P1237.15 INFORMATION RESOURCES PROTECTION

Starting in May of 2006, the Office of National Policy Management began reformatting policies that contain change notices. With the rapid growth in word processing and electronic distribution via Sallyport and the internet, many of these WordPerfect 5.0 documents have become unstable.

No word or substance changes have or will be made to any of these documents. To avoid confusion these documents will be re-issued electronically with a new number and new date.

Thank you for your patience during this conversion process and please give me a call if you have any questions or concerns.

Robin Gladden
Directives Manager
(202) 616-9150

U.S. Department of Justice
Federal Bureau of Prisons

Program Statement

OPI: IPD/OIS
NUMBER: P1237.15
DATE: 12/31/2007
SUBJECT: Information Resources Protection

This is an electronic re-issuance for technical reasons only. There are no substance or word changes to the document.

1. **PURPOSE AND SCOPE.** To protect the Bureau's information resources from unauthorized use, misuse, and destruction.

Pursuant to OMB Circular A-130, Appendix III, all federal agencies are to establish a set of rules of behavior concerning the use of, security in, and the acceptable level of risk for computer systems.

These requirements apply to all Bureau paid and non-paid employees, including contractors, volunteers, interns, college students, etc.

2. **PROGRAM OBJECTIVES.** The expected results of this program are:

a. Information resources will be used by staff in a professional and authorized manner.

b. Sensitive information will be protected from disclosure to unauthorized individuals or groups.

c. Employees will be sanctioned for unauthorized use, disclosure, destruction or misuse of information resources.

d. Contract facilities will establish procedures to convey sanctions for contractor employees.

e. Security violations and system vulnerabilities will be immediately reported to the appropriate authorities.

3. **DIRECTIVES REFERENCED**

PS 1237.10	Personal Computers Network Standards and Manual (6/18/97)
PS 1237.11	Information Security Programs (10/24/97)
PS 1351.04	Release of Information (12/5/96)
PS 3420.08	Standards of Employee Conduct (3/7/96)

OMB Circular A-130 (2/6/96)
DOJ Security Bulletin 93-04

4. **STANDARDS REFERENCED**

American Correctional Association 2nd Edition Standards for Administration of Correctional Agencies: 2-CO-1F-06

5. **RESPONSIBILITIES OF INFORMATION AND COMPUTER USERS.** The following responsibilities are based upon best practices for protecting the Bureau's Information Resources.

a. **Official Business.** Personal use of Government office equipment such as computers, printers, fax machines, telephones, copiers, and calculators is permitted, if it does not involve more than a negligible cost to the Government.

- Use of such items by an employee in any employment category may occur before or after official working hours or during non-paid meal breaks, provided the use does not adversely affect the performance of official duties by the employee or the Bureau.

Government computer resources are placed at the disposal of all categories of employees to help them more efficiently and effectively carry out the agency's business and to serve the public better. Certain prohibitions are associated with the use of these resources including:

(1) Using the computer for non-work purposes during duty hours.

(2) Accessing external computer systems (such as bulletin boards and the Internet) when the access is not necessary to perform an official duty during normal work hours.

(3) Using government-owned software, information, or equipment including the development of computer programs for unofficial purposes exceeding what is licensed or authorized above.

(4) Accessing Internet sites that impose a cost to the Government or provide sexually explicit, racially degrading, or other material inappropriate for the workplace.

* (5) Storing on government hard drives (or diskettes, directories, or archives)or copying, displaying, generating, recording, transmitting or printing files or data, sending or forwarding E-mail (attachments, photos, information, etc.), from or to Government computers, which could be offensive or inappropriate for the Bureau work environment.

- Including but not limited to, items or descriptions that are sexually explicit or degrading to any other person, as it relates to a person's gender, sexual orientation, race, creed, culture, etc. *

(6) Accessing Internet sites during normal duty hours for other than official business. (It is permissible to access sites, except as noted in subsection (4) above, before or after duty hours or during non-paid lunch periods.)

(7) Sending or re-sending "Chain Letters" via the Internet or BOPNet GroupWise mail or by other methods on Government equipment. Chain letters sent through the U.S. Mail are illegal; using government resources to do so is strictly prohibited by this Program Statement.

(8) Using local area network (LAN) disk space/storage and telecommunications bandwidth by sending attachments consisting of elaborate graphics for unofficial purposes via E-mail transmissions. This activity wastes computing resources, particularly when sent to multiple addresses.

(9) Divulging sensitive Government information to any person who is not authorized to have access to the information.

(10) Leaving sensitive Government information unprotected or accessible to unauthorized persons by leaving a workstation logged onto a LAN without invoking a currently required Bureau approved screen saver with password protection.

(11) Removing sensitive documents (electronic media or paper) from the workplace without proper authority.

(12) Failing to secure "Privacy Act Protected Information," "Limited Official Use," "Extremely Sensitive Information," or classified documents adequately, regardless of the manner in which the information is recorded.

(13) Permitting inmates to use **Staff Only** workstations.

(14) Permitting or having use of, or access to systems which is facilitated through the use of a personal ID and password issued to another person.

b. **Information Access.** Although not all information on personal computer hard drives, file servers, and removable media (diskettes) is considered sensitive (critical to the Bureau's daily operation) or protected because of the Privacy Act requirements, much of the information in electronic systems is vulnerable because once the system is accessed, all information (regardless of sensitivity) is available to the user or a perpetrator.

This level of vulnerability requires that the entire system be protected from unauthorized access. Therefore, employees shall:

(1) Only access systems or data for which the supervisor has determined a need and additionally, have been granted authorization by the system administrator(s).

(2) Not retrieve information (printed or electronic) from a system for someone who does not have authority to access the information.

(3) Only provide information, forms, surveys, etc., to persons who have shown a legitimate official need.

(4) Not provide paid or non-paid employees, contractors, volunteers, or other types of employees with a system USER ID and PASSWORD without proper clearance as defined in the Program Statement on Information Security Programs.

c. **System Integrity.** All systems, whether automated or manual, must provide information to the user quickly, accurately, and reliably. To ensure that the information contained in Bureau systems continues to be responsive, employees shall:

(1) Scan all files and disks for viruses before use and execute virus protection on computer workstations according to procedures defined by local Computer Services Managers (CSM) or policy. Discontinue the use of any computer workstation showing indications of being infected with a virus and notify the local CSM.

(2) Use only U.S. Government, Bureau, Information Security Programs or Office of Information Systems (OIS) authorized software (i.e., personally owned software, shareware, public domain software, or similar programs must not be used unless specifically authorized by the local Information Security Officer). Users are responsible to ensure that all software installed on the hard drives of their workstations comply with licenses, agreements and copyright laws.

(3) Ensure that only authorized and accurate information is entered into information databases.

(4) Protect personal passwords from disclosure and not share them with anybody or ask another person for his or hers for any reason. Exceptions are limited to prescribed circumstances noted in the Program Statement on Information Security Programs.

d. **System Availability.** To protect data and system availability employees shall:

(1) Make backups of critical and sensitive systems and files regularly.

(2) Store backups away from originals and from devices that produce magnetic fields.

(3) Protect disks and equipment from spillage of food and drink.

(4) Know whom to contact for emergencies and significant malfunctions.

6. **OTHER SYSTEM USER RESPONSIBILITIES.** Although all information users have responsibility for system security, some users, because of the uniqueness of their positions, have additional responsibilities.

a. **Local Area Network (LAN) Administrators.** The CSM, LAN Administrator, or other designee at each Bureau location has collateral responsibilities as an Information Security Officer.

A large portion of that responsibility is to protect the operation of the system, the information contained on it, and how it is used.

Personal Use of the LAN is not authorized for any reason while functioning in supervisor or administrator accounts. LAN administrators control the configuration of the local file servers, have access to every file, and can enable and disable all internal and external access controls. Therefore, LAN Administrators shall:

(1) Protect the supervisor or root password at the highest level demanded by the sensitivity level of the LAN system.

(2) Excluding workstations, not develop applications or programs on any part of the LAN system for non-work purposes.

(3) Ensure that adequate administrator training is requested.

(4) Excluding workstations, watch for unscheduled or unauthorized applications or programs running on a recurring basis.

(5) Not permit or facilitate LAN accesses for unofficial purposes.

(6) Safeguard users' LAN accounts against unauthorized access.

(7) Take action to reduce damage caused by security incidents (e.g., lock up property, logout a terminal, or disconnect a PC with a virus from the LAN).

(8) Not abuse the privileges and responsibilities associated with the position by doing anything that would:

- be dishonest;
- breach security; or
- violate the trust bestowed upon the position.

(9) Report any security violations to the Information Security Programs Section, Central Office and to the respective Chief Executive Officer (CEO), within 24 hours of discovering the event. The 24 hour period does not include weekends or holidays, unless the event

is so serious that it would require immediate intervention. Then, the Regional Duty Officer should be contacted and, in turn, he or she shall contact the Central Office Duty Officer about the incident.

(10) Ensure that employees receive adequate and appropriate information systems security training.

(11) Ensure that all software installed on hard drives or systems for which they are responsible is licensed properly.

(12) Test the system contingency plan and document the test results annually and make appropriate modifications to the documents as required.

(13) Apply all security devices, software, system configurations, or other prescribed security measures to the system under his or her management as directed by the Deputy Assistant Director for Information Resource Management or the Information Security Programs Section (ISPS). This should be accomplished within the time frame specified by policies (DOJ Orders, Program Statements or Operations Memorandums) or written instructions (E-mail or memorandums) initiated by the ISPS, unless otherwise authorized in writing.

(14) Not use any software or device that would permit the circumvention of any security measures established to protect data without the CEO's written approval.

(15) Remove any account from the system for any person who has retired, resigned, transferred, or who has been fired.

b. **Users of Public Access Systems.** Users of public access systems such as the Internet, CompuServe, and bulletin boards shall take extra precautions to protect against viruses and system hackers who may try to penetrate a system from the public access system or capture information being received or sent.

Users of public access systems should:

(1) Use these systems for official purposes only except when permitted. Personal use of the equipment and system capabilities such as e-mail or Internet use is authorized during non-duty hours. An "official purpose" implies that the use is for the purpose of

conducting normal Government business which would include such things as communicating with other Government agencies or searching the Internet for sites directly related to one's work and confining one's work to typical tasks associated with the job.

(2) Never transmit "Limited Official Use" or any other sensitive Government information across public access systems (i.e., Internet, telephone lines, etc.) unless the information is encrypted and it has been authorized by the CEO or designee.

(3) Use virus protection/scanning software on every information file and diskette received.

(4) Never use a modem from a workstation connected to a critical or sensitive network, unless the network connection is disabled. The modem must be physically disconnected either from phone lines or the workstation prior to establishing or re-establishing the network connection.

c. **Managers and Supervisors.** Supervisors at all levels of the organization play a crucial role in ensuring that sensitive information is neither accessed nor used inappropriately. The local manager establishes the requirements for an employee to gain access to systems that contain protected information. Managers shall:

(1) Notify the LAN Administrator and Information Security Officer when an employee terminates or transfers to another department or facility.

(2) Counsel all employees on their responsibilities prescribed in this Program Statement and the non-disclosure of sensitive information, including employees leaving the Bureau.

(3) Appropriately restrict access to information by former or retired employees.

/s/
Kathleen Hawk Sawyer
Director