the denial of the use of the workstation in the future. Any suspected violations will be brought to the attention of the Director of Information Technology for investigation and report to the chief probation officer.

3.4 Termination of Workstation Use

If any employee is voluntarily or involuntarily terminated from the probation office, the employee must immediately cease to use any assigned workstation.

If a former employee fails to stop using the workstation and continues to use it after the date that they have officially resigned or were terminated from the probation office, the previous employee is responsible for any expenses incurred by the probation office. In addition, the employee may face legal charges if the violation is substantial.

3.5 Maintenance

Occasionally workstations will be checked for physical damage and proper configuration. All unauthorized software will be removed. The IT Unit is not responsible for any personal files

left on a workstation. Personal files found on the workstation are subject to removal. Any irregularities or violations of section D. Use of Equipment will be reported to the Director of Information Technology and the Chief Probation Officer.

The judiciary's desktop PCs, portable PCs, application and file servers, and printers are presently funded for replacement on a three-year cycle. With equipment replacement occurring regularly, court units/FDOs should include end-of-life equipment retirement in their systems life-cycle planning. *(Guide to Judiciary Policy § 550.20 Equipment Replacement Funding)*

The workstation can be used for temporary storage of files. All files should be scanned for viruses and then transferred to the employee's network drive. Any file that is left on the workstation is subject to removal by the IT Unit without notification of the owner of the file. Employees must take responsibility for their work and provide accurate and safe backups of their work material when using the office workstations.

4. LAPTOP COMPUTER FOR HOME PROGRAM

Staff may request surplus laptops for home use in support of the Work-at-Home program. Requests for laptops for home use should be made in writing or e-mail and submitted to the Director of Information Technology and the appropriate supervisor. Every attempt will be made to furnish individual staff members with the equipment that is necessary for special assignments or projects.

Staff members must follow the policy stated in Section 2 - Use of Equipment - General. In addition, the staff must be aware of the dangers of viruses and should follow the policy and procedures in Section 5 Network and Computer Security when transporting files from their home PC to their work PC.

All equipment (except mobile equipment) that leaves the building must be identified on an equipment hand receipt that will be created by a member of the IT Unit and signed by the assignee (staff member) of the equipment. The equipment receipt will be retained by the IT Unit and will be signed off by an IT Unit member when equipment is returned. All staff members who have been issued equipment in support of the Work-at-Home program must read and sign Acknowledgment Receipt/Return of Automation Equipment. When the staff member is separated from service with the office, all equipment issued for home use must be returned. The returned equipment must be in satisfactory condition.

Any unsatisfactory condition will be reported to the Director of Information Technology, who will take the appropriate action. In addition, the IT Unit may request return of any issued equipment at any time provided that it supplies the staff member with a responsible explanation for the request.

The IT Unit will install an OS (Operating System) on the laptop and the basic software for office duties, no other support will be provided. See Section 3.2 Workstation configuration fro an example of basic software types. In the event of a hardware failure, the equipment will not be fixed. The equipment will be returned to the IT Staff and based upon availability, an equivalent piece of equipment will be substituted immediately.

5. NETWORK AND COMPUTER SECURITY

The probation office's local network security policy is designed to adequately protect the confidentiality, integrity, and availability of information accessed by users authorized to view and/or manipulate the information during the course of business-related duties. By adhering to these standards, users help to ensure the protection of the probation office network.

The network security policy is binding in all situations where probation office's equipment and services are in use, whether an active connection to the probation office's network is in use or not i.e. working on a laptop with no connectivity to the network. The policy outlined pertains equally to permanent probation office employees, temporary contractor personnel, and to courts personnel visiting from family districts.

5.1 Maintaining a secure and stable technology infrastructure

5.1.1 Computer Security Training

Prior to accessing the probation office network, users are required to attend a computer security orientation that educates users on local network security policies and how to consistently use strong computer security practices during their normal work duties. Since computers are now an inseparable tool in an employee's workday, such a computer security orientation is critical for giving employees the information they need to continually succeed.

Additionally, users are required to attend a Computer Security Training class offered annually.

5.1.2 Windows Domain Group Policy

Computer systems that authenticate to the probation office network are updated at each logon session with a Windows operating system policy that enforces a standardized configuration on every system, which includes settings for enforcing probation office network password requirements and periodic inactive workstation locking

5.1.3 Computer Security Banner

At the network logon phase, probation office network users are informed of the probation office's rights and capabilities to actively monitor network activities. Systems monitoring is for the purpose of investigating suspicious network activity and

taking appropriate actions deemed necessary to protect network resources. Monitoring and scanning is also authorized for the proactive measurement of system vulnerabilities and troubleshooting technical issues, (e.g. anomalies in systems performance).

5.1.4 Workstation Locking

Computer systems actively logged on with probation office network credentials are locked when no interactions with the system are detected. Computer systems are locked with a screen saver when they are inactive for 10 minutes.

5.2 Password Requirements:

5.2.1 Network Access

Passwords are an important aspect of computer security and are critical to the successful use of probation office systems and applications. Access to the probation office network infrastructure is strictly governed with the use of verifiable user account/password combinations.

First-time network users are required to create a strong password before logging into the probation office network. Passwords must adhere to the following criteria,

1) Contains 1 or more uppercase characters [e.g., U, C, L]
2) Contains 1 or more lowercase characters [e.g., w, e, p]
3) Contains 1 or more numeric characters [e.g., 2, 5, 9]
4) Contains 1 or more special characters [e.g., @, &, #]

Additionally, passwords cannot contain character string matches to a user's network name. For example, Frank Thomas' user name, thomasf, would be forbidden from use in his probation office network password [e.g., "thom", "masf", "thomas", etc.].

If any probation office network violations are detected in the process of creating a new or updating an existing network password, the probation office network will advise the user of the violation and prompt the user to choose a network password that meets security policy criteria.

Password changes are forced every 45 days. Further, passwords must be unique for the first 10 changes. For example, if Frank Thomas decided that his password was to be Rhod3@Island, he would not be able to use this exact password again until he had changed his passwords at least 10 times. However, Frank would be allowed to use the same password as his base (Rhod3@Island) plus adding a number at the end (Rhod3@Island1), thus creating a new password to meet the probation office's requirements.

For help with creating easy to remember, but hard to guess passwords, review the following resources:

- Guide to Creating and Protecting Strong Passwords
- Five Password Best Practices
- Pass the Word – Don't Share

5.2.2 Applications Access

There are numerous applications in use at the probation office, all of which require a password for authenticated access.

The IT Unit grants access to probation office applications on an as-needed basis. As such, the majority of probation office staff will not have access to all of the actively used probation office applications at any given time. Executive management staff [chief probation officer, deputy chief probation officers, and the director of information technology] are the only exceptions to this rule, who may exercise the right to have access to all active probation office applications at once.

All active probation office applications are fully tested by the IT Unit and a committee of staff testers prior to production use. Official probation office applications are implemented to assist in the effective administration of our District's specific duties, as recommended by the Administrative Office of the United States. All applications are implemented in such a manner as not to interfere with the operations of any required IT-related applications or services implemented by the Administrative Office, or with the operations of optional IT-related applications or services provided by the Administrative Office which our District has chosen to adopt.

5.3 Symantec EndPoint Protection

The probation office uses Symantec Endpoint Protection v12, hereafter referred to as SEP, as its comprehensive security solution. The program integrates the operations of antivirus, antispyware, and desktop firewall clients into one. The solution is installed on all Windows operating system-based machines, including servers and user workstations - both desktop and laptop systems. Definitions for each component are automatically updated on every system weekly, or more frequently as released by Symantec.

5.3.1 Antivirus

When actively running, users are not required to administer the SEP's antivirus operations at all, as the client will update its definitions automatically, as well as automatically scan for and block detected threats. However, occasionally the client may become disabled, at which time a user should either attempt to re-enable the client by right-clicking on the SEP shield icon on the system taskbar [the lower right-hand corner of their system's desktop] and select"Enable Auto-Protect",or contact an IT Unit member for immediate assistance if this doesn't re-activate the SEP client.

If users encounter a virus warning message on their system, they are to follow the actions recommended by the SEP client, except in any cases where those actions may request the user to delete any files. If a file deletion is recommended, the user must not delete the reported file but must contact an IT Unit member for further assistance.

5.3.2 Antispyware Programs

Antispyware protection is continuous as definitions are automatically loaded when available and full scans run weekly on a predetermined schedule to detect and remove spyware

Users must allow the SEP anti-spyware scans to run as configured by the IT Unit on a weekly or more frequent schedule. Further, users are not allowed to disable the SEP client's antispyware solution on their system without express permission from an IT Unit member.

5.3.3 Firewalls

All user workstations - desktops and laptops - are protected with the SEP client's desktop firewall solution. This component blocks unauthorized access and control of the workstation's data and/or the computer itself, or access to probation office network resources. Updates for the SEP client's firewall solution are administered automatically and does not require the user to interact with the product.

Users are not allowed to disable the SEP client's desktop firewall solution at any time without express permission from an IT Unit member.

5.3.4 User Responsibilities

Users are not required to interact with the SEP solution, as the SEP client persistently monitors its target system's activity and enables appropriate protections, as needed. However, there are certain responsibilities that probation office users must assume when using officially provided computer equipment, such as:

- Periodically checking their operating system trays to verify that the SEP shield icon  is active and running. The icon is found next to the Time Clock at the lower right-hand corner of the Windows desktop.
- Attempt to re-enable the client if it becomes disabled by right-clicking on the SEP shield icon and selecting "Enable Auto-Protect", or contact an IT Unit member for immediate assistance if the attempt to re-activate is unsuccessful.
- Call an IT Unit member for immediate assistance if the SEP client's protection appears to be missing.

5.4 Systems Patch Updates

Probation office systems are regularly maintained with operating system and applications patches released by their respective vendors. Such patches are installed to maintain the efficiency of installed programs and for preventing the exploitation of known system vulnerabilities. All system updates are administered automatically and do not require any user interactions.

Probation office users are not allowed to install any systems or application updates without the express approval of the IT Unit. Since the operation of technical office solutions are sometimes dependent on a specific software configuration or version, users may accidentally render these solutions inoperative by installing software program upgrades and/or system patches.

5.5 Systems Monitoring

The probation office IT Unit reserves the right to use technical solutions specifically designed to:

- Gather and analyze network traffic,
- Determine the vulnerability status of probation office systems and remediate discovered vulnerabilities, and
- Detect and block network activities that may indicate the unauthorized use of network resources, including the unauthorized collection and use of data by either internal personnel or external parties lacking authorization to use probation office material and resources.

Presently, the probation office IT Unit uses a collection of systems that assists with these goals, some of which are listed below:

- Websense
- CISCO firewalls
- Solarwinds ipMonitor

6. WIRELESS ACCESS POINTS

A Wireless LAN (WLAN) is a local area network without physical interconnecting wires The computing devices in a WLAN communicate with one another using radio frequency electromagnetic airwaves. In an infrastructure WLAN, wireless stations communicate with one another via the access point, which also serves as the bridge that interconnects the WLAN and the wired network.

Physical Security for WLAN Operations - the wireless LAN controller (WLC) is housed in the same physical location as the network switches in the New Haven office. The wireless access

points (WAPS) are located in the ceiling of each office to provide coverage throughout the office space.

Authentication is provided by a RADIUS server, users must use their JPORT/VPN user name and password to gain access to the WAP. Once the user's credentials have been verified by the RADIUS server the user will have access to the intranet and internet using the courts gateways. All wireless connections follow the same guidelines and security as wired connections.

6.1 WLAN Administrator Responsibilities

The WLAN Administrator manages the day to day operations of the WLAN devices and keeps the management and security administrator up to date on issues as they arise.
Responsibilities include:

- Ensuring patches and updates are implemented and devices maintenance is performed to keep the WLAN running efficiently and safely.
- Assigning user accounts and managing laptop devices which are used to access the WLAN.
- Ensuring that the wireless devices access the WLAN through only approved methods.
- Ensuring services and access permissions for lost or stolen devices are disabled as soon as possible.
- Notifying the Director of Information Technology if issues arise which may cause security risks to the WLAN including forwarding reports of lost or stolen wireless devices.
- Safeguarding the wireless information resources with which they have been entrusted.
- Adhering to policies and procedures for the administration of wireless devices, including:
    - Labeling all wireless devices with identification information prior to deployment
    - Maintaining an inventory of all wireless devices

6.2 WLAN User Responsibilities:

WLAN user responsible for:

- Adhering to the procedures and policies of their local court.
- Safeguarding the wireless devices in their possession.
- Safeguarding the information resources being accessed or transmitted via any wireless technology.
- Promptly reporting the loss or theft of wireless devices, or any other breach of wireless security, to their supervisor or administrator.

6.3 Access Points

An Access Point (AP) is the point of entry into the wired network from a wireless device. Our AP's utilize a minimum encryption standard of Wi-Fi Protected Access 2 (WPA2)2 or better and is certified by the WiFi Alliance as an enterprise device that supports this standard.

All interfaces, such as management interfaces using Hypertext Transfer Protocol (HTTP) or Simple Network Management Protocol (SNMP), must be encrypted to ensure protection of the network.

The Service Set Identifier, SSID, provides the name of a wireless network and is not encrypted in transmission. Therefore, APs should be configured with an SSID which does not immediately identify the organization. The SSID can be any name or combination of letters and numbers and should not offer information about the network. Additionally, access points should be configured with the SSID broadcast feature disabled.

6.4 User Devices

A wireless Network Interface Card (NIC) installed in the wireless client should be 128-bit WPA2 capable, allowing encrypted communications between the wireless client and the AP.

Before connections are made, the client must be configured to meet the policies of the local court unit. These policies should provide guidance on maintaining and updating antivirus software, routinely verifying that the wireless device is free of spy-ware and malware, and ensuring that all patches and updates have been applied to the Operating System (OS) and applications.

On each computer accessing the AP, network connection properties should be configured to allow connection to AP networks only, which means computer-to-computer (peer-to-peer or ad-hoc) connections should be disallowed.

Computers should be specifically set up to connect to the WLAN through the SSID of the AP as default. The SSID needs to be set up on the client machine manually.

Access by wireless should be limited to only the information and devices necessary to perform assigned duties and only devices that have been approved by the WAN Administrator. If file sharing is not needed, it should be disabled on wireless networks or local networks interconnected with wireless access.

Password protected screen savers should be used to ensure that only authorized users access the machine and networks. Screen savers should be activated after no more than 10 minutes of idle time.

6.5 Technical Controls

When implementing new devices, several configuration parameters need to be modified to ensure that security is taken into consideration before the devices are activated. Below are technical steps that are followed.

- **Default Accounts:** Vendor and default account passwords must be changed on all devices. Additionally, the administrator accounts must be modified to ensure that unauthorized users cannot easily identify them.

- **Activity Logs:** Wireless devices must collect activity logs. The purpose of these logs is to identify use of the wireless network by unauthorized users. Activity logs should contain information to identify the user ID, machine ID, date, time and actions taken. Logs containing activity data must be protected from unauthorized access or modification. Security administrators must examine activity logs daily for suspicious activity and attempts to gain unauthorized access.

  Activity logs can generate large files which may cause deterioration of system capabilities if not monitored closely. Machines with limited memory should be configured to save logs to files on other servers if they are unable to store the files locally.

- **RF Monitoring:** A radio frequency (RF) monitor provides a periodic snapshot of the wireless environment and helps to identify rogue APs and other unauthorized devices. It can also be used as a wireless intrusion detection system (IDS) for WLAN. The purpose of the RF monitor is to collect communication traffic so that notable events can be seen in real-time. If the RF monitor is to be used as an IDS, it should be able to recognize known network attacks such as man-in-the-middle, denial of service, and port scanning. Attack signatures need to be made available to the RF monitor, and should be updated frequently. RF monitoring can be done on a continuous basis.

- **IDS Use:** An intrusion detection system can be installed to monitor the activities on wireless segments, and report suspicious activities to network administrators. Isolation of networks must be practiced to protect interior networks and devices and to protect information.

- **File Sharing:** File and directory sharing should be turned off unless required. Users should be granted privileges only to the network data that they are authorized to view or alter.

7. STORAGE OF DATA

A Networked Attached Storage capability has been configured for the probation office. All of the current probation office data is located on a Dell PowerEdge server located in each divisional

office, running the MS Windows 2003 operating system. Each user has access to a personal directory located on the Microsoft Windows 2003 server. Only business related data files must be stored on the user assigned network drives. Personal pictures, music and video files are prohibited from being stored on network drives.

The N: drive is used to save user's private folders and files. The O: drive is used for sharing all probation office documents. The Q:drive is used to share temporary work and should not be a repository for users to store all of their data. The L: drive is used to store user's Lotus Notes files.

Data on the network drives are backed up every night and saved on a local device as well as an offsite location. Data can be restored by the IT Unit upon user request.

8. INTERNET ACCESS

The Internet is an unsecured network. Information and e-mail on the Internet can be read, broadcasted, or published without the knowledge or consent of the author. Most sites maintain records of all users or entities accessing their resources. These records may be open to inspection and publication without the user's knowledge or consent. If the activity of the user is other than official business, the publication of that activity could prove to be an embarrassment for the Court and the entire Federal Judiciary.

The Internet service is primarily used to access popular Internet applications and to connect to federal/state government agencies, private companies, public organizations, and educational institutions for official business use only. Users have open access to the .org,.gov, and. edu. domains. According to US Government guidelines, Internet research should be limited to business uses. Guidelines do allow some personal use of the internet, as long as it is not conducted during normal working hours. Personal use is also limited and the restrictions on Internet sites are enforced.

The probation office may monitor any Internet activity occurring on government equipment or accounts. We currently employ filtering software to limit access to sites on the Internet. If the probation office discovers activities which do not comply with applicable law or departmental policy, records retrieved may be used to document the wrongful content in accordance with due process. Management reserves the right to change which web sites are blocked as it deems necessary.

8.1 Appropriate Use of Internet Service

Individuals are encouraged to use the Internet to further the goals and objectives of the probation office. The types of activities that are encouraged include:

- Communicating with fellow employees, agency partners, and clients within the context of an individual's assigned responsibilities;
- Acquiring or sharing information necessary or related to the performance of an individual's assigned responsibilities; and
- Participating in educational or professional development activities.

8.2 Inappropriate Use

Individual Internet use will not interfere with others' productive use of Internet resources. Users will not violate the network policies of any network accessed through their account. Internet use will comply with all Federal and State laws, and all Judiciary policies. This includes, but is not limited to, the following:

- The Internet may not be used for illegal or unlawful purposes, including, but not limited to, copyright infringement, obscenity, libel, slander, fraud, defamation, plagiarism, harassment, intimidation, forgery, impersonation, illegal gambling, soliciting for illegal pyramid schemes, and computer tampering (e.g. spreading computer viruses).

- The Internet may not be used in any way that violates Judiciary or local probation office policies, rules, or administrative orders. Use of the Internet in a manner that is not consistent with the mission of the probation office, misrepresents the probation office, or violates any policy is prohibited.

- Individuals should limit their personal use of the Internet. The probation office allows limited personal use for communication with family and friends, independent learning, and public service. The probation office prohibits use for mass unsolicited mailings, access for non-employees to probation office resources or network facilities, uploading and downloading of files for personal use, access to pornographic sites, gaming, competitive commercial activity unless pre-approved, and the dissemination of chain letters.

- Individuals may not establish government computers as participants in any peer-to-peer network.

- Individuals may not view, copy, alter, or destroy data, software, documentation, or data communications belonging to the probation office or another individual without authorized permission.

- In the interest of maintaining network performance, users should not send unreasonably large electronic mail attachments or video files not needed for business purposes.

- Usage of streaming radio and video for a period exceeding 5 minutes is prohibited. Videos and training being streamed from within the Judiciary such as J-Net - are exempt from this rule.

8.3 File Transfer

Employees can transfer files from remote Websites for official business use only. If the file is to be used in conjunction to network applications or enhancement to documents, the file should be scanned with Norton Anti-Virus that is provided on all probation office assigned systems.

8.4 Posting a Web Page

Posting or creating a personal Web page to Internet service is strictly prohibited.

8.5 Social Networking Web Sites

Social networking web sites have become increasingly popular and include such sites as MySpace, Facebook, Twitter, LinkedIn, and many blogging web sites. Due to the potential of inappropriate material being posted on these web sites, access to these sites is prohibited and blocked by the web filtering software. However, limited access may be granted by the chief probation officer or deputy chief probation officers for investigative purposes.

9. INTRANET ACCESS

The probation office maintains an Intranet for sharing local information to employees. It also includes helpful links to other Judiciary sites, as well as areas that certain employees may maintain and keep up-to-date with current events. The Intranet may be accessed here: USPO-CT Intranet.

Information concerning the Intranet page is outlined below:

- Use of Intranet Server: The Intranet server is a webserver primarily used to deliver and share information to all staff. The Intranet is accessed via a web browser and is currently set as the homepage for all probation office CT users.

- Access to Intranet Server: Access to the Intranet server is exclusively provided within the office through all computers connected to the network. Remote access to the Intranet server from computer equipment purchased by the office is also possible through the use of the VPN software or J-Port.

- Access to Intranet Server via Wireless Access Points (AP): Access to the intranet is available using the AP located in each office. Staff can connect to these points by selecting the proper access point and entering their VPN user name and password to gain access. Reference Wireless LAN Better Practices for information on the configuration of the wireless network.

- Use of a Web Browser: The IT Unit primarily supports the Microsoft Internet Explorer(IE) web browser for accessing the Intranet server from local and remote computers. Default software configuration is maintained by IT to provide an efficient and secure connection to the host server. Upon opening IE, the user is directed to the HTTP address http://www.ctp.circ2.dcn.

- Posting a Web Page: The Web server administrator is responsible for posting the HTML documents to the Intranet server. The Web server administrator allocates disk space on the Intranet server to designate file locations that represent distinct subject and group discussions. For example, Document Library, Supervision, and Personnel have specific disk locations to post any topic of discussion for all employees. In addition, employees have access and ability to create, edit and post documents to the Intranet server.

- Access to Information: Information such as office manuals, software instructions, and other documents are posted on the Intranet server. Employees will be notified via e-mail or blog posting of pertinent web addresses of specific subjects, such as PACTS-ECM, Policy Manual, Human Resources, Training, etc.

10. USE OF PERSONAL SOFTWARE ON GOVERNMENT MACHINES

Our office adopts the policies and procedures outlined in the IRM BULLETIN 94-17 with one notable exception. No employee, under any circumstance, shall request to add their personal software to machines used in the office. If there is a software package that an employee uses on their personal PC they may request that the office purchase a copy for their use. Each request will be individually considered and a decision made in accordance with Section 3.2 – Configuration of Workstation. If the software is purchased the employee may bring their data files from their personal PC and copy them to their work PC, after scanning for viruses.

To ensure that no unlicensed or personal software is loaded on our machines the IT Unit, via network management software, will periodically scan all of the office's PC hard drives. We will only target software programs and no data files will be considered. Any unauthorized software will be deleted upon detection. The user will be notified in writing of what software was eliminated. Continually installing unauthorized software will result in disciplinary actions by the chief probation officer.

The same policy and procedures apply as indicated in the Section 4: - Laptop Computers for Home Program. The IT Unit does not support or is responsible for troubleshooting personal software on the home computer.

11. REMOTE ACCESS TO NETWORK

Remote access to Judiciary resources (or DCN) is provided by the Office of Information Technology Infrastructure Management Division(OIT-IMD) by utilizing the VPN, JPort or J-RAN.

11.1 Virtual Private Network (VPN)

Using a VPN connection is one method by which users can connect to the DCN from a remote location. VPN technology establishes a secure, encrypted tunnel between the remote PC and the DCN as the communication path traverses the Internet. VPN technology is typically used with fast broadband (wireless broadband, cable modem or DSL) connections to the Internet. A Cisco VPN Client is available for distribution to all judiciary VPN users which includes IPsec and an embedded firewall. The VPN software is allowed for use on government supplied equipment, such as laptops or home use computers.

Real-Time analysis and monitoring services are performed by the AO's Security Operation Center (SOC), which is staffed by a combination of security consultants and federal court employees. All network traffic is identified, depending on the level of criticality, the SOC will:

1. Create a ticket and assign it out to the Director of Information Technology and the Assistant Systems Manager;
2. If the threat is critical, the SOC places a phone call to one or both of above identified employees.

Based on the Guide to Judiciary Policy, Vol. 15 Ch. 3, Section 310.10.20: Importance of Security, the Probation IT Staff will respond to SOC alert notifications for suspect traffic on the VPN by:

1. Disabling the identified user's VPN account;
2. Requiring the user to change their VPN Password;
3. Alerting the user through email of the above actions.

11.2 JPort

Uses secure socket layer (SSL) technology to set up an encrypted virtual private network (VPN) connection without the need for an installed remote client on the computing device in use, and it removes any locally stored (cached) data from the computer at the end of each session. JPort is implemented on SSL VPN servers installed at both of the DCN gateways and is licensed to handle one thousand simultaneous user connections. As always, users should use trusted and secure PCs whenever possible for remote access. The JPort home page is tailored by the local IT staff for the probation office, to reflect local court access requirements. Local IT administrators can add, change, or delete menu items as needed to support our needs and to comply with local policies. JPort access is allowed on any government assigned equipment, as well as the employee's personal computers.

Further information on the use of JPort, including a basic user guide and pocket reference guide can be obtained by visiting the following link on J-Net.

JPort User Guide

11.3 Judiciary Web Mail

The Judiciary Web Mail formerly known as J-RAN allows judiciary staff access to their Lotus Notes e-mail from any computer with Internet access and a compatible browser. To access Lotus Notes e-mail visit the web page https://webmail.uscourts.gov/

11.4 Authorized Users

Only users who have requested and received approval are authorized to use the VPN service and JPort. Those services are not to be used for any activities other than official government business.

11.5 Position Status

Because of security issues, access will be limited to permanent employees. Non-court employees, such as contractors or consultants, will not normally be granted remote access privileges. Government contract employees who perform work in place of agovernment employee may be given VPN or RAS access, if warranted by their job duties and responsibilities. If a temporary employee is granted access, then an expiration date will be established before the user account is activated.

11.6 Security Responsibility

If the employee wishes to use JPort, VPN or Judiciary Web Mail on their home computer, they agree to maintain up-to-date versions of court approved anti-virus software and use a firewall product with their home or portable computer. Maintenance related to security should be performed by the user with instruction from the IT staff, or, when appropriate, performed by the IT staff directly. Security maintenance might include the installation and continued updates of secure client software, anti-virus software, or firewall products. For additional information about security guidelines please see the Network and Computer Security chapter of this document.

If the employee uses a privately owned personal computer, as opposed to a court provided computer, passwords must not be saved or stored for automatic processing. Storing plain passwords on any computer is not recommended as good security practice. Unauthorized use, or use that exceeds the level of authorized access, is a violation of federal law.

11.7 Appropriate Use

Because remote access is provided for work-related use, users are required to follow all policies, contained in this chapter, outlining appropriate use of the Internet, e-mail and government resources.

11.8 Separation or Termination of Employee

Remote access will be terminated immediately in the event of separation from the Court, for whatever reason.

12. USE OF THE OFFICE E-MAIL SYSTEM

12.1 Users of the Lotus Notes E-mail

The electronic mail service is provided for business use only. As the messaging service has become a vital communication mechanism for conducting office business, and an increasingly more frequent, direct linkage with the Court, employees should access and respond to messages while on duty. For security reasons, employees should not leave their email account open when away from their workstation.

All probation office employees are provided access to the email Server. All users of the email system must conduct themselves in a professional manner and will refrain from using profanity and/or obscenities in any electronic communications. The email system is not a forum for soliciting goods and services not directly related to official business. However, certain bulletin boards are available for posting courthouse-related messages.

Users are reminded that e-mail is for official correspondence and each unit's local policies and practices for other written communications applies. Keep in mind at all times that an email is easily copied or forwarded to anyone without the sender's knowledge. So, ensure that all email correspondence will pass the "newspaper test", meaning that the correspondence, if made public, will not hurt judiciary employees or embarrass the judiciary in any way.

Users are expected to follow the email policy when sending messages to individuals not located within the probation office. Incoming messages which violate the email policy should be reported to your supervisor.

12.2 Files Attached to EMail

Any file from an outside source (i.e. AO, Internet, another court) which is attached to an e-mail message is automatically scanned for viruses at the Gateway Mail Server before being delivered to the probation office network.

12.3 Spam Sentinel

Spam Sentinel is a Domino-server-based protection solution that prevents Spam from being delivered to a user's mail file. Verification is based on a subscription service that collects, inspects, and reports known Spam. Spam Sentinel works by comparing all of the mail messages from the Internet against a real-time list of known Spam. Messages identified as Spam are moved to a quarantine database. Unlike Symantec content filtering, the number of false positives for Spam Sentinel is very low. A message must be sent to thousands of external e-mail addresses, and blocked by many members of SpamNet (a network community of SpamSentinel users) before it will be added to the SpamSentinel database as Spam.

In addition to the list of 100 million plus known Spam signatures in the SpamSentinel database, courts can also use a Blacklist to prevent a single e-mail address or an entire domain from sending mail to their users. On the other hand, courts (and even end users) can use a Whitelist to allow an entire domain or a single e-mail address to send messages to their court even though SpamSentinel quarantines them.

A daily report is automatically generated and mailed to each user who received Spam messages in the previous 24 hours (72 hours on Monday morning) so they can review quarantined Spam mail without assistance from the Court Unit Administrator. This report contains the message date, subject, sender name, and a synopsis of the message body without any offensive pictures.

If a message on the report appears to be okay, the user can click the included doclink to view the entire message content from the quarantine database. After viewing a quarantined message, users can forward the message, release the message from the quarantine back to their own Inbox, or add the sender or domain to their own personal Whitelist.

All messages in the quarantine database are secured, so users can see only their own messages or those they are privileged to see through delegation or shared mail file access.

12.4 Privacy and Disclosure

The e-mail system is office equipment and anything contained therein is office property. The confidentiality of e-mail messages shall normally be protected. However, if any in appropriate behavior and e-mail contents are suspected, the probation office may direct the director of information technology to provide him/her with the contents of the suspected e-mail.

12.5 Responsibility

12.5.1 Information Technology (IT) Unit

The IT Unit is responsible for managing the probation office Lotus Notes E-mail Database. Local Court Administrators maintain access control. The Local Court Administrators are responsible for creating Domino Directory entries for their particular users and groups, renaming and terminating users. The role of the Local Court Administrators is as follows:

1) Provide user access - Users are provided a user login name (First and Last Name) to access the probation office e-mail.

2) Creating Groups & Mail Lists - The e-mail administrator is responsible for creating Groups and Mail Lists which is intended for use by office staff or designated members of the Group. The same applies to Mail Lists. Users may create Mail Lists for their own intended purposes, and do not require administrator involvement, unless requested.

3) Client Software Installation - Software installations include the desktop client for LAN access or on the laptop which is used for “mobile” (remote) access.

4) Troubleshooting - The IT Unit E-mail administrator or the unit Help Desk is responsible for troubleshooting all e-mail related problems. The IT Unit Help Desk can also be used to “unlock” e-mail accounts or provide temporary passwords to users who are locked out due to expired e-mail accounts. The user is responsible for changing these “temporary” passwords immediately to ensure the password is not known by others. To assist the email administrator, users should provide IT with any error messages that appear on the monitor when problems arise.

5) Training - The IT Unit will provide necessary email training which is not handled by the probation office training staff. Training is provided to telecommuters and users of office laptop computers.

12.5.2 User Responsibility

1) Password Security - It is the user’s responsibility to protect his/her email password. Passwords should not be shared with others. EXCEPTION: Users may provide the password to the e-mail administrator for troubleshooting purposes or during initial/re-installation(s) of the e-mail application. A person who gains access to users’ email account will be able to read all of their email, and may send messages to others in their name.

2) Screen Security – Users should ensure that their computers are logged off before they leave, or protected by screen saver software that requires a password to reactivate to ensure that their email will not be available to unauthorized users in their absence. By default the Windows Screen Saver will be activated by Domain Group Policy after 10 minutes of inactivity.

3) Email Maintenance - Users are encouraged to review email messages within one (1) hour after reporting for work, and frequently during the remainder of the business day, no less than three additional times throughout the day. If you are out of the office for an extended period of time, please use the "Out of Office" agent.

13. MAINTENANCE OF THE NETWORK/DISASTER RECOVERY PLAN

Currently, the probation office uses a back-up company, Barracuda Networks., to store daily, monthly and yearly network back-up files offsite. The office also employs an on-site barracuda backup appliance for daily backups

14. TELECOMMUNICATIONS

14.1 National IPT System

The Administrative Office of the US Courts (AO) has contracted for a National Internet Protocol Telephony (IPT) system to provide telephony service to court sites throughout the US. The National IPT service is a managed service provided by AT&T under the umbrella of the AO sponsored and managed Networx contract. This centralized, managed IPT service offers a cost effective and efficient path for courts to replace their legacy PBX systems or Centrex services with state-of-the market Voice of Internet Protocol (VoIP) technology. The District of Connecticut has converted to the National IPT system in 2012.

14.2 Court Telephone Coordinator

Unit Executives are designated to be Court Telephone Coordinators for their judiciary offices. The Unit Executive may designate other court officials and personnel to perform the various telecommunications duties required, but he/she remains ultimately responsible for full compliance with these guidelines.

14.2.1 Duties of the Court Telephone Coordinator

- Manage the telecommunication system (equipment, lines, and services) at the court to include liaison with equipment vendors, maintenance personnel, and all other providers of telecommunications lines and services;
- Request for additional telecommunications equipment and lines in accordance with these regulations are made through the Unified Communications group;

- Manage all requests for follow-up services such as moves or rearrangements to the telecommunications system;
- Ensure all services maintenance procedures, as identified in this chapter, are appropriately followed;
- Track and maintain an inventory of all telecommunications services, equipment, and lines;
- Oversee the renewal of telecommunications leases and contracts for service maintenance and/or follow-on services;
- Certify that all telecommunications bills are correct before payment is rendered;
- Develop and execute a court telecommunications training plan to ensure effective utilization of installed telecommunications systems;
- Be familiar with the type and cost of telecommunications equipment and lines available to the court. Assist in the preparation and projection of funding for related telecommunications Budget Object Codes; and
- Develop and manage a continuity of operations plan for the court in the event of a major telecommunications systems failure.

14.3 Telephone Usage Guidelines

No long distance personal calls may be placed through the probation office telephone system using the telephone system or a long distance telephone company, who will bill the office, unless for a reason stated above, as these are considered to be deemed official business.

Any employee who attempts to make unauthorized long distance calls over the telephone system using a long distance carrier will be liable for any expenses accrued by the Government.

Any employee who attempts to make unauthorized calls using the telephone system will be in violation of office policy for the probation office and is subject to any disciplinary actions deemed appropriate by the chief probation officer.

Advanced features of the phone system (i.e. Call Forwarding and Do Not Disturb), are available to assist employees but they should not be used to reduce contact with callers screen/avoid calls.

14.4 Personal Calls

In general, the use of a government telephone is allowed as follows:

1) A brief daily call to speak to a spouse, minor child, or day care center to check on their well-being;
2) Brief calls that can be made only during working hours such as to a local government agency or physician;

3) Brief calls to arrange for emergency repairs to his/her residence or automobile.
4) A brief call to family regarding a delay in returning home from government business travel.

Regardless of the reason, all personal calls on government telephones must meet the following criteria.

1) The calls do not adversely affect the performance of the employee.
2) The calls are of reasonable duration and frequency.
3) The calls reasonably could not be made at another time.

14.5 Assignment of Telephone Numbers

All probation officers and administrative staff will be issued a telephone number. Every attempt will be made to have this number stay with the individual in the event of a physical office move.

All employees will have a voice mail box assigned which will correspond to the format 9xxxxxxxxx, where the x's are their full 10 digit phone number. Employees should refer to the voice mail section of this manual for special policies and procedures relating to the use of voice mail.

The IT Unit is responsible for updating all telephone directories. To ensure that the most accurate listing is distributed to the staff, the following procedures will occur when telephone changes are made.

The Telecommunications Coordinator in conjunction with the Unified Communications group will make changes to the telephone and voice mail system as needed.

The IT Unit will modify the directory and distribute as necessary and post the updated directory to intranet site.

14.6 Voice Mail

14.6.1 Password Security

The user is responsible for ensuring that the voice mail system is secure by having a voice mail box password of at least 4 digits. Trivial passwords are not allowed, trivial passwords are defined as:

- Consisting entirely of repeated numbers, such as 4444;
- Containing at least one group of repeated numbers, such as 1117;
- Containing consecutive ascending numbers, such as 1234;
- Containing consecutive descending numbers, such as 8765;

- Matching your primary extension

Voicemail PINs expire after 90 days, users will receive a warning before the expiration date.

Users must protect the voice mail system against hackers by not giving their password to anyone other than their supervisor or the Director of Information Technology.

14.6.2 Voice Mail Retrieval

All voicemails are saved on the centrally located voicemail servers at the data centers hosting the voicemail system. Voicemails should be retrieved every day and deleted once they have been listened to. If voicemails are not deleted in a timely matter the mailbox can fill up which prevents the caller from leaving a message.

Messages may be retrieved in one of the following manners:

- Press the voicemail button on the Cisco desktop phone, it looks like the envelope.
- All voicemails are routed to the email inbox of the recipient for playback, deleting the email message DOES NOT delete the message from the voice mailbox
- From any phone not on the IPT system, dial 1.855.621.7919, the system will prompt for a user ID. The caller's ID is 9 followed by the caller's full 10 digit work number followed by the # sign.
- On the internet at https://vmail-a.ipt.srvc.dcn:8443/ciscopca/home.do, login using Jenie username and password.

Please read the Voice Mail Basics guide for additional information.

14.6.3 Special Voice Mailboxes

The probation office has developed a few special mailboxes to better serve the public. Creation of special voice mailboxes is available by special request to the Director of Information Technology.

The voice mailbox number 92037732100 is the main office mailbox that is only in effect in the evenings or district office closings. Individuals calling our main number, who do not know where to leave a message, can do so there. Front Office staff is responsible for checking that voice mailbox every morning and distributing the messages to the appropriate parties.

14.6.4 Maintenance

It is the responsibility of the Unified Communications group and staff to maintain a secure voice mail system. No guest or unassigned accounts will be created on the system. In addition, the default voice mail box password will be a random five digit number.

14.6.5 Employee Use

Voice mail greetings are to be updated on a daily basis. All greetings should include the following:

1) In Office: You have reached probation officer (name). Today is (date) and I will be in the office until (time). I am unable to answer your call at this time as I am on another line or away from my desk. Please leave a brief message at the tone. If immediate assistance is needed, please dial "0."

2) In Field: You have reached probation officer (name). Today is (date) and I will be in the field for the day. Please leave a message at the tone as I will be checking my messages periodically. If immediate assistance is needed, please dial "0."

3) Telephone Incident Reporting: If a threatening phone call or voice mail is received, the Call Detail Records may be used to identify the origin of the caller. Any information gathered will be submitted to the investigating law enforcement agency.

While a telephone number alone is not a record within the meaning of the Privacy Act, when linked with a name it does fall under the Act. To comply with the Privacy Act of 1974 the probation office can obtain call records from the previous 30 days with the following restrictions:

- relating to the identification of individual employees
- linking them with specific calling numbers;
- linking them with specific called numbers

14.7 Billing

The chief probation officer for the District of Connecticut has delegated the certification of telephone billing to the Budget Analyst. Each month, the probation office receives the following telephone bills.

- WITS 2001 bill for telephone lines, including long distance calls
- Verizon Wireless invoice for all wireless phones

- Verizon broadband invoice for broadband wireless internet provided to officers for their laptops

In addition, the office may receive bills, from several different vendors for telephone equipment, line changes, or service calls.

The budget analyst reviews all telephone bills to insure accurate billing. Items reviewed may include: number of message units, number of telephone lines, service, duration and time of calls. The analyst will also verify all service charges with the director of Information Technology. After verification, the director will forward the bill back to the analyst. The analyst may choose to investigate any calls that he/she feels are suspicious in nature. After the analyst certifies the telephone bill, it is forwarded to the financial manager for procurement specialist for payment.

15. iPHONE POLICY

15.1 User Policy

iPhones are accountable property of the probation office and must be treated, used, and safeguarded as such. Users will be required to sign an Acknowledgment Receipt upon receipt of the iPhone, (see Acknowledgment Receipt/Return of Automation Equipment for a sample).

If an iPhone is lost, damaged, or stolen, a memo must be sent to the user's immediate supervisor within 24 hours with a cc: to the IT Unit and notice given to the appropriate law enforcement authorities. Once notified, the IT Unit has the capability of wiping out the data on the iPhone via remote control and will initiate such action as necessary.

iPhones must be used appropriately, responsibly, and ethically. In accordance with the Judicial Code of Conduct, the devices are not to be used for the purpose of illegal transactions, harassment, or obscene behavior. Billing records are audited.

- Users must be accessible and responsive.
- Users must remain within the allocated minutes/dollars covered in the monthly service plan. Users who exceed the allocated minutes/dollars will be required to provide justification, may have to pay for overage, may lose cell phone privileges, and/or receive disciplinary actions.
- Whenever possible, the user must use the iPhone to call other iPhone users (in-network calling).
- Users must dial 800-FREE-411 (800-373-3411) for directory assistance to avoid additional costs.
- Personal use of the iPhone is allowed, but should be kept to a modest level.

- Hands-free devices must be used while operating any motorized vehicle during the course of official agency business.
- Misuse or abuse of the iPhone, as outlined above, could result in deactivation and/or disciplinary action, which may be reported in the user's performance appraisal.
- The same internet policy stated in Section I - Internet Access applies to the iPhone device as well.

IT will not support any 3rd party application that is not approved by the Director of Information Technology. Should the iPhone have any reported problems, any non- approved 3rd party applications will be removed as part of the troubleshooting process. This includes any data that was associated with the 3rd party application. IT will not be responsible for any installation of non-approved applications for the iPhone.

15.2 Monthly iPhone Bill Distribution

This document outlines how the monthly IPhone bill will be distributed to all staff for verification that the charges for the phones are valid. Each person who has a IPhone will be held accountable for reviewing their bills to verify accuracy and for identifying charges above the allowed usage limits of the cell phone policy. The steps for verification are outlined below:

The assigned data quality analyst will sort the bill by supervisory probation officer and deliver to each supervisory probation officer their unit's bills for the month.

The supervisory probation officer will distribute all bills to be reviewed and signed off on by the iPhone user.

The supervisory probation officer will collect and deliver all signed bills to the assigned data quality analyst

The data quality analyst will reassemble the bill and deliver it to the and report to the director of information technology any inconsistencies.

The supervisory probation officer has seven (7) business days from receipt of bill to return to the assigned data quality analyst.

15.3 Security

Users are responsible for damage to and/or loss or theft of loaned iPhone devices. In order to avoid loss or theft of property or data, please follow these guidelines:

Airports: Never leave the IPhone unattended. Do not check the IPhone as baggage. Exercise diligence in watching the IPhone as it is passed through any x-ray devices.

Cars: Avoid leaving the IPhone in the car. However, if circumstances require it, keep the car locked and stow the IPhone away from exterior windows, out of view to avoid a smash-and-grab scenario. Ensure that the IPhone is securely stored so that it does not slide while driving. Avoid storage of the IPhone in a car during very hot or very cold weather.

Hotels/Conferences: Never leave an iPhone unsecured in a hotel or conference room.

Data Security: The iPhone will be configured to require a password prior to use. The phone will automatically lock after 10 minutes of inactivity.

If the IPhone is lost, damaged, or stolen, a memo must be sent to the user's immediate supervisor within 24 hours with a cc to the IT Unit and notice given to the appropriate law enforcement authorities. Once notified, the IT Unit has the capability of wiping out the data on the IPhone via remote and will initiate such action as necessary.

If an IPhone is lost, damaged, or stolen, a Board of Survey will be convened.

If an iPhone screen becomes accidentally broken (i.e. iPhone is dropped) the user should still send a memo to their immediate supervisor within 24 hours with a cc to the IT Unit. The user should make arrangements with the IT unit to drop off the iPhone at the New Haven office so that the IT unit can have the screen fixed at the nearest Apple authorized dealer. There will be no need for a Board of Survey.

15.4 Government Cell Phone Overage Review

All iPhone users are expected to stay within the allotted minutes and/or cost parameters of their cell phone plan.

Any overages on a user's phone bill for either minutes or cost will be subject to review to determine the reason(s) for such overages.

Overages of either minutes/cost not approved by the deputy chief probation officer may result in disciplinary action, to include, but not limited to: suspension of cell phone privileges for a length of time at the discretion of the deputy chief probation officer; revocation of the privilege to use a government cell phone; and/or repayment of any monetary overages. Any disciplinary action may be reported in the user's performance appraisal.

The cell phone user is responsible for notifying his/her immediate supervisor if there are overages of either minutes/cost after review of his/her phone bill. This notification must take place within seven (7) working days of receipt of the user's phone bill.

The immediate supervisor will have no more than three (3) working days to present his finding on overages to the deputy chief probation officer.

This does not preclude an independent evaluation of any cell phone bill as directed by the deputy chief probation officer.

The chief probation officer has delegated authority for enforcement of this policy section to the deputy chief probation officer.

15.4.1 Notification by User of Overages:

Upon receipt of their government cell phone bill, the user will review the bill to determine if either the cell phone minutes/cost exceeds the limit. If not, the user will process the bill in accordance with the relevant section(s) of this chapter.

If there is an overage, the user will complete the 'Overage Explanation Form'(OEF) (see Appendix IT-B) and submit to their immediate supervisor with a copy of their bill attached. The user will keep a copy of both for their records.

15.4.2 Supervisor Actions upon Receipt of Overage Explanation Form:

1) The immediate supervisor will note his/her receipt date on the OEF.
2) The immediate supervisor will review both the user's overage explanation and attached phone bill to determine whether there is justification for the overage(s).
3) The immediate supervisor will then document his/her findings, with a recommendation, on the OEF and submits a memo the deputy chief probation officer within three (3) working days after receipt.
4) The immediate supervisor will keep a copy of all material submitted to the deputy chief probation officer.

15.4.3 Deputy Chief Probation Officer Actions upon Receipt of the Overage Explanation Form:

1) The deputy chief probation officer will note his/her receipt date on the OEF.
2) The deputy chief probation officer will review the OEF form submitted by the immediate supervisor and make his/her own determination as to whether any overages are justified or not and state same on the OEF within three (3) days of receipt of the OEF.
3) If the overage is not justified, the deputy chief probation officer will use the OEF as the means of informing the user of the decision/sanction. The deputy chief probation officer may discuss the decision/sanction with the user.
4) There will be no appeal of the deputy chief probation officer's decision unless there is new and compelling evidence presented by the user within 30 days of the deputy chief probation officer's decision.

15.4.4 Final Processing of the Overage Explanation Form:

1) The deputy chief probation officer will provide a copy of his/her OEF decision to the user, immediate supervisor, and procurement specialist.
2) The procurement specialist will place his/her copy of the OEF with the appropriate phone bill in the procurement folder.

15.4.5 Overage Payment:

1) Checks should be made payable to the U.S. District Court and should be given to the financial manager.

16. NATIONAL PACTS REPORTING (NPR) EXTRACTION

Our office complies with the directives from the AO to submit the data requested. This data is important to provide funding for our office.

The DQA shall supervise and direct the monthly PACTS NPR extraction for statistical reporting. This shall be completed on or before the 20th day of each month. Prior to submitting the extraction report, the DQA shall ensure all errors in the PACTS extraction error report are corrected by a probation officer or supervisory probation officer prior to the extraction. Some errors may require the assistance of the IT director to resolve.

17. PACTS DATA QUALITY

PACTS is the primary office database and is used to ensure accurate case tracking and provide the required statistical data for decentralized funding and staffing formulas. To maintain a dynamic and statistically accurate database, the director of IT and a deputy chief probation officer shall serve as the PACTS administrators. The IT director manages all technical components of PACTS and the DQA manages the front end components and works with non IT staff to implement strategies for correct and effective use of PACTS. These administrators must collaborate to ensure the probation office has timely and accurate information at all times.

Each employee is provided access to PACTS and trained on all aspects of PACTS including PACTS forms, database access, and reports. The PACTS administrators determine the level of access depending on the needs and role of the user. The rights to delete entire records in PACTS is solely held by the IT director and a designated employee of the IT unit, but before any record may be deleted the chief probation officer or deputy chief probation officer must provide an agreement in writing (e-mail) to the IT director.

18. ATLAS

ATLAS (Access To Law enforcement Systems) is a web-based application developed by the Administrative Office of the U.S. Courts (AOUSC) that allows users to retrieve criminal justice and law enforcement information from the National Crime Information Center (NCIC) and

National Law Enforcement Telecommunications System (NLETS) via their desktop computers through the Data Communications Network (DCN). Accessing NCIC and NLETS through this network connection provides a more efficient and effective service, at each user's desktop, and for less cost.

The purpose of these regulations is to assure that criminal history record information where ever it appears is collected, stored, and disseminated in a manner to ensure the accuracy, completeness, currency, integrity, and security of such information and to protect individual privacy.

18.1 General Information

Court Unit Executive: The chief probation officer must sign an ATLAS Court Unit Executive Agreement provided by the AOUSC. Once signed, the AOUSC provides the probation office with an Originating Agency Identifier (ORI).

For questions relating to probation office ORIs, contact the office Terminal Agency Coordinator (TAC). Otherwise, contact the following:

FBI CJIS Division PDS IOAG NCIC ORI Staff
304-625-3598 - Phone 304-625-3393 - Fax

For questions relating to FLASH notices, contact the following:

FBI CJIS Division NCIC FLASH Unit

Terminal Agency Coordinator: The chief probation officer appoints one Terminal Agency Coordinator (TAC). The TAC is required to sign the TAC Agreement provided by the AOUSC. All new TACs must be trained by a certified ATLAS trainer. The TAC will create and certify accounts for each user.

The TAC shall be certified and successfully pass the ATLAS examination. The TAC is responsible for ensuring compliance with ATLAS policies and procedures. The TAC serves as the liaison between the chief probation officer and the AOUSC in matters involving NCIC, NLETS, and ATLAS.

New or replacement TACs are required to receive training regarding their roles and responsibilities. Training will be administered by a TAC who is certified by the AOUSC to train new TACs. The training can occur in person or by telephone. Any travel and lodging expenses incurred during a new or replacement TAC's training are borne by the probation office.

Alternate Terminal Agency Coordinator: The alternate TAC is designated by the chief probation officer. There may be more than one alternate TAC. Alternate TACs can be trained by a certified TAC. Each Alternate TAC must sign an Alternate TAC agreement provided by the AOUSC.

In the absence of the TAC, the Alternate TAC will fulfill the roles and responsibilities of the TAC.

Local Agency Instructor: The Local Agency Instructor (LAI) is designated by the chief probation officer. The LAI may also be the TAC or Alternate TAC. There may be more than one LAI. Each LAI is required to sign the LAI agreement provided by the AOUSC. The LAI is responsible for training, testing, and certifying each new user and recertifying each user under the direction of the TAC. In the District of Columbia, every TAC or Alternate TAC is also an LAI.

18.2 Security Requirements

18.2.1 Fingerprint-based Record Check

Before any user (including support personnel and computer-support personnel, i.e., IT Unit employees) can have an account or access ATLAS, they must have:

- their identities positively confirmed by a national fingerprint comparison;
- passed criminal history checks; and,
- be authorized by the probation office to access ATLAS in the course of their duties.

Any person having a felony conviction will not be granted access under any circumstances. Any person having a misdemeanor conviction may only be granted access by the AOUSC Control Terminal Officer or Control Security Officer (CTO/CSO).

Permission may not be granted at a district level.

18.2.2 Physical Security

The computer sites must have adequate physical security to protect against any viewing or access to computer terminals, access devices, or stored/printed data at all times. This includes all notebook or portable computers, including hand held devices or PDAs.

The AOUSC requires that all computers that access ATLAS have a password protected screen saver that activates after 7-10 minutes of inactivity. Users must lock their computers from access whenever they are away from their computers. The lock must be deactivated with a password.

18.2.3 Systems Staff Security Information

All system staff accessing ATLAS must undergo a national fingerprint comparison records check to comply with FBI requirements.

The systems staff will help the TAC with the following:

- Ensure all computers used to access ATLAS meet the ATLAS computer security requirements listed in the CJIS Security Policy Manual;
- Assist the TAC to determine if a problem with ATLAS is with the user computer, the local area network, the DCN, or the ATLAS server; and
- Assist the TAC to physically isolate and secure any computer equipment that was used to access ATLAS inappropriately or without authorization.

18.3 Compliance Audits

By the AOUSC: The AOUSC will conduct a compliance audit of the probation office every three years. The purpose of the audit is to evaluate the probation office's compliance with NCIC regulations. As part of the audit, the probation office will be responsible for completing a mail-in (or e-mail) audit questionnaire. This questionnaire shall be completed by the chief probation officer or the TAC, if designated to do so by the chief probation officer. The AOUSC will assign a TAC from another district probation office to conduct the audit review. If an on-site audit review is required and initiated by the AOUSC, it could last up to five days depending on the number of users and locations of the probation office. Any travel and lodging expenses incurred by one or two auditors during the audit review will be borne by the probation office.

Additional information on this subject can be obtained from the ATLAS Terminal Agency Coordinator Guide, Section 2.13, Compliance Audit Coordination, Appendix B - Local Agency Audit, and Appendix C - Mail-in Audit Questionnaire.

By the TAC (in-house): Every inquiry made on the ATLAS system is recorded, logged, electronically stored, and maintained indefinitely for access, review and inquiry by the AOUSC or the TAC at any time for any reason. The purpose of this audit is to ensure compliance with NCIC regulations, including compliance with 28 CFR §§ 20.1 through 20.37.

The TAC may appoint alternate TACs (A-TACs) to help manage NCIC use by staff members. The A-TACs must also pass special certification before assuming this role.

In the District of Connecticut, the TAC or A-TACs will complete a monthly audit of 5 transactions per officer and maintain a log of the transactions audited.

18.4 Points of Access

Within Office via the DCN: Access to ATLAS is permitted within the probation office while connected to the DCN on an authorized computer that meets the requirements for access to ATLAS.

Remote Access to ATLAS: Many ATLAS users have indicated that they desire to use ATLAS outside of the office, particularly on mobile devices such as laptops that they bring on visits, home, etc. This policy addresses how ATLAS can (and cannot) be used outside the physically secure office environment.

Laptop Use: Currently, ATLAS users can use their government furnished laptops to access ATLAS under the following conditions:

- The government furnished laptop must connect to the DCN via an approved virtual private network (VPN). JPORT also serves this purpose.

- The laptop must have its entire hard drive encrypted or perform partitioning such that all the temporary data/files are getting stored on the encrypted part of the disk.

All ATLAS computer and physical security requirements must be followed.

NOTE: These conditions also apply to other mobile devices such as PDAs, Blackberries, and smart phones and also to government-owned, non-mobile computers in use outside of the office (such as at home).

Physical security is especially important and challenging to achieve. If the laptop is used in a vehicle while on government business, it must be secured out of sight and the vehicle locked. No one else should have access to the vehicle (e.g., another key). If the laptop is kept at home, it must be stored in a secure place (e.g., locked filing cabinet). When in use, the ATLAS user must ensure that uncleared personnel do not have the ability to view the screen. For example, use of films can help restrict viewing from the sides. The laptop should not be used to access ATLAS in a public environment where casual observers can possibly view the screen. The ATLAS user has to be with the laptop at all times when it is not secured.

Home Use: ATLAS is not to be accessed on home computers, even those with approved VPN connections. The actions stated in the conditions below are required for the ATLAS staff to carry out their responsibilities to protect FBI/States information and investigate security incidents. It is probably not possible nor appropriate for the ATLAS program to ask employees to agree to a condition similar to the one below as it pertains to their privately-owned equipment and as this would require at-home auditing. Because use of government-owned equipment does not prohibit these actions, the ATLAS program's only option is to limit the use of ATLAS to government-owned equipment.

Employee shall consent to and cooperate with unannounced examinations of any computer equipment owned or used by employee, including but not limited to retrieval and copying of all data from the computers, connected devices, storage media, and any internal or external peripherals, and may involve removal of such equipment for the purpose of conducting a more thorough inspection.

Laptops can be used at home provided they meet physical and computer security requirements. For example, use in a separate, locked room with a locked cabinet is permitted.

Frequency of User Checks: The TAC and alternate TAC will conduct random monthly checks of users to ensure compliance with NCIC and ATLAS policies and procedures.

At least monthly, the TAC and/or alternate TACs will review all transactions to ensure that PACTS numbers are associated with every inquiry. Once notified, the requestor for each inquiry without a PACTS numbers will have 30 calendar days to revise their inquiry and input a PACTS number. A user may enter an inquiry without a PACTS number if a PACTS number does not yet exist (e.g., a PSI referral and an inquiry is made the same or next day before a PACTS number is generated). For all "C" and "J" inquiries, the following codes must be entered in place of a PACTS number:

- Criminal Justice Employment Checks: 99991
- Security Program and Jury Checks: 99992
- Officer Firearm Background Checks: 99993
- FBI Firearm Instant Record Checks: 99994
- ATLAS Training Checks: 99995

18.5 Internal Restrictions

Supervision/Investigation: ATLAS-based inquiries in the probation office are limited to cases under the supervision or investigation of this office or the Federal Bureau of Prisons, in which this office has an interest for purposes of investigating a collateral investigation, pre-release plan, or pre-transfer plan. Under no circumstances, shall the ATLAS system be used for any other purpose.

NOTE: Adverse personnel action, up to and including termination from employment and/or criminal prosecution, may be taken against persons making unauthorized inquiries or having authorized access.

Prospective/Current Employees: Criminal record inquiries, including inquiries on drivers licenses and registration and automobile registration, using NCIC or NLETS through ATLAS, shall only be conducted using the purpose inquiry code "J."

These inquiries include background checks on support staff personnel or officers, and firearms compliance checks for domestic violence or criminal activity. Only a designated

employee is permitted to run "J" purpose code inquiries. The chief probation officer must designate, in writing, those employees authorized to run a "J" inquiry. The designation must be maintained on file by the TAC. Under no circumstances shall any other authorized user conduct a "J" purpose code inquiry in this office.

Adverse personnel action, up to and including termination from employment and/or criminal prosecution, may be taken against persons making unauthorized inquiries or having authorized access.

19. MANAGING SUPERVISED RELEASE FILES (SRFs) IN NCIC (ATLAS)

19.1.1 Entering Records in the SRF

All pretrial release cases under supervision, all post-sentence supervision cases and any juvenile case must be entered into the SRF. The supervisor can grant an exclusion to these cases, but it must be approved and documents in the PACTS chronological record. The officer assigned to the case is responsible for entering the SRF record. When cases transfer, inter-district, the newly assigned officer is responsible for entering the SRF record.

National policies do not allow pretrial diversion, witness security (WitSec) and pretrial release cases with no condition of supervision to be entered into the SRF.

19.1.2 SRF Data Entry

SRF records entered into NCIC must be kept accurate and up-to-date. The entering agency is responsible for the SRFs accuracy, timeliness and completeness. In this district, SRFs are to be entered, updated, modified, validated and canceled/cleared, by the assigned officer, as needed. Upon a transfer of supervision amongst officers, the SRFs should be modified by the officer receiving the case. (Districts are still required to submit Flash Notices on cases under post-sentence supervision, as the SRF does not include fingerprint identification.)

Data entered into the SRF should be entered in a timely fashion (ie: upon commencement of supervision) and shall be removed promptly once supervision has ended. Records shall include all identifiers and pertinent details, and shall be updated in the event information change.

The SRF shall contain the name and telephone number of the supervising officer. The telephone number may be a local number, or cell phone, on a case-by-case basis or as directed by the Supervising U.S. Probation Office (SUSPO).

19.1.3 SRF Validation

SRFs are to be validated 90 days after entry and on a yearly basis, thereafter. The validating officer is required to consult PACTS, as needed, during validation to ensure the information reflected in the SRF is up-to-date and remains accurate.

During the first week of the month, the TAC or assistant TAC sends an email out to all USPOs advising them that the new NCIC Validation List is available in ATLAS. The email further instructs the USPOs to check the list and complete any appropriate validations on their assigned cases prior to the end of the month. USPOs are then required to email the TAC upon completion of their validations. (In order to validate, USPOs compare the case data in pacts with that reflected in the SRF and make any modifications or clears that are needed.) The TAC rechecks the monthly validation list in Atlas during the last week of the month, to ensure that all validations have been completed.

In the event an SRF needs to be cleared (either because it was entered in error, or because the defendant/people under supervision's supervision has been revoked, or they have received an early termination) the USPO assigned submits an "XC/CC" query in ATLAS. Upon submission of this query, the officer receives a response from NCIC indicating the record has been successfully "cleared." Occasionally, officers have difficulty completing this query and receive a response from NCIC indicating the record was not successfully "cleared." This unsuccessful response sometimes reads "Reject - not on file," or "Reject - Invalid NIC number" etc.. In the event an officer receives one of these "Reject" messages, the officer should submit a QWI and obtain the NIC number from that query. They should then resubmit the "XC/CC" query until they receive the successful "cleared" response from NCIC.

19.1.4 Review of SRF Hits

Officers are required to review their SRF hit list three times per week and to ensure coverage of this function during any extended periods of leave. The SRF hit list is a tool to aid in the officers' supervision of a case. The reviewer should have the ability to determine if a hit requires follow up with the agency that made the inquiry.

19.1.5 Use of CAPTAIN in reviewing SRF Hits

In some cases, when a positive SRF hit occurs, the message includes a notation that the inquiry was made by the Capitol Region Mobile Data System (CRMDS). The CRMDS includes local police departments in the greater Hartford area. Telepartner is responsible for the support of many of the technical aspects of the CAPTAIN MDT software. Telepartner is contracted by the Capitol Region Council of Governments (CRCOG). CRCOG operates the CAPTAIN MDT software.

Captain Collect Audit Logs: Effective June 24, 2011, the U.S. Probation Office for the District of Connecticut has access to the Captain Collect audit logs, which will tell the U.S. Probation Officer the name of the police officer who made an inquiry on the person under supervision that the U.S. Probation officer currently supervises.

Steps to Access the Captain Collect Audit Log:

1) Go to https://portal.captainct.org
2) Enter the user id: usprobation and the password: password#1 Note: We all have the same user id and password.
3) Click on the Police tab, and select the Collect Audit tab.
4) You will see a page with Telepartner.DnnWhoRanAPlate.
5) Enter the date and time when the SRF inquiry was made.
6) In the "Search message that contains" field enter the license plate or the driver's license number. Note: You will get the license plate from your SRF hit under LIC. You will get the driver's license number from your SRF hit under OLN.
7) Click the search button.
8) You then will get the result for your search, the name of the police officer who made the inquiry.

Note: It is recommended that you then cut and paste this information into the PACTS chronological entries.

If you have any questions regarding the use of Captain, please contact the Captain coordinator, currently U.S.P.O Otto Rothi.

20. JOINT AUTOMATED BOOKING SYSTEM (JABS)

JABS is a Department of Justice, FBI, CJIS information sharing project among its law enforcement components. JABS provides the department's "front end" to the FBI's Integrated Automated Fingerprint Identification System (IAFIS) by providing an automated process for the collection and transmission of fingerprint, photographic, and biographical data.

The mission of the JABS information sharing system is to:

1) automate the booking process,
2) enable each agency to share and exchange booking information, and
3) establish a federal offender tracking system. The strategic goal of the JABS Program is to facilitate electronic access to IAFIS for any Federal law enforcement agency/office that has a requirement to submit fingerprints to the FBI. This avoids duplicate efforts in other Federal agencies.

The JABS-IAFIS interface has reduced the time to identify an individual from several weeks for a paper fingerprint submission to less than one hour. Additionally, JABS supports an IAFIS

query transaction that reduces the identification processing time to less than 10 minutes. Equally important, the JABS booking submissions provide a "real-time" updating of the FBI's criminal master files that are available to all Federal, state, and local law enforcement agencies through the National Crime Information Center (NCIC).

20.1 Access to JABS

The JABS interface is accessed via Law Enforcement Online (LEO). LEO is a web-based database that provides general law enforcement information and is the probation office's gateway to the JABS database. Access to LEO is granted through the Department of Justice in response to an enrollment form which is faxed to the LEO administrative office in Louisiana. A designated probation officer is the Local Agency Coordinator (LAC) for the probation office. The LAC will provide each probation officer with the requisite forms and avail them of the requirements of the LEO/JABS programs.

LEO/JABS access is available to all probation officers who have met the requirements set forth for access to the ATLAS/NCIC/NLETS program.

The information obtained from JABS is considered sensitive, and not for public dissemination. Access and usage is subject to the same requirements as outlined in Section 18 ATLAS.

20.2 Uses, Procedures, and Benefits

JABS affords the probation office with unfettered access for booking defendants/people under supervision after an arrest by a participating agency. The booking packet includes a photo, demographic information, biographic information, and charges among other information. This information and booking package is available from the probation officer's agency issued computer via the internet.

Currently, the probation officer is the primary designated booking agent. The JABS booking station is used when a defendant does not have an assigned FBI number (e.g., misdemeanor cases or entry of a plea via an Information when arrest does not occur). The assigned probation officer will coordinate with the probation officer assistant or their designated booking agent to schedule a booking which will be electronically submitted for assignment of an FBI number (all people under supervision must have an FBI number).

The JABS booking station is the only acceptable fingerprinting accepted by the Criminal Justice Information Service (CJIS)/FBI for an initial booking. The JABS software will allow the probation office to book a defendant while attributing the initial arrest to the appropriate agency (i.e. U.S. Park Police, ATF, FBI, etc.). Upon acceptance of the booking packet by CJIS, the person under supervision will be assigned an FBI number in NCIC.

21. CASE MANAGEMENT/ELECTRONIC CASE FILING (CM/ECF)

CM/ECF is the federal courts' case management and electronic case files system. It provides courts enhanced and updated docket management, and it allows courts to maintain case documents in electronic form. ECF also provides each court the option of permitting case documents - pleadings, motions, petitions -to be filed with the court over the Internet.

21.1 Authorized Filers

Authorized filers are chief probation officer, deputy chief probation officers, supervisory probation officers, and the sentencing guidelines specialist.

21.2 Documents that are Filed

- Draft Presentence Reports (PSRs) (disclosures)
- Final PSRs
- PSR recommendations
- Petitions (Forms 12-A, B and C) (the standard order must accompany the petition; use when you are requesting action from the Court)

21.3 ECF PACTS DOCUMENT IMAGING (PDIM)

Probation officers must upload all documents to PDIM that are filed in ECF.

21.4 Sealed Cases

In all instances where there is a sealed case AND a public case, all documents must be provided to the Clerk's Office for them to file on probation office's behalf.

21.5 Criminal Cases in ECF

The types of criminal cases in ECF are public, sealed, and partially sealed. In partially sealed cases, the defendant's name and, for example, the arrest and Indictment, may be public record. However, the fact that the defendant pled guilty and was sentenced may be sealed (thus, partially sealed).

21.6 Case Type in Which ECF is Required

Following are the case types for which ECF is required:

- Cases originating tin this transfer
- Transfers of Jurisdiction
- Unsealed cases
- Sealed cases as noted above

When the District judge delegates a case to a magistrate judge, the Clerk's office opens a referral to the magistrate judge on criminal duty at the time. That referral will remain open for the duration of that person's supervision and that magistrate judge, as well as the District judge will receive notice of all of our filings. The magistrate judge assigned to handle the

matter the first time will continue to handle all further supervision matters for the district judge unless the district judge rescinds the referral.

21.7 Cases In Which the Sentencing Judge is Retired or Deceased

In cases where the sentencing judge is no longer available and the case has not yet been reassigned to an active judge (typically the Chief Judge), the documents are filed in ECF. Once filed, the Clerk's Office will receive notice and assign the case to an active judge. The probation officer should contact the Clerk's Office and find out which judge has been assigned.

21.8 Follow up on Filings - Documentation in PACTS

21.8.1 Supervision Filings

1) Officers should enter all cases into ECF as an interested party. Once this is completed, officers will receive notice of any filings in that case;
2) Our office receives e-mail notification of the filing and notice of the action taken by the judge if a minute order is entered or if a standard order is signed and then filed;
3) Is it the officer and supervisory probation officer's responsibility to follow up on filings, if action had been requested.
4) Officers and supervisory probation officers should always use the proper chrono codes indicating filing with the Court. If it si a violation and/or a new arrest. The officer and SUSPO should also use the non-compliance and/or new arrest modules.

21.8.2 Presentence Filings

1) Disclosures: All disclosures should be filed in ECF.

2) Final Reports: All final reports should be filed in ECF. The judge, the AUSA and opposing counsel must receive notification. Never file the final report and the recommendation as one document. The recommendation is ony available to the judge.

22. CLEAR

(policy to follow once in production)

23. ELECTRONIC REPORTING SYSTEM

The Electronic Reporting System (ERS) will ultimately allow the Judiciary to exchange case-related information with defendants, people under supervision, and treatment providers using kiosks, the internet, and telephones. Kiosks are located in each of the three divisional offices, and may be accessed during regular office hours. The District of Connecticut has chosen the 5-Point kiosk brand, which consists of a steel housing unit (the physical kiosk), internal computer with connection to PACTS, keyboard, trackball, and fingerprint scanner. Persons using the

kiosk are granted access upon a fingerprint match, and must open and close their kiosk sessions with a fingerprint match. Internet reporting allows defendants and people under supervision to submit reports, and receive messages from their officers, any time, via any internet connection.

Use of supervision reporting by ERS has several benefits and features. For example,

- the system will send an email notification to one or more recipients;
- display questions associated with an assigned question set (i.e. pretrial or post-conviction);
- display certain information from PACTS;
- allow the defendant/person under supervision to provide/update residential information;
- allow the -person under supervision to provide/update employment information;
- allow the person under supervision to provide/update financial information;
- allow the person under supervisionto provide treatment attendance information;
- allow the person under supervision to provide community service completion information;
- allow the person under supervision to answer standard questions;
- display a summary screen of answers;
- create a Monthly Supervision Report (MSR) automatically from the data entered by the person under supervision;
- place the MSR in the PACTS PDIM module automatically;
- create a MSR submission chrono automatically;
- highlight changes entered by the person under supervision in an email sent to you immediately upon the person under supervision exiting the ERS module

The ERS system records information entered by the person under supervision and reports it to the officer, via an email message, or, alternately, when the officer reads the PDIM copy of the MSR. PACTS does not automatically update with new information provided by the person under supervision. For security purposes, the person under supervision should not have direct access into the PACTS system. Therefore, the officer will be required to verify the information submitted by the person under supervision, and, utilizing the "update" feature in the PACTS ERS module, manually update the appropriate information. Once this information is updated, on their next report submission, the officer will see that information as the "current" information in the ERS system.

23.1 Usage

23.1.1 High-Risk People under supervision

Because certain high-risk people under supervision require face-to-face contact, this option is not available for people under supervision with high PCRA scores, unless approved by a supervisor, or used as a controlling intervention.

23.2 Revocation of Privilege

The privilege of using the internet to submit supervision reports may be extended to people under supervision if required at the officer's discretion.

23.3 Kiosk and Internet Registration Process

In order for any person under supervision to access a kiosk or internet reporting system, they must be registered in the PACTS ERS module. This is a relatively simple, self-explanatory process wherein the person under supervision's fingerprints are recorded, a question set is selected, and they are instructed on correct kiosk/internet use. The JNET IT section provides clear, step-by-step instructions for ERS use.

23.3.1 Kiosk

In general, the officer selects the "Enroll Client" option, found in the "Client Reporting Functions" option on the PACTS tree. With the fingerprint scanner plugged in, the officer selects the "Click here to enroll into WEB-key" option. The registration process requires the officer to select at least two fingers to be used by the person under supervision for fingerprint matching. The officer can change the current finger selection by clicking on the finger they wish to use. The finger being registered is identified by a green arrow. This allows for the officer to accommodate anyone with missing or damaged fingers. Each finger will require three scans, then the selection of the question set. We are using the national question sets for both pretrial and post-conviction cases.

23.3.2 Internet Registration Process

Internet enrollment is accomplished through the same method as for the Kiosk; section 23.3.1: Kiosk. However, the officer selects "internet" as the reporting method.

23.3.3 Multiple Enrollments

Any client may be enrolled for both internet and kiosk reporting. Two enrollments must be completed (one for each method). Check the district web site for instructions and updates.

24. CREDIT REPORTING SYSTEM AND USAGE

Court ordered conditions of Bond, Probation and Supervised Release, authorize access to defendant or person under supervision's consumer credit report. A credit report check may be authorized for the purposes of a pretrial investigation, presentence investigation, and supervision of Probation/Supervised Release/Parole. A credit report that is obtained must match up to a case in PACTS and have a legitimate purpose in connection with official duties.

Web Based Training: All officers shall obtain software training by CBC Innovis through a web based training portal. Upon completion of the training all officer will be given a protected password that will allow access to CBCWeb.

Release of Information: It is imperative that a release of authorization be signed by the defendant/person under supervision. Officers must have a signed Financial Release on file for every credit report that is obtained. The financial release (Prob Form 48E for PSR, which is only valid for 90 days from the date of signature, and a Prob Form 48I for Supervision, which is valid while under the term of supervision), must be uploaded in PACTS and available for audits.

Access: To access CBCWeb, go to https://creditbureaureports.com you can then bookmark the site.

Data fields: On the Entry Form, enter the PACTS number in the field that says "Application/Loan #" This must be filled in with the PACT# as a reference number. It needs to be entered for audit purposes, similar to audits done for ATLAS and CLEAR. A copy of the credit report can be uploaded in PACTS.

25. PACTS DOCUMENT IMAGING (PDIM)

This policy covers the upload of electronic documents, storage of documents on the central hosting server and the destruction of documents for a given case.

Documents in PACTS Document Imaging Module are organized into groups (such as Charging, Court and Investigation documents) to facilitate identifying, finding and working with various documents. Document groups are not standardized and can be created and deleted depending on the needs of the district.

Each document group contains various document types (such as Arrest Report, Intake Form, etc.). Unlike document groups, document types are standardized. Document type standardization is essential for inter-district case transfers that involve sending document images from one district to another.

Paper Documents to be Scanned: Paper records created or received by probation offices shall be scanned into the Electronic Probation and Pretrial Services System (EPPS) of PACTS. The scanned record shall be deemed to be the official record.

Electronic Documents: Original electronic documents (i.e., those created or received in electronic format and never printed) shall be transferred into EPPS. Once the file has been loaded into EPPS, the original file may be deleted from the author's/recipient's local directories.

Hardware/Software: There are network-attached scanners provided to each officer. All staff will be able to scan and upload documents into PACTS. Adobe Acrobat software will be used at every computer/desktop to produce document images in pdf format. The Document Upload utility in PDIM is used to import and index the document images.

25.1 Destroying Temporary Records

Title 36 § 1226.24 provides guidance on how agencies must destroy temporary records. The National Archives and Records Administration (NARA) has concurred with the Judicial Conference's approval to destroy paper case file records once they have been scanned into the Electronic Probation and Pretrial Services System (EPPS) and verified for quality control purposes. This authority to dispose of paper records will require a quality control program to ensure that the scanned records are identical to the paper version. Disposition of paper records must be conducted according to the procedures outlined in 36 C.F.R. § 1226.24, which states:

25.1.1 Sale or salvage of unrestricted records

1) **Paper records**: Paper records to be destroyed normally must be sold as wastepaper or otherwise salvaged. All sales must follow the established procedures for the sale of surplus personal property. (See 41 C.F.R. part 101-45, Sale, Abandonment, or Destruction of Personal Property.) The contract for sale must prohibit the resale of all records for use as records or documents.
2) **Records on electronic and other media**: Records other than paper records (audio, visual and electronic records on physical media data tapes, disks and diskettes) may be salvaged and sold in the same manner under the same conditions as paper records.

3) **Destruction of unrestricted records**: Unrestricted records that agencies cannot sell or otherwise salvage must be destroyed by burning, pulping, shredding, macerating or other suitable means authorized by implementing regulations issued under E.O. 12958, as amended or its successor.

25.1.2 Destruction of classified or otherwise restricted records

If the records are restricted because they are national security classified or exempted from disclosure by statute, including the Privacy Act, or regulation:

1) **Paper records**: For paper records, the agency or its wastepaper contractor must definitively destroy the information contained in the records by one of the means specified in paragraph a. (1) of this section and their destruction must be witnessed either by a Federal employee or, if authorized by the agency, by a contracted employee.

2) **Electronic records**: Electronic records scheduled for destruction must be disposed of in a manner that ensures protection of any sensitive, proprietary or national security information. Magnetic recording media previously used for electronic records containing sensitive, proprietary or national security information must not be reused if the previously recorded information can be compromised in any way by reuse of the media.

The Administrative Office's Public Access and Records Management Division and OPPS have identified the following issues that each office is in need of considering before disposing of paper records:

25.1.3 Disposal Authority

The destruction of a paper record is allowed after the information has been converted to an electronic medium and verified, when it is no longer needed for legal or audit purposes or to support the reconstruction of, or serve as a backup to, the electronic files.

25.2 Quality Control

Scanned documents must be "verified" before the paper is destroyed. The quality control review should ensure that (1) the scanned document and the copy have the same number of pages; (2) the scanned image is properly aligned; and (3) the scanned image is clear and readable.

Prior to destroying any document, the officer destroying the document (or placing the document in a Shred-It box for destruction) needs to be 100% sure that the document is scanned correctly and is readable. This should occur by viewing the document in PACTS.

For paper records that have already been scanned and are stored on-site, the destruction of documents may be handled by shredding. The office may identify a contractor (e.g., Shred-It) to either securely transport the records to their facility or send a mobile facility to do on-site, witnessed destruction. The witness may be a government employee or a contractor, if authorized by the agency. It is preferred that the destruction occur on-site and that the witness be a government employee.

25.3 Restriction Memorandum

A memorandum shall be prepared by the supervising government employee listing/describing:

- the records to be destroyed (e.g., case filed with PACTS numbers 0001-9999); case files closed between January 1, 2000, to December 31, 2008);
- the method of destruction;
- the vendor performing the destruction; and
- the date of destruction.

All supporting documentation should be attached to the memo. The memo and documentation must be retained by the office for the purpose of audits and program reviews.

25.4 Electronic Probation and Pretrial Files

25.4.1 Pretrial

Initial documents to be scanned and uploaded (or copied from CM/ECF) at the opening of a pretrial case are as follows. Do not scan or upload the NCIC/ATLAS or any criminal history information;

- Notice to Defendant (PS1) – complete information in boxes at the top of the form prior to scanning;
- Warrant/Summons;
- Charging document (Complaint, Information, Indictment);
- CJA23 (Financial Affidavit);
- PS2;
- Photo page;
- Release of Information (if there are no signatures on the release form, do not upload);
- Supervisor's Case File Audit Report – PS13 Initial to be uploaded after SUSPO completes;

Rule 5 In: In addition to the documents mention in Section 25.4.1, upload the following documents from the sending district:

- PS2
- Bail Report
- Transfer letter

Rule 5 Out: All documents listed above will be uploaded in addition to the letter to the receiving district regarding the transfer.

25.4.2 Detained Pretrial Case

In addition to the documents listed above, the following documents will be scanned and uploaded (or copied from CM/ECF):

- Temporary Order of Detention
- Order of Detention

25.4.3 Released Pretrial Case

In addition to the documents listed above, the following documents will be scanned and uploaded (or copied from CM/ECF), as applicable:

- Appearance Bond
- Conditions of Release
- Notice Regarding U.S. Passport for Criminal Defendant (PS40)
- Pretrial Release Reporting Instructions
- If Courtesy Out – Letter to district requesting courtesy supervision

- If Courtesy In – upload the bail report, PS2 and letter requesting courtesy supervision from the district of jurisdiction. The court documents may be accessed through PACER and uploaded as with ECF.
- Do not scan routine NCIC/ATLAS reports run during pendency of pretrial case. Routine correspondence, Consent to Modify Conditions of Release, pay stubs, MSRs (if USPO requires), etc., are to be scanned and uploaded after documents are placed in USPO's filing basket.
- Upload the PS13 Final after the final audit is completed. Perform a quality review of all documents imaged to be sure they are correctly named, scanned and dated.

25.4.4 Pretrial Collaterals

Scan and upload the request for a pretrial collateral investigation and the subsequent response/report as separate documents. Scan and upload the supporting documentation. If the USPO responds by email, request a copy of that email to upload. No paper copies are kept and, in fact, the WordPerfect versions of the response also do not need to be kept.

25.4.5 Pretrial Diversion

For a normal diversion case, there will not be any court documents to upload from CM/ECF. Documents necessary to keep from the investigation state will be scanned and uploaded at the time the case is accepted for diversion supervision. Diversion cases will have the following documents scanned and uploaded into PACTS.

- AUSA Recommendation for PTD;
- Pretrial Diversion Investigation report;
- Pretrial Diversion Agreement;
- Release of Information form(s);
- Investigation materials;
- Photo page;
- PROB 1;
- MSRs

If the investigating officer does not recommend pretrial diversion, then all investigative materials will be kept in a paper file pending the possible charging and subsequent prosecution, PSI, etc. you will only upload the pretrial diversion request and Pretrial Diversion Report.

25.4.6 Investigations

Documents must be scanned and uploaded during investigation and completed by sentencing.

25.4.7 HIV/AIDS documents

All confidential documents dealing with AIDS/HIV defendants will not be scanned and uploaded. The paper will be the only record for these cases in accordance with confidentiality regulations.

25.4.8 Presentence Investigations

At the time an investigation closes, the following documents have been scanned and uploaded or converted to Adobe format (pdf) from either CM/ECF or from the WordPerfect document:

- Charging documents (Complaint, Information, Indictment or superseding documents) if not already done so during Pretrial;
- Plea Agreement or Verdict;
- Presentence Report with the correct sentencing date reflected on the Facesheet;
- Addendum/Addenda to Presentence Report (separately);
- Recommendation to Presentence Report (separately);
- Judgment & Commitment Order and any subsequent Amended Judgments;
- Statement of Reasons;
- Objections to the Presentence Report (if any);
- PROB 1 Worksheet

25.4.9 Cooperation Agreement/5K1.1 Motions

Upon receipt of a Cooperation Agreement or a motion pursuant to Guideline 5K1.1, Substantial Assistance to Authorities, the documents will be scanned into PACTS by the officer and marked "Sealed." To facilitate this, select "Yes" from the drop down box labeled "Sealed." The sealed document will be highlighted in red. Only these documents need to be marked as such, not the entire file. The paper copy is to be shredded.

25.4.10 Collaterals

Scan and upload the request for a collateral investigation (pretrial and post-trial) and the subsequent response/report as separate documents. Scan and upload the supporting documentation. Email the response and attachments to the requesting office. No paper copies are kept, and, in fact, the WordPerfect versions of the response do not need to be kept.

25.4.11 Prerelease/Pretransfer Investigations

Scan/upload request for investigation including supporting documents (PSR, J&C, etc.):

- Scan/upload investigative materials used in making decision
- Scan/upload response

25.4.12 Postsentence Investigations

Most documents should already be scanned during pretrial. However, if not, see the pretrial section and add those documents.

Scan/upload the postsentence report using the same guidelines as for the presentence report. Postsentences are usually done when sentenced to probation and waived the presentence. See the supervision section also for additional guidance on opening a supervision case in PDIM.

25.4.13 Miscellaneous Investigations

There are some miscellaneous investigations which may be requested or warranted during the period of supervision: preliminary interviews, violations, etc. for these, the final report will be scanned and uploaded into PDIM.

25.4.14 Supervision

Investigation file not in PDIM: You will need to scan and upload the necessary documents from pretrial and the investigation (see those sections). If the file is being sent from another district to us, all documents will be scanned and uploaded. Many documents come in during the time a defendant is incarcerated,

- furlough requests,
- pre-release planning,
- Progress Reports from BOP,
- Notice of Release and Arrival,
- communications with the halfway house,
- letters from defendants and responses to those letters, etc.

These documents need to be scanned and uploaded into PDIM. These documents can then be shredded.

Any documents which are confidential due to AIDS/HIV, etc., will be kept in the confidential folder centrally located in each office.

Pretrial and Investigation file already in PDIM All documents received while the person under supervision was incarcerated will be scanned and uploaded.

During supervision: There will be many documents received and created during the term of supervision. We will attempt to identify and deal with the most common or troublesome ones in this guide.

Documents received: Documents will be date-stamped in, scanned and uploaded with notification to the officer. The hard copy will be forwarded to the officer.

Documents created: If the document is created in Word and an electronic signature is used, the document must be converted to pdf format, electronically signed and upload into PACTS.

If the document has an original signature, it must be scanned and upload it in PDIM and then shredded.

25.5 Documents to Scan/Upload and Keep in Paper Format:

- Monthly Supervision Reports must be kept for one year from the date of receipt;
- Documents signed by the defendant/person under supervision under the penalty of perjury (18 U.S.C. § 1101) must be kept for 20 years from the date of completion/termination of supervision;
- Original sex offender registration forms must be kept for 20 years from the date of completion/termination of supervision;
- Probation Form 48D, which is signed under the penalty of perjury, must be kept for 20 years from the date of completion/termination of supervision. Accompanying forms (Net Worth Statements, Cash Flow Statements, etc…) may be scanned and uploaded into PDIM. These original documents may then be shredded.
- Probation Form 45 must be kept with the financial or procurement files for financial audit, but not in the case file, and must be destroyed three years after final payment or until records have been audited, whichever is later.

These documents will be kept in a centralized cabinet in each office location. Each individual persons' documents will be clipped together, in alphabetical order, which will yield quick access if such documents are needed, and will be monitored by clerical.

25.6 Documents not Scanned/Uploaded – Only Kept in Paper Format:

- AIDS/HIV documentation/correspondence
- Anything else highly confidential that the officer indicates should not be in PDIM Schedule Changes for Location Monitoring cases
- NCIC/ATLAS criminal record checks

When closing a supervision file: The officer who enters the closing information in PACTS will perform a quality review of the scanned/uploaded documents starting from the date that the supervision file opened.

26. VIDEOCONFERENCING TO WYATT DETENTION CENTER

Video conferencing with Wyatt Detention Center is available in the New Haven, Bridgeport and Hartford Probation Office conference rooms. Use of the equipment can save time for probation officers, attorneys, and U.S. Marshal staff. Video conference equipment is available between 9am and 4pm Monday through Friday. If possible, please avoid scheduling the start of interviews at count times, 11am and 3pm.

To arrange a video conference:

- The probation officer assigned the case should contact defense counsel to see if he/she has any objection to conducting an interview via video conference. Counsel may also contact the USPO and request video conferencing. Counsel may attend the interview either with the officer at the probation office or at Wyatt with the defendant.

- Contact Joyce Crowther to check availability of the conference room at the requested time. Contact the IT department and advise of the date and time that you plan to conduct the interview so that there is someone available in case of equipment malfunction.

- The probation officer will schedule the interview with the Wyatt Detention Center by sending a request via email on letterhead. The letterhead should include the defendant's name and the proposed time and date of the interview. If the defense attorney plans to participate in the interview at Wyatt, include the attorney's name and his intention to do so. Video requests should be emailed to hhammond@wyattdetention.com with a carbon copy sent to jsingleton@wyattdetention.com In the event that an interview needs to be cancelled, please contact Wyatt advising them of the cancellation.

27. ELECTRONIC SIGNATURES

The U.S. Code defines an electronic signature for the purpose of U.S. Law “an electronic sound, symbol, or process, attached to or logically associated with a contract or other record and executed or adopted by a person with the intent to sign the record.” This allows documents which would normally be printed and signed using pen and ink to be submitted electronically thus allowing for the reduction of paper.

When certain allowable documents are created, an electronic signature may be affixed to said document by placing the signature box at the required point in the document. Using the Cosign software application for electronic signatures, the document is signed and then verified by a digital certificate created by the Administrative Office.

The only authorized and accepted electronic signature is from the Cosign application installed on the individual’s work computer. Scanned JPG or other image files of staff signatures are not authorized.

The user’s signature requires authentication to Infoweb to be considered valid. Therefore a DCN connection will be required to sign a document and as such adherence to the district internet policy is a must.

An employee who is authorized to use electronic signatures may not delegate to anyone else the use of their signature.

The following documents may utilize electronic signatures:

- correspondence to attorneys
- correspondence to clients
- correspondence to other probation offices
- correspondence to other law enforcement agencies
- collateral requests and contacts
- travel permits
- correspondence to the Court
- Financial instruments including travel permits

28. COMPUTER SECURITY TRAINING

All probation office staff must understand the vulnerabilities, threats, and risks inherent in using automated information systems. Training office network users to be aware of computer security-related issues and enacting appropriate responses is required in new employee orientation programs and in periodic programs designed to reinforce and enhance security awareness. Every probation office network user is responsible for attending at least one computer security training session per calendar year. Users are required to sign the User Memorandum of Agreement, which acknowledges user responsibility to conform to the requirements and conditions established by the District of Connecticut Information Security Guidelines document.

Computer security training increases the knowledge and awareness of current computer security policies and issues affecting the courts' systems and resources, thus helping to protect DCN resources. Computer security training emphasizes the user's role in computer security, explains what can be done to reduce security risks, and reminds staff of the policies and procedures in place to protect the network. Most importantly, the training conveys the fact that practicing effective computer security is everyone's responsibility.

28.1 Goals of Security Training

The probation office regularly conducts computer security training to accomplish the following goals:

- Ensure personnel are consistently trained to employ approved security practices while using probation office computer equipment and networks.
- Educate users regarding effective password and data management

- Educate users of the nature and source of security threats, and provide them with approved resources to effectively detect and respond to security-related issues, when needed.
- Develop and present formal computer security training and orientation programs to disseminate new computer security-related office policies and information, as needed. Information may include security awareness bulletins and banners and official memoranda, either as paper or electronic distributions.
- Demonstrate security features of computer equipment and/or utilized software packages, and instruct personnel on the officially approved use of such features, as needed.
- Describe the rules and responsibilities when using Government IT resources, if such rules and responsibilities differ from established office policies.

In addition to the IT unit's established computer security training, the IT unit regularly evaluates the need for training staff on the use of approved systems and software, and develops training programs, as needed. Such training includes, but is not limited to, usage of IPhone devices, employing updated feature sets on e-mail clients, and using enhanced remote connection technologies.

29. IT Security Log/Intrusion Detection Management Policy

Connecticut Probation will routinely generate, collect, store, analyze, and protect computer security logs for intrusion detection and protect against the insider threat. To ensure security logs are managed in a consistent and effective manner, supporting processes are documented below and periodically updated when required**.** If it is believed that there has been an unauthorized intrusion or a possible insider threat has occurred, Systems staff, the ITSO, and the CUSPO will be notified immediately and as per policy the Incident Response program will be activated.

29.1 Policy

Logging will be turned on for all servers, computers and network hardware (CTP managed switches, access points, etc.). Log generation and retention will be protected in such a manner so that changes to server logging can only be done by a domain administrator account. Primary server logs (Domain Controllers, File servers, wireless access points, etc.) will be reviewed on a routine basis by IT personnel familiar with logging functions in order to determine if there is an anomaly that requires further investigation. Specific computer logs will be further reviewed when suspicious or unusual activity is detected. The Kiwi Syslog program is used for this purpose and provides real-time alerts to Systems staff when attempted changes are made to accounts, group policies, and servers.

29.2 Log Review

It would be too overwhelming and time consuming to expect that every log on every computer, server, and network device will be reviewed/monitored daily. However, there are specific logs on primary servers that should be reviewed at least daily.

In CTP's Active Directory environment, important activities are logged by the domain controllers (DCs) that can be very revealing as to who is accessing what resources and when. Specifically, three DC logs need to be reviewed on a daily basis: Application, Security, and Systems. If a rogue account is created, or if an account's privileges were elevated, these instances will be recorded within the DC's Security Log. If the DC's anti-virus program was turned-off, this would be recorded in the Application log. Anyone using secure wireless access points would be logged in the Systems log.

Kiwi Syslog sends a daily syslog statistics email report each evening to the IT staff which will display any critical errors or messages contained in the logs. Staff will then monitor any systems that are reporting syslog messages by severity (i.e. errors, notices and warnings).

29.3 Log File Retention

All log files are subject to the normal backup procedures, so this allows the staff to retrieve log information for up to seven years.

29.4 Analysis

Log data will be analyzed regularly to understand the expected behaviors of IT systems as well as to assist with identifying and troubleshooting anomalous events. Logs must be reviewed in response to suspected or reported security incidents. CTP uses Kiwi Syslog and Solarwinds Event Log Forwarder (ELF) as our automated log auditing tool. ELF forwards all log information to the Kiwi Syslog server providing real time email alerting to Systems. Systems personnel will regularly review retained log files on the Kiwi server (Application, Security, and System logs

29.5 Log Security and Protection

For Windows servers and computers, Group Policy will control and secure client logging. Individual users will not be able to delete logged events or change a particular log's properties. Network infrastructure hardware is password protected and can only be accessed by domain administrators. Server Systems logs are transmitted from the host servers securely to the ELF server.

29.6 Log Disposal Requirements

Logs required for auditing (Application, Security, Systems, IDS, etc.), will be retained on the server for a minimum of the current month or as disk space allows. This means that every month the previous months logs will be deleted from the server. When further investigation warrants or if directed from senior management, the responsible administrator will increase the log retention time as required.

29.7 Roles and Responsibilities

Periodic log auditing will be performed by the responsible system administrator. Because CTP has a small IT staff, it will be impossible to maintain a reasonable separation of duties during security investigations that are considered serious in nature. However, when deemed appropriate by senior management (the Chief Probation Officer), the IT Security Officers' delegate will be responsible for extracting log data for the investigation. This helps to ensure the integrity of the log files and avoids any perceived conflicts of interest.

30. IT Security Incident Response

30.1 Introduction

The District of Connecticut (CTP) is committed to providing a timely and comprehensive response to adverse events such as computer viruses, IT device theft, automated attacks, and intrusions. It is the policy of the court to ensure that appropriate action is taken to minimize the consequences of an adverse event.

30.2 Purpose and Scope

The purpose of this section of the policy is to establish a process for reporting and responding to information technology (IT) security incidents. This policy also acknowledges the collaboration between the JASIRC and the district for the coordination and execution of incident reporting and response services.
This Policy applies to all IT resources owned, leased, or operated on behalf of the district. All district employees, contractor personnel, interns, visitors, and other non-government employees are obligated to comply with this policy.

30.3 Roles and Responsibilities

This Incident Response Policy identifies essential roles and responsibilities of incident response management and support personnel. The following roles perform incident response support activities:

CTP Computer Incident Response Team (CIRT) – The CTP CIRT is specifically trained and authorized to address IT security issues. It is responsible for providing a quick, effective and orderly response to computer related incidents such as virus infections, hacker attempts and break-ins, improper disclosure of sensitive information, system service interruptions, breach of personal information, and other events with serious information security implications. The CIRT coordinates with the Judiciary Automated Systems Incident Response Capability (JASIRC) according to procedures established in the CTP Incident Response Plan and JASIRC Handbook; receives, processes, and disseminates notifications and guidance from the JASIRC; and works with the JASIRC to analyze and resolve IT security incidents, as appropriate.

Court Information Technology Security Officer (ISO) – Responsible for developing, implementing, coordinating, and maintaining IT security policy and procedures for the court.[1]

Director of Information Technology and Systems (DIT) – Is ultimately responsible for the security of the system, including ensuring that adequate event logging is enabled and ensuring incident response policy and procedures are documented, followed, and periodically reviewed. At CTP, this person also fills the roles of **CIRT Leader**[2] and **JASIRC Liaison.**[3]

Chief, U.S. Probation Officer – The Chief has primary authority and responsibility for information security within the court unit[4] and is responsible for the review and approval of the incident response policy and plan.

Court Non-IT Staff and Non-CIRT Personnel – Responsible for actively securing their systems and notifying the Computer Incident Response Team of any suspected information security incident.

Additionally, the following AOUSC offices provide national incident response support to court units:

Judiciary Automated Systems Incident Response Capability (JASIRC)- The JASIRC team operates within the Security Operations Center (SOC). This dedicated team responds to all confirmed or suspected **critical** and **serious** security incidents affecting the judiciary and works with local court stake holders to resolve incidents and to reduce security vulnerabilities that may cause incidents to recur. The JASIRC team also collects and analyzes incident trends within the judiciary. JASIRC uses InfoWeb to determine court points of contact for incident-related communication.

Security Operations Center **-** The SOC is a 24-hour, 7-day-a-week support center that addresses information security incidents, e.g., identifying a court computer that is beaconing to a known malicious site, that do not need to be escalated to the JASIRC team. The SOC works in collaboration with the court to remediate the vulnerability and restore the affected system(s) to an operational state. If the incident requires escalation to the JASIRC, the SOC facilitates this transition.

[1] Guide to Judiciary Policy, Volume 11, Chapter 6, Section 640
[2] The CIRT Leader is responsible for the activities of the CIRT and, unless delegated, manages the incident response and all incident-related communication and notification. The CIRT Leader also coordinates reviews of CIRT actions, which might lead to changes in policies and procedures for dealing with future incidents.
[3] The JASIRC Liaison coordinates incident response with the JASIRC.
[4] Guide to Judiciary Policy, Volume 15, Chapter 3, Section 320.20

Office of the Deputy Director - Chief of Staff - The *Office of the Deputy Director - Chief of Staff* is responsible for assisting with incidents involving law enforcement, such as the FBI or local police, and judiciary employees as the perpetrators of the incident. The JASIRC team provides this office with incident-related communication concerning judiciary employees, law enforcement agencies, executive branch offices of the government, or any non-judiciary organization. This office is not directed by the JASIRC team when handling incidents. Rather, they work collaboratively on incident resolution. The *Office of the Deputy Director - Chief of Staff* maintains a contact list in InfoWeb.

Office of General Counsel (OGC) - OGC is responsible for advising judiciary organizations and the JASIRC of legal implications surrounding a security incident, and ensuring the judiciary organization is not in violation of any laws or personnel rights when responding to an incident.

The JASIRC will work with the OGC to handle any legal issues associated with an incident. OGC maintains a contact list in InfoWeb.

Office of Public Affairs (OPA) - OPA is responsible for handling all internal and external communications with non-judicial organizations and individuals concerning security incidents, representing the judiciary organization on these issues. OPA is the judiciary's point-of-contact for all media inquiries. OPA maintains a contact list in InfoWeb.

30.4 Policy

In preparation for timely and adequate response to information security incidents, the court will develop and maintain an Incident Response Plan which addresses:

30.4.1 Roles and Responsibilities

- Identify the resources and staff assigned to plan and support incident response;
- Define the responsibilities for each identified incident response role; and
- Identify and routinely review/update the district's "Computer Security", "IT Security Officer", and "Systems Staff" contact information in InfoWeb.

30.4.2 Response Procedures

- Provide detailed instructions for implementing the court's incident response capability;
- Describe reporting and tracking requirements;
- Define reportable incidents and establish incident categories;
- Define impact containment procedures;
- Define evidence preservation and collection procedures;

- Establish internal and external procedures for incident notification, including the facilitation of information sharing across the court regarding IT security vulnerabilities, threats, alerts, and incidents;
- Describe how the court interfaces with external (e.g., JASIRC) incident response support; and
- Define expectations of incident response performance, both internally and when interfacing with JASIRC.

30.4.3 Training and Testing

- Establish procedures for initial and annually recurrent role-based incident response training for incident response staff and end users; and
- Establish procedures to test the district incident response capability at least annually, using a table top approach involving the CIRT and several of the non-CIRT court staff.

30.4.4 Plan Approval, Review, and Revision

- Document Plan approval by designated court officials;
- Keep the plan secure and protected from unauthorized distribution;
- Distribute the Plan to key incident response persons designated in the Incident Response Plan;
- Review the Plan at least annually;
- Update the Plan, as appropriate, to reflect changes in staff, procedures, and lessons learned from post-incident reviews; and
- Redistribute the Plan to key incident response personnel whenever it is updated.

30.5 Applicable Guidance

Guide to Judiciary Policy, Volume 11, Chapter 6: Information Systems and Security
Guide to Judiciary Policy, Volume 15, Chapter 3: Security

IT Security Incident Response Policy, October 2012.

JASIRC Handbook, March 2012

Guide to Implementing the Judiciary Information Security Framework, Appendix B: Judiciary Recommended Security Safeguards

30.6 Policy Review

The DIT and the ISO review this IT Security Incident Response Policy at least annually to ensure the policy statements set forth remain effective and reflect best practices and judiciary policy/guidance.

30.7 Exemption

Exceptions to overall judiciary incident response policy require a documented local waiver that has been reviewed by the IT Director and the ISO, and approved by the IT Director and the Chief USPO. The waiver should include a justification for the exception, a description of the residual risk, and any alternative safeguards employed to compensate for the exception. Approved waivers are reviewed annually for on-going validity.

30.8 Policy Authorization

This policy was reviewed and approved by the Director of IT and the Chief USPO in June of 2015.

31. POINTS OF REFERENCE:

Overview

2000-01 Definition of Information Technology
IT Information on the J-Net
IT Key Documents from the AO

Distribution of Equipment

AO IT Procurement Guidelines

Use of Equipment

"Personal Use of Government Office Equipment"

Personal computer for home program

Use of Judiciary-owned Portable and Personal Computers in Private Residences. IRM BULLETIN 2001-02

Network and computer security

Guidelines of Computer Security Practices and Standards
IT Security Policy 2007-06
Network and Security Policy
Wireless Technology Use V2.5
Security Guidelines for Wireless LAN Implementation

Storage of Data

IRM Bulletin 2003-01: Electronic Media Backup and Storage Procedures for Automated Information Systems

Internet Access

GUIDE TO JUDICIARY POLICY, Volume 15, Computer Security
97-19 Access to and Responsible Use of the Internet

Procedures Discouraging Personal Web E-Mail
Procedures Prohibiting Peer-to Peer File Sharing, Chat Rooms and IM

Intranet Access

IRM Bulletin 97-15: Intranet DNS Domain Name Standards

Use of software on government machines

IRM Technical Bulletin 94-17

Remote Access to network

IRM Bulletin 2003-02: Guidance on VPN and RAS to the DCN
Judiciary Remote Access

Maintenance of network and disaster recovery plan

Emergency Preparedness
Emergency Notification System
2003-01 Electronic Media Backup and Storage Procedures for Automated Information Systems

Telecommunications

Telecommunication Guidelines
Current AO Telecommunications Bulletins
For the latest AO telecommunications updates, visit the IT Memos page.

PACTS NPR extraction

National PACTS Reporting User Guide, Version 5.5.2, November 14, 2008