POLICY STATEMENT

Policy Statement 2001
Policy Area: Information Technology
Effective Date: JUN 22 2004
Approved: _____
Paul A. Quander, Jr., Director

_____
Susan W. Shaffer, PSA Director

PERSONAL USE OF INFORMATION TECHNOLOGY RESOURCES

I. COVERAGE

This policy covers all permanent, temporary, and part-time employees and interns of the Court Services and Offender Supervision Agency (CSOSA) and the Pretrial Services Agency (PSA) (hereafter referred to collectively as the "Agency"), as well as contractors or other entities that access Agency information technology (IT) resources.

II. BACKGROUND

Agency employees are provided with a professional supportive work environment. They are given the tools needed to effectively carry out their assigned responsibilities. Allowing limited personal use of these tools helps enhance the quality of the workplace and helps the Government to retain highly qualified and skilled workers.

The Agency recognizes that employees are responsible individuals who are the key to making the government more responsive to its citizens. Consequently, employees are expected to follow rules and regulations and to be responsible for their own personal and professional conduct.

III. POLICY

This policy establishes the rules for limited acceptable personal use of Agency-owned IT resources (Appendix B) from any location (i.e., office, home, other locations). Employees are permitted limited personal use of Agency IT resources. This personal use must not: 1) result in the loss of employee productivity, 2) interfere with official duties or 3) result in other than "minimal additional expense" to the government. Employee personal use of IT equipment must: 1) be performed on the employee's non-work time, 2) not interfere with the mission or operations of the Agency, and 3) not violate the Standards of Ethical Conduct for Employees of the Executive Branch or supplemental CSOSA and/or PSA policy or regulations.

Unauthorized or inappropriate use of Agency IT resources may result in: 1) loss of use or limitations on use of equipment, 2) disciplinary or adverse actions, 3) criminal penalties and/or 4) employees or other users being held financially liable for the cost of inappropriate use.

IV. AUTHORITIES, SUPERSEDURES, REFERENCES, AND ATTACHMENTS

A. Authorities.

- OMB Circular No. A-130 Appendix III (Security of Federal Automated Information Resources)
- Computer Security Act of 1987, PL 100-235, 101 Stat. 1724
- 5 U.S.C. § 552a (The Privacy Act)
- 5 U.S.C. §§ 7321-7326 (The Hatch Act)
- 5 U.S.C. § 552 (The Freedom of Information Act)
- OMB Circular A-130, "Management of Federal Information Resources"
- 5 C.F.R. Part 2635 (Standards of Ethical Conduct for Employees of the Executive Branch" promulgated by the Office of Government Ethics)

B. Policy Supersedures.

Agency Policy Statement 2000.1 – Internet and Electronic Mail Use (7/18/2001)

C. Procedural and other References.

Standards of Employee Conduct (8/30/1999)
Remote Access Policy - PS 2012
Account Management Policy - PS 2003
Network Security Policy - PS 2011

D. Attachments.

Appendix A. Definitions
Appendix B. Personal Use of Information Technology Resources Rules

APPENDIX A
DEFINITIONS

- **Agency Information Technology resources -** includes but is not limited to: personal computers and related peripheral equipment and software, network and web servers, telephones, facsimile machines, photocopiers, Internet connectivity and access to Internet services, e-mail and, for the purposes of this policy, computer-related office supplies. It does not include data stored in or transported by such resources.

- **Browser -** a software tool used to locate and view data in standardized formats on other computers.

- **Employee non-work time -** times when the employee is not otherwise expected to be addressing official business. This includes an employee's off-duty hours such as before or after a workday (subject to local office hours), lunch periods, authorized breaks, or weekends or holidays (if their duty station is normally available at such times).

- **Information technology -** any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data.

- **Internet -** a worldwide electronic system of computer networks which provides communications and resource sharing services.

- **Minimal additional expense -** the personal use of Agency IT resources is limited to those situations where the government is already providing equipment or services and the use of such equipment or services shall not result in any additional expense to the government or the use will result in only normal wear and tear or the use of small amounts of electricity, ink, toner or paper. Examples of minimal additional expenses include making a few photocopies, using a computer printer to print a few pages of material, making occasional brief personal phone calls (within Agency policy and General Services Administration Policy) infrequently sending personal e-mail messages, or limited use of the Internet for personal reasons.

- **Personal use -** activity that is conducted for purposes other than accomplishing official or government business. Agency employees are specifically prohibited by both the federal and Agency's Standards of Employee Conduct from using government office equipment to maintain or support a personal private business or personal activities (e.g., parties, clubs, etc.). Examples of this prohibition include employees using a government computer and Internet connection to run a travel business or investment service. The ban on using government office equipment to support a personal private business also includes employees using Agency IT resources to assist relatives, friends, or other persons in such activities. However, limited use under this policy of government office equipment to, for example but not limited to, check their Thrift Savings Plan

or other personal investments, or to seek employment, or communicate with a volunteer charity organization is permissible.

- **Shared Agency IT resource** - any Agency IT resource that is managed by one Agency organization but used by many.

- **World-wide Web (WWW) -** the collection of web pages (documents) which are developed in accordance with the hypertext (HTML) Web format standard and may be accessed via Internet connections using a WWW browser.

APPENDIX B
PERSONAL USE OF INFORMATION TECHNOLOGY RESOURCES RULES

A. Rules for Personal Use of IT Resources

1. Employees and contractors neither have an inherent right to employ Agency IT resources for personal use, nor does this policy create such a right for employees and contractors to use IT equipment for personal use.

2. Under this policy, employees and contractors are permitted limited personal use of Agency IT resources. This personal use shall not result in loss of employee productivity, interference with official duties or other than "minimal additional expense" to the Agency in areas such as:

   (a) Communication costs for voice, data, or video image transmissions;
   (b) Use of consumables in limited amounts (e.g., paper, ink, toner);
   (c) General wear and tear on equipment;
   (d) Data storage on storage devices; and/or
   (e) Transmission impacts with moderate e-mail message sizes, such as e-mails with small attachments.

3. Employees and contractors are expected to conduct themselves professionally in the workplace and to refrain from using government office equipment for activities that are inappropriate. Misuse or inappropriate personal use of Agency IT resources include:

   (a) Any personal use that could cause congestion, delay, or disruption of service to any Agency IT resource. For example, greeting cards, video, sound or other large file attachments can degrade the performance of the entire network as some uses of "push" technology, such as audio and video streaming from the Internet do.
   (b) The intentional creation, downloading, viewing, storage, copying or transmission of sexually-explicit or sexually-oriented materials;
   (c) The intentional creation, downloading, viewing, storage, copying or transmission of materials related to gambling, illegal weapons, terrorist activities, and any other illegal activities or activities otherwise prohibited;
   (d) Use for commercial purposes or in support of "for-profit" activities or in support of other outside employment or business activity (e.g., consulting for pay, sales or administration of business transactions, sale of goods or services);
   (e) Engaging in any outside fundraising activity, including non-profit activities, endorsing any product or service, participating in any lobbying activity, or engaging in any prohibited partisan political activity;
   (f) Posting Agency or personal information to external newsgroups, bulletin boards or other public forums without authority, including information that is at odds with the Agency's mission or positions. This includes any use that could create the

perception that the communication was made in one's official capacity as a Federal Government employee, unless appropriate Agency approval has been obtained;

(g) Establishing personal, commercial and/or non-profit organizational web pages on government-owned machines;
(h) Use of Agency systems as a staging ground or platform to gain unauthorized access to other systems;
(i) The creation, copying, transmission, or retransmission of chain letters or other unauthorized mass mailings regardless of the subject matter;
(j) Use of Agency IT resources for activities that are illegal, inappropriate, or offensive to fellow employees or the public. Such activities include, but are not limited to: hate speech, or material that ridicules others on the basis of race, creed, religion, color, age, sex, disability, national origin, or sexual orientation;
(k) The addition of personal IT resources to existing Agency IT resources without the appropriate management authorization, including the installation of modems on Agency data lines and reconfiguration of systems;
(l) Use that could generate more than minimal additional expense to the government;
(m) The intentional unauthorized acquisition, use, reproduction, transmission, or distribution of any controlled information including computer software and data that includes information subject to the Privacy Act, copyrighted, trademarked, or material with other intellectual property rights (beyond fair use), proprietary data, or export controlled software or data;
(n) Installing and/or running unauthorized software (e.g., Hotbar, Gator, etc.);
(o) Using another person's digital authentication or password;
(p) Sending anonymous messages; and
(q) Avoiding established security procedures.

4. Any use of Agency IT resources, including e-mail, is made with the understanding that such use may not be secure, is not private, is not anonymous and may be subject to disclosure under the Freedom of Information Act (FOIA). Agency employees do not have a right to, nor shall they have an expectation of, privacy while using Agency IT resources at any time, including accessing the Internet through Agency gateways and using e-mail, which may be subject to release pursuant to the FOIA. To the extent that employees wish that their private activities remain private, they should avoid making personal use of Agency IT resources.

5. Electronic data communications may be disclosed within the Agency to employees and contractors who have a need to know in the performance of their duties (e.g., with manager approval technical staff may employ monitoring tools in order to maximize the utilization of their resources, which may include the detection of inappropriate use).

B. Monitoring and Access

1. The Agency reserves the right to monitor and access IT resources including e-mail messages sent or received on its electronic information systems and Internet access.

2. Use of the Agency's electronic information systems constitutes consent to monitoring by the Agency of any type of use, including official and personal use.

3. Internal and external e-mail messages related to official business are subject to the provisions of the Freedom of Information Act and the Privacy Act (PA). E-mail messages that are retained or stored on Agency computers, on employees' personal computers when they are used for official duty, or in Agency filing systems may be reviewed for purposes of responding to a request under the FOIA or PA in the same manner as any other official Agency document or record.

4. Operate in accordance with special requirements for accessing, protecting, and utilizing data, including Privacy Act materials, copyrighted materials, business sensitive information, and classified information. Any official, work-related e-mails, electronic documents, or files may constitute a Federal record. If the item does meet the definition of a Federal record, it is the employee's responsibility to incorporate it into the Agency's official record keeping system. Any e-mails, electronic documents, or files are subject to the FOIA, the PA, and the confidentiality the Agency promises its clients related to business-sensitive information. National Security Classified information is never to be documented on a personal computer or on an uncleared electronic system. Questions about special requirements should be directed to the Agency Information Security Officer and/or the Office of the General Counsel.

5. Agency employees and contactors do not have a right, nor should they have an expectation, of privacy while using Agency systems to create, receive, store, or send information, including via the Internet or e-mail. Any information intended to be personal or private should not be placed on any Agency computer system. By using Agency electronic information systems, employees imply their consent to disclosing the contents of any web site visited or any contents or files contained in e-mails that pass through the Agency's information systems. As part of its monitoring or investigation of the use of its computer systems, the Agency may access the electronic files of employees, including e-mail and/or electronic records of Internet usage.

6. Employees' access to Internet sites is not anonymous. (e.g., for each use of the Internet over Agency information systems, the name and computer address of the employee user is recorded by the Agency and also, in many instances, by the locations accessed.) Employees should be aware that when access is accomplished using Internet addresses and domain names registered to the Agency, they could be perceived by others as

representing the Agency. Employees and contractors are prohibited from using the Internet for any purpose that would reflect negatively on or could embarrass the Agency or its employees. In addition, participation in news-groups, chat-sessions and list-serves, including information posting, must include the following disclaimer: "Views expressed by the author do not necessarily represent those of the 'Court Services and Offender Supervision Agency' or 'Pretrial Services Agency'" as appropriate.

7. The Agency has established controls to ensure that its electronic information systems are used appropriately. In accordance with applicable laws and regulations, use of the Internet by employees may be monitored. The Agency may, but is not obligated to, conduct electronic audits of employee computers to ensure that use of the Internet is business-related and does not include inappropriate uses as outlined in this policy statement.

8. Information that is sent, received or stored on any Agency computer equipment becomes the property of the Agency and may be accessed by Agency officials.

C. Personal Internet e-mail Attachments

When using Agency computers and browsers to access personal Internet e-mail (e.g., Hotmail, Yahoo Mail, etc.), copies of opened attachments to e-mail messages are automatically downloaded to Agency information systems and are subject to Agency monitoring and access controls as outlined in this policy. Employees and contractors may inadvertently infect Agency information systems with viruses if they access personal Internet e-mail attachments containing viruses. Therefore, employees and contractors must use the same caution as with their Agency e-mail, and are asked to delete any suspicious personal e-mail messages **without** opening the attachments. Employees are reminded that they must follow all the provisions of this policy when using Agency computer resources to access personal e-mail accounts (See Section B.).

D. Agency-wide messages

Agency-wide e-mails consume valuable network resources. Therefore, Agency-wide e-mails must be restricted to only those messages that are significant and important to the Agency and its mission. Agency employees and contractors are prohibited from sending Agency-wide e-mail messages without prior approval from their CSOSA Associate Director (includes the Agency's General Counsel and Chief Technology Officer), or their Agency Deputy Director, or PSA's Office of the Director, as appropriate. This includes messages announcing various significant events such as births, deaths, retirements, etc. Agency-wide e-mail messages from the Agency, PSA Director or Deputy Director (or authorized by the Agency or PSA Director or Deputy Director), and those from the CSOSA Office of Management and Administration or PSA Office of Finance and Administration related to safety, evacuations, security and other emergency situations are allowed. Agency employees

shall adhere to the following procedure when requesting approval to send an e-mail message to the entire Agency.

1. Obtain approval from your Supervisor on the message content.
2. The Supervisor will forward the e-mail content, their recommendation to distribute the e-mail Agency-wide, and any document that would be included as an attachment to their Associate Director (AD) or Deputy Director or PSA Office of the Director, as appropriate.

3. The Associate Director (AD) or Deputy Director or PSA Office of the Director, as appropriate will review the request and make a determination.

4. If the request is approved, the AD (or designee) or Deputy Director or PSA Office of the Director (or designee), as appropriate will send the e-mail out Agency-wide.

5. The AD (or designee) or Deputy Director or PSA Office of the Director (or designee), as appropriate will notify the requestor via e-mail of the determination. If the message is not determined to be appropriate for Agency-wide e-mail, an alternate method of distribution may be suggested.

E. Roles and Responsibilities

1. The Agency Chief Technology Officer (CTO) is responsible for:
   (a) The dissemination of this policy to all Agency employees and contractors.
   (b) Reviewing and maintaining this policy to adhere to future legislative changes or changes in OMB and Congressional guidance.

2. Management officials, in their supervisory role, are responsible for:
   (a) Informing users of their rights and responsibilities, including the dissemination of the information in this policy to individual users;
   (b) Addressing inappropriate use by employees who report to them;
   (c) Receiving reports of inappropriate use from IT resource management officials and sharing these reports, as appropriate, within their own management structure; and
   (d) Notifying, when appropriate, law enforcement officials. (Such a notification should be discussed with OGC first.)
   (e) Managers of Agency IT resources may use system-monitoring software in order to improve the performance of the resource. When a resource manager identifies an inappropriate use, he/she shall notify the Agency CTO through the normal chain-of-command and, as appropriate, terminate the access of the individual(s) to the IT resource after informing the employee's supervisor of the action to be taken.

3. Agency Employees and Users of Agency IT Resources, are responsible for:
   (a) Seeking guidance from their supervisors when in doubt about the implementation of this policy;
   (b) Ensuring that they are not giving the false impression that they are acting in an official capacity when they are using Agency IT resources for non-government purposes. If there is expectation that such a personal use could be interpreted to represent an Agency, then an adequate disclaimer shall be used. For example: "The contents of this message are those of the author and should not be construed to be endorsed (inferred or implied) by the Government nor by the Court Services and Offender Supervision Agency or Pretrial Services Agency, as appropriate."
   (c) Following policies and procedures in their use of IT Resources (e.g., Internet and e-mail) and refraining from any practices which might jeopardize Agency computer systems and data files, including but not limited to virus attacks, when downloading files from the Internet;
   (d) Learning about Internet etiquette, customs and courtesies, including those procedures and guidelines to be followed when using remote computer services and transferring files from other computers.
   (e) Familiarizing themselves with any special requirements for accessing, protecting and utilizing data, including Privacy Act requirements, copyright requirements, and procurement sensitive data; and
   (f) Adhering to all conditions set forth in this policy.

F. Enforcement of Policy

Violations of this policy will be reviewed by the Office of Professional Responsibility, the Chief Technology Officer, the Director of Information Technology/Pretrial Services Agency, the General Counsel, the Associate Director of the Office of Human Resources, or the Director of Human Resources/Pretrial Services Agency and may result in restricted network access, loss of network access, disciplinary action or legal action, including termination or referral for criminal prosecution.

G. Information and Assistance

Direct questions, comments, suggestions or requests for further information should be directed to the Agency IT Enterprise Director at 202-220-5370.