Global Information Assurance Certification Paper

Acceptable Use Policy

1. Purpose. This document establishes policies, assigns responsibilities, and prescribes standards and procedures for the management and use of an Automated Information System security program for the District Office.

2. Authority. This document implements guidance and standards published in: the Office of Management and Budget (OMB) Circular No. A-130, Management of Federal Information Resources Management Regulations (FIRMR) on security, privacy, and automated data processing, telecommunications management, and acquisition, the National Institute of Standards and Technology's Federal Information Processing Standards Publications (FIPS PUBS) dealing with Information System security, and the Office of Personnel Management's Federal Personnel Manual issuance's on personnel security as they relate to Automated Information Systems. The above guidance implements numerous laws dealing with Automated Information Systems security including the Brooks Act of 1965, the Privacy Act of 1974, the Computer Fraud and Abuse Act of 1986, and the Computer Security Act of 1987.

3. Definitions for the purposes of this document:

   - Security. The management controls, operational procedures, and controls established to provide an acceptable level of protection from vulnerability that could result in attacks against confidentiality, integrity or availability of the Automated Information System.
   - Application. Computer programs and routines that run on one or more computers that are designed to accomplish automated tasks in support of administrative or mission oriented functions.
   - Automated Information System (AIS). The combination of computer equipment, operating system software, applications, network functionality, and established methods and procedures designed to collect, process, store, and/or communicate information for the purpose of supporting specific administrative or mission related requirements.
   - Computer/ADP Designated Position. Any position where the duties involve participation in designing, developing, operating, or maintaining sensitive computer installations or applications, as well as those positions requiring access to sensitive data.
   - Personnel Security. The safeguards established to ensure that all personnel who have access to AIS have the required authorities and the appropriate levels of training, computer/ADP position designations, and security clearances.

4. Scope.

- The provisions of this document apply to, but are not limited to Information created, processed, stored, or transmitted by a Federal AIS, Information in any form when used as input to, output from, or documentation of an AIS, AIS installations and facilities used in the collection, processing, storage, communication, and retrieval of information, and all software, operating systems, utilities and application programs, etc. used on the AIS by users of the AIS
- This document applies to users of the AIS including this District's employees, contractors and other organizations, which operate the AIS on behalf of the District and/or the Bureau.
- Since the re-writing of OMB A-130, all Federal Automated Information Systems are now considered sensitive. This means that all Federal systems contain data that require protection due to the risk and magnitude of the loss or harm that could result from inadvertent or deliberate disclosure, alteration, or destruction of the data.
- Sensitive data include proprietary data, records about individuals requiring protection under the Privacy Act, confidential data such as payroll, financial, or management information, or data that is critical to the mission of the Bureau.

5. Policy.

- All Bureau information technology facilities and equipment shall be protected against loss, damage, theft, and misuse, and all data processed by Bureau AIS shall be protected against unauthorized disclosure, modification, or destruction, as well as attacks against confidentiality, integrity and available.
- The level of protection shall be commensurate with the sensitivity of the information created, processed, stored, or transmitted by the AIS.
- Violations of Federal and Bureau regulations and policy pertaining to AIS security will result in appropriate administrative, disciplinary, or legal action against the violators.
- District employees can, when appropriate for their job responsibilities, communicate via E-mail with consumers, other government agency officials, and contractors (as long as the use complies with OMB Circular A-130 requirements for electronic release of agency information), access external databases and files to conduct research, and read E-mail from listserv discussion groups on job-related topics.
- Supervisors shall allow and encourage staff to attend Internet training sessions and to use official time to practice the skills learned in those sessions. It is in the interest of the District to have employees trained in the use of the Internet.
- Employees shall use the Internet responsibly. Employees who use the Internet are required to learn about network etiquette (""netiquette""), customs, and courtesies. Certain procedures and guidelines should be followed when using E-mail communications, participating in E-mail discussion groups, using remote computer services, and transferring files from other computers.
- Employees shall abide by existing security policies, procedures, and guidelines in their use of the Internet, and shall refrain from any practices, which might jeopardize the District's data, network, and systems security. Employees are required to be aware of computer security and privacy concerns and to guard against computer viruses and security breaches of any kind.
- Unless specifically stated, copyright laws prohibit sending or receiving copyrighted materials (including articles and software) via the Internet. Employees are responsible for validating the copyright status of any file requested, downloaded or received before use. All data files and programs MUST be scanned for viruses before being loaded on the District's local area network. Copyright infringement can result in felony convictions.
- Employees will not send, forward or solicit offensive or harassing statements including disparagement of others based on their race, national origin, sex, sexual orientation, age, disability, religious or political beliefs. Sending or soliciting sexually oriented messages or an image is prohibited.
- All employees who are to use, manage, or operate AIS must receive computer security awareness training to ensure that all individuals are appropriately trained in how to fulfill their security responsibilities before allowing them access to the system.

6. The Computer Security Act of 1987 requires periodic training for all employees who are involved with the management, use, or operation of each Federal AIS within or under the supervision of the Bureau. Such training shall assure that employees are versed in the rules of the system, be consistent with guidance issued by NIST and OPM, and apprise them about available assistance and technical security products and techniques. Conduct consistent with the rules of the system and periodic refresher training shall be required for continued access to the system. The training shall be designed to enhance employee's awareness of the threats to and vulnerabilities of computer systems and to emphasize their responsibilities for protecting Bureau information resources and for using these resources in a proper manner. Bureau managers are responsible for ensuring those employees under their supervision who meet the above criteria receive the appropriate level of training. Computer security awareness training shall be documented on the Standard Form 182 and retained in each employee's official personnel folder.

    - Basic Security Awareness training creates a basic knowledge of AIS sensitivity to threats and vulnerabilities and the recognition of the need to protect data, information, and the means of processing them.
    - In Depth training provides sensitive AIS owners/managers, administrators, information technology personnel, and computer security personnel with the abilities to perform risk analyses, design AIS protection programs, implement security measures, or evaluate the effectiveness of existing security programs.

7. District employees are required to use access to the Internet in a responsible and informed way, conforming to network etiquette. Use of the Internet encompasses many different interconnected networks and computer systems. Each system has its own rules and limitations, which are usually explained to a new user along with the electronic greeting. Guests on these systems have an obligation to learn and abide by the rules posted on each system.

8. Use of the Internet is a privilege, not a right, which may be revoked at any time for inappropriate conduct. The District employs procedures for routine monitoring of Internet activities to identify and correct policy violations. Examples of inappropriate conduct include a) use of the Internet for unlawful or malicious activities, including copyright infringements and non-official use b) use of abusive, offensive or objectionable language in either public or private messages c) misrepresentation of oneself or the Department or d) other activities that could cause congestion and disruption of networks and systems (local or remote), including the sending of chain letters.

9. The content and maintenance of a user's electronic mailbox and file storage areas are the user's responsibility. Users should ensure the following:

    - Check electronic mail daily.
    - Use signature blocks or a typed name and e-mail address at the bottom of E-mail messages. Some E-mail systems used by recipient's strip header information from messages, including Internet E-mail address. Appending a signature block to the end of message ensures that the receiver will know who sent it. Signature blocks should be short, preferably not more than six lines, and should include your name and Internet E-mail address at a minimum and, optionally, your work telephone number and postal address.
    - If an E-mail message, which you are sending, contains personal opinions that might be mistaken as Interior or government policy, add a clear personalized disclaimer to the signature block. An example of a personal disclaimer is: The opinions expressed here are my own and do not represent official policy of the Bureau.
    - Be aware that E-mail is not private communication, since others may be able to read or access it. E-mail may best be regarded as a postcard rather than as a sealed letter.
    - Delete unwanted messages or files immediately, because they take up disk storage space.
    - Keep messages stored in electronic mailboxes to a minimum.
    - Transfer to your local hard disk or diskettes for future reference any messages or files to be saved.
    - Maintain file storage areas (your personal directory). Users should keep their files to a minimum, as server storage space is limited. If users utilize excessive server storage, the System Administrator will notify them and ask them to remove files.
    - Check for viruses before using any executable files (especially with DOS file name extensions of .exe or .com) or data, which you receive as attachments to an E-mail message. Do not use infected files and report all viruses to your System Administrator.

10. References.

- The Office of Management and Budget Circular A-130
  http://www.whitehouse.gov/omb/circulars/a130/a130.html

- Management of Federal Information Resources Management Regulations
  http://www.itpolicy.gsa.gov/firmr.txt

- The National Institute of Standards and Technology's Federal Information Processing Standards Publications
  http://csrc.nist.gov/publications/fips/index.html

- The Office of Personnel Management's Federal Personnel Manual issuance's on personnel security as they relate to Automated Information Systems
  http://www.itpolicy.gsa.gov/roadmap.htm

- The Privacy Act of 1974
  http://www.eff.org/pub/Legislation/privacy_act_74_5usc_s552a.law

- The Computer Fraud and Abuse Act of 1986
  http://www4.law.cornell.edu/uscode/18/1030.html

- The Computer Security Act of 1987
  http://csrc.nist.gov/secplcy/csa_87.txt