

## **5 FAM 720 GENERAL POLICIES**

*(TL:IM-39; 06-13-2003)*  
*(Office of Origin: IRM/APR/RG)*

### **5 FAM 721 GENERAL POLICIES**

*(TL:IM-33; 02-27-2002)*

a. Access to the Internet through the Department of State's facilities is for official and unclassified use by authorized personnel. Limited personal use is authorized as described in 5 FAM 723, *Personal Use of U.S. Government Equipment*. The OpenNet is the network for intra-Departmental unclassified and sensitive-but-unclassified (SBU) e-mail, web and other standard client/server computer systems services. Policies regarding the content and usage of e-mail transmitted on Department networks are contained in 5 FAM 750, *E-Mail Policy*.

b. All users of the Internet and Department of State intranets (classified and unclassified) through the Department of State's facilities are required to abide by the security requirements outlined in 12 FAM 600, *Information Security Technology*. For more information, contact the Office of Information Security Technology (DS/CIS/IST).

c. Under 5 FAM 443.5, *Points to Remember About E-mail*, e-mail messages may be subject to the Federal Records Act and/or they may be considered official records. Official business messages shall comply with the requirements of the Federal Records Act.

### **5 FAM 722 RESPONSIBILITIES**

#### **5 FAM 722.1 Chief Information Officer**

*(TL:IM-33; 02-27-2002)*

The Chief Information Officer:

(1) Provides technical policy and related procedural guidance for establishing, operating, and maintaining sites on the intranet and Internet domestically and for locations abroad;

(2) Maintains liaison with the Assistant Secretary for Public Affairs and the Coordinator for International Information Programs to provide policy oversight and guidance to ensure the effective dissemination of foreign affairs information on the Internet;

(3) Serves as the authority for Department wide information systems security programs. In conjunction with this authority, implements and maintains security solutions on worldwide Department networks developed in conjunction with the Assistant Secretary for Diplomatic Security to prevent unauthorized access and tampering;

(4) Provides operational support to all Department bureaus, posts, and tenant organizations to protect Department IT resources from computer virus invasion and to recover IT systems that have been infected by computer viruses;

(5) Develops handbooks and other guidance, as necessary, to direct or assist with intranet and Internet activities;

(6) Evaluates evolving web technologies and tools for deployment on Department sites to improve their efficiency and effectiveness;

(7) Provides host servers and expertise for the ongoing development of the intranet. Maintains intranet servers and develops sites for other Department elements on a fee-for-service basis;

(8) Provides TCP/IP address and network management for all sites. Advises and assists locations abroad in adding their sites to the worldwide network;

(9) Administers firewall protection for Department networks;

(10) Performs operational monitoring of networks to detect unauthorized access and for improper use by employees;

(11) Provides network traffic management in accordance with policies approved by the IT CCB and administered by the Office of Enterprise Network Management. Provides application monitoring of Internet and intranet use; and

(12) Models and analyzes network traffic growth and prepares an annual Network Capacity Plan for the Department which is used for circuit management in cooperation with DTS-PO. Models, tests, and analyzes new bureau enterprise applications for their impact on network performance and capacity. Reports these results to the IT CCB.

## **5 FAM 722.2 Assistant Secretary for Diplomatic Security**

*(TL:IM-33; 02-27-2002)*

The Assistant Secretary of Diplomatic Security:

- (1) Implements the Department's intrusion detection system program;
- (2) Implements a computer security awareness training program, that includes Internet and intranet security;
- (3) Implements and maintains security solutions on worldwide Department networks developed in conjunction with the Chief Information Officer to prevent unauthorized access and tampering;
- (4) Provides consultation on Internet web page development to ensure the content does not violate security requirements contained in 12 FAM 600, *Information Security Technology*;
- (5) Leads the Computer Incident Response Team (CIRT) and is the point of contact for reporting unauthorized activity on Department of State computer systems. Diplomatic Security is responsible for providing incident reports to the OIG and other appropriate offices; and
- (6) Provides computer and communications security evaluations.

## **5 FAM 722.3 Assistant Secretary for Public Affairs**

*(TL:IM-33; 02-27-2002)*

The Assistant Secretary for Public Affairs:

- (1) Operates and maintains the Department of State's web site (<http://www.state.gov>) which is the official primary point of public access to information about the Department and Departmental foreign policy material;
- (2) Provides content and design guidance to Department elements that publish public web pages in order to ensure credibility of information released and to maintain a degree of consistency in its appearance throughout the Department. Approves Internet publication of information in accordance with clearance procedures outlined in 10 FAM 132, *Electronic/Hard-Copy Dissemination*; and
- (3) Works with the Coordinator for International Information Programs on web site content related to public diplomacy programs abroad.

## **5 FAM 722.4 Coordinator for International Information Programs**

*(TL:IM-33; 02-27-2002)*

The Coordinator for International Information Programs:

(1) Operates and maintains the International Information Program home page for the Department;

(2) Provides advice and assistance to missions abroad that set up their own web pages. Serves as the primary point of contact for guidance on content of pages containing material related to the public diplomacy mission; and

(3) In conjunction with the Office of the Legal Adviser (L/PD) and Bureau of Public Affairs, oversees compliance with the Smith-Mundt Act, which prohibits domestic dissemination of public diplomacy program materials the Department has prepared for dissemination abroad.

## **5 FAM 722.5 Department Heads of Bureaus, Offices and Other Elements**

*(TL:IM-33; 02-27-2002)*

Department heads of bureaus, offices, and other elements are responsible to:

(1) Establish a process for identifying information appropriate for posting to the Internet or intranets;

(2) Ensure all information to be placed on public web sites is properly reviewed for security levels of sensitivity and is cleared through the Public Affairs' Office of Electronic Information, as necessary, using Form DS-1837, *Request for Approval of New or Recurring Information Dissemination* (see 10 FAM 132, *Electronic/Hard-Copy Dissemination*);

(3) Ensure appropriate privacy, security, copyright notices and any other applicable disclaimers are used on all web pages under their purview;

(4) Conform to Department security requirements and cooperate with all risk assessments conducted on their web sites;

(5) Provide for regular functional review and management oversight of all web pages under their purview;

(6) Provide resources to adequately support web site operations including funding, equipment, staffing and training; and

(7) Work with A/RPS/IPS to preserve e-mail and other data that qualify as Federal records (see 5 FAM 443, *Electronic Mail (E-Mail) Records* and NARA regulations).

## **5 FAM 722.6 Internet/intranet Site Managers**

(TL:IM-33; 02-27-2002)

The following responsibilities apply to all sites, whether managed internally with Department resources, or by an external Internet service provider. Internet/intranet site managers are responsible to:

(1) Ensure that a system is in place to provide effective day-to-day operation and maintenance of web servers or pages in their control, including making routine backups and contingency plans in the event of external attack or server failure;

(2) Immediately report server anomalies or evidence of unauthorized access to the Computer Incident Response Team (CIRT) and Information Systems Security Officer (ISSO);

(3) Ensure internally hosted sites conform to all Department security requirements. Site managers using external Internet Service Providers should select those that most closely meet Department security requirements and recommendations;

(4) Ensure no classified information or NOFORN (no foreign dissemination) material is published on any unclassified Internet or intranet site and that no SBU (sensitive but unclassified) material is published on the Internet;

(5) Assist users in learning how to use web browser software;

(6) Keep all operating system software, web server, and anti-virus software updated with the latest IT CCB-approved patches, releases, and definitions. In the case of externally hosted sites, encourage the hosting Internet service provider (ISP) to do the same;

(7) Keep web site content current. Remove old pages that are no longer relevant or useful. Routinely verify that links are still valid;

(8) Ensure the Department's Cookie Policy as described in 5 FAM 741, *General Policy*, is enforced; and

(9) Comply with the revised Section 508 of the *Rehabilitation Act of 1973*, on accessibility of web sites.

## **5 FAM 722.7 Intranet and Internet Users**

*(TL:IM-33; 02-27-2002)*

A user is any person who is given intranet and Internet access. Internet and intranet users must:

- (1) Follow e-mail usage policies as outlined in 5 FAM 750, *E-Mail Policy*, and Internet access policies stated in 5 FAM 780, *Internet Access*;
- (2) Ensure that only unclassified data is transmitted via the Internet;
- (3) Appropriately mark the classification of e-mail messages, as detailed in 5 FAM 751.3, *Marking of E-mail*; and
- (4) Abide by the user security requirements outlined in 12 FAM 600, *Information Security Technology*.

## **5 FAM 722.8 Office of Inspector General**

*(TL:IM-33; 02-27-2002)*

The Office of the Inspector General:

- (1) Conducts an annual evaluation of the Department of State's information security program which may include the use of the Internet and intranet, under the Government Information Security Reform Act;
- (2) Investigates misuse of U.S. Government computer resources for personal gain, and the excessive personal use of official U.S. Government computers; and
- (3) Investigates conduct when the Internet and/or Intranet is being used by an employee or contractor of the Department of State in furtherance of a fraud or crime.

## **5 FAM 723 PERSONAL USE OF U.S. GOVERNMENT EQUIPMENT**

*(TL:IM-39; 06-13-2003)*

*a. The following policies, in addition to all relevant laws and regulations, including those relating to copyright, trademark, obscenity, defamation, the right of privacy, false advertising, and fraud, apply to all U.S. Government equipment and all methods of accessing the Internet using U.S. Government equipment. In addition to such laws and regulation, use of U.S. Government equipment and the Internet is governed by the Standards of Ethical Conduct for Employees of the Executive Branch. The*

*definitions in 5 FAM 724, Monitoring and Auditing Procedures, shall apply for purposes of this section.*

*(1) Employees may make personal use of unclassified Department of State office equipment if it involves negligible additional expense to the U.S. Government such as electricity, ink, small amounts of paper, and ordinary wear and tear. Such use is authorized as long as only small amounts of paper are involved and as long as the use does not interfere with official duties.*

*(2) Personal use of U.S. Government classified computers is strictly prohibited.*

*(3) Employees may use the Internet if basic access to the Internet does not result in increased cost to the Department. Employees may use the Internet in moderation, on personal time, for matters that are not directly related to official business. This includes the use of Internet e-mail; however, anyone making personal use of Internet e-mail should make it clear that his or her personal e-mail is not being used for official business. See 5 FAM 751.3 paragraph d.*

*(4) Employees have no expectation of privacy while using any U.S. Government-provided access to the Internet. The Department considers electronic mail messages on U.S. Government computers, using the Internet or other networks, to be government materials and it may have access to those messages whenever it has a legitimate purpose for doing so. Such messages are subject to regulations and laws covering government records, and may be subject to Freedom of Information Act (FOIA) requests or legal discovery orders.*

*(5) Employees must conduct themselves professionally in the workplace and must refrain from using Department resources for activities that may be offensive to co-workers or to the public.*

*(6) The following personal uses of U.S. government equipment and networks are strictly prohibited, regardless of whether the use occurs on or off government premises or whether the use is during or outside normal work hours:*

*(a) Use that results in an additional charge to the U.S. Government. It is the employee's responsibility to be aware whether an additional cost is involved.*

*(b) Use that compromises the security of U.S. Government systems. For example, e-mail attachments sometimes contain a virus or other destructive package. Up-to-date virus protection software must be used. Be particularly wary of ".zip" files, which can contain multiple compressed files (including viruses).*

(c) *Viewing or accessing sexually explicit material.*

(d) *Visiting or subscribing to any Internet-based service (e.g. mailing lists) in violation of any applicable law.*

(e) *Use that involves gambling.*

(f) *Use that generates either personal income or income for any organization with which the employee is affiliated including advertising, conducting a personal business, soliciting clients, and making sales.*

(7) *Personal use of U.S. Government equipment must be restricted to personal time, and must not detract from an employee's performance of official duties. It is the responsibility of each employee to protect and conserve U.S. Government property, and to use official time in an honest effort to perform official government duties.*

(a) *Supervisors are authorized to, and should, limit personal use if it becomes necessary because of cost, time away from official duties, degraded computer or network performance, or other deviation from the letter or spirit of this section.*

(b) *Where non-employees are authorized access to or use of U.S. Government equipment, they must comply with the policies set forth above, as well as all other applicable legal and regulatory requirements.*

(c) *Failure to comply with the provisions in subsection a. may result in a number of corrective actions ranging from minor to severe. For example, employees accessing, distributing, or generating pornography using Department resources are subject to disciplinary action that may include dismissal and/or applicable legal proceedings.*

(d) ***The personal use of U.S. Government equipment and Internet access is a privilege, not a right. It may be restricted or revoked, whenever appropriate, in the interest of the U.S. Government.***

## **5 FAM 724 Monitoring and Auditing Policies**

*(TL:IM-39; 06-13-2003)*

a. *As stated in 5 FAM 723, personal use of Government equipment is a privilege, not a right, and there is no expectation of privacy while using any U.S. Government-provided equipment or access to the Internet. It is imperative that individuals make every effort to maintain the security of the network, comply with all requirements, and act in such a manner that will not bring discredit on the Department. Monitoring and auditing user activity is a means by which the Department can ensure compliance with 5 FAM 723, Personal Use of U.S. Government Equipment.*

*(1) Definitions, roles and responsibilities*

*The term supervisor will refer to the supervisor or higher-level manager of an employee. A supervisor may request an audit of an employee's activities on government-owned communications equipment or networks.*

*The reviewing official makes the decision whether an audit is justified and has the authority to task the systems administrators, Information System Security Officers, and firewall administrators to conduct an audit and report the result.*

*(a) Domestically, the reviewing official function shall rest with the office director or higher; the bureau Executive Director may also serve as the reviewing official.*

*(b) Overseas, the reviewing official function shall rest with the Deputy Chief of Mission at an Embassy, or consul general/principal officer at other posts, or their designee.*

*An employee may be a Department employee in the Foreign Service, Civil Service, or a Foreign Service National; an employee of another government agency authorized to use Department resources; or a contract employee working on a Department contract.*

*Non-employees include all other authorized users; for example, Eligible Family Members at overseas posts. Non-employees will be held to the same standards of use as employees when using government equipment.*

*Firewall administrators will be responsible for reviewing audit logs for e-mail and Internet access as directed by a reviewing official.*

*Systems administrators and/or Information System Security Officers (ISSOs) will be responsible for reviewing content of local workstation files and server files as directed by a reviewing official.*

*Personal use of government equipment is any IT activity that does not support the official business of the Department.*

*b. Continuous monitoring is performed to ensure the integrity of the Department networks and systems. Activities found in the course of continuous monitoring that appear to be in violation of applicable law, regulation, or policy will be referred to Diplomatic Security for investigation (see 12 FAM 600, Information Security Technology), or referred to the employee's reviewing official for action. Continuous monitoring includes but is not limited to:*

*(1) ISSO review of audit logs for security violations as required in 12 FAM 629, General Procedures.*

(2) *Firewall administrator review of audit logs for inappropriate access and use of the Internet.*

(3) *Firewall administrator review of audit logs of electronic communication activity for inappropriate content and/or attachments.*

(4) *System administrator and/or ISSO audit of user workstations to ensure a prescribed configuration is in effect.*

c. *Auditing of an employee's network activity or workstation use, which includes but is not limited to electronic communication, Internet access, local disk files, and server files, may be performed under the following conditions:*

(1) *When there is suspicion that improper use of government equipment has occurred.*

(2) *When the concurrence of a reviewing official has been obtained. The supervisor identifying a need to audit an employee's activity or workstation must explain the reasons for requesting an audit to the reviewing official who has authority to approve the audit.*

(3) *The reviewing official must send a memorandum to whomever performs the audit, authorizing the audit to be conducted.*

(4) *The results of the audit must be returned to the reviewing official who will make a determination whether the reported activities should be referred to Diplomatic Security (DS) for further investigation. Where appropriate, matters may be addressed administratively as described in subsection c.(5), below.*

(5) *Where an allegation of improper use of Government equipment has been substantiated by an audit:*

(a) *An allegation against a government employee will either be addressed administratively within the employee's bureau or all documentation will be forwarded for HR for review and administrative action as described in 3 FAM 4300, Disciplinary Action (Including Separation for Cause (Foreign Service), or 3 FAM 4500, Civil Service Disciplinary and Adverse Actions (Civil Service).*

(b) *An allegation against a contractor will be addressed by the cognizant contracting officer and domestically the bureau executive director or overseas the Deputy Chief of Mission at an Embassy or consul general/principal officer at other posts.*

(c) *An allegation against a non-employee may result in suspension of the privilege to use government equipment and, in some circumstances, may subject the non-employee's sponsor to discipline.*

*d. Should the allegation result in disciplinary action, Department employees have the right to appeal as described in 3 FAM 1580, Processing Mixed Case Complaints. Employees of organizations other than the Department should refer to their own organizations for appeals procedures.*

## **5 FAM 725 THROUGH 729 UNASSIGNED**