

FEDERAL COMMUNICATIONS COMMISSION Washington, D.C. 20554 FCC DIRECTIVE	FCC DIRECTIVE	
	FCCINST 1479.3	
	Effective Date: July 2008	Expiration Date: July 2013

TO: All Employees and Contractors

SUBJECT: FCC Information Security Program

1. PURPOSE

This directive establishes policy and assigns responsibilities for assuring that there are adequate levels of protection for all FCC information systems, the FCC Network, applications and databases, and information created, stored, or processed therein.

2. CANCELLATION

This directive supersedes FCCINST 1479.2, FCC Computer Security Program Directive, dated October 2, 2001.

3. TITLE

FCC Information Security Program

4. BACKGROUND

This document addresses issues relating to all aspects of computer systems security, including issues concerning day-to-day security safeguards, business continuity, system accessibility and authentication, software licensing, and administrative precautions, which can be taken by users of the FCC computer systems and those who manage them.

5. SCOPE & APPLICABILITY

The provisions of this directive apply to all FCC staff made up of federal employees, contractors, temporary staff, and interns, to include telecommuters (herein referred to as FCC users) who use an information system or access computer generated data to collectively conduct business on behalf of the FCC. This directive discusses safeguard measures to be taken for computer related information systems processing or containing sensitive and Commission critical data. The directive should also be used as a minimum standard for safeguarding other non-sensitive information processed or stored on FCC computer equipment.

6. AUTHORITIES

This directive fulfills the requirements of Office of Management and Budget (OMB) Circular A-130, Appendix III, Federal Information Security Management Act of 2002 (FISMA) (Public Law 107-347), and other applicable guidelines and laws.

7. POLICY

FCC information systems are for FCC authorized purposes only. As noted in the FCC network login banner, users shall have no expectation of privacy. Administrative, audit, and investigative efforts may result from inappropriate system use. All information within FCC systems is subject to access by authorized FCC personnel at any time. Additional system usage such as Internet and e-mail are discussed under Section 25 and 26 respectively. FCC users must not process or store national security classified data on FCC information systems, unless specifically authorized by both the Security Officer (SO) and the Computer Information Security Officer (CISO) in accordance with FCC Directive 1131.

The FCC will protect its information and information systems (IS) from threats to confidentiality, integrity, availability, accountability, and authenticity. The FCC will implement and maintain an Information Security Program (ISP) that ensures adequate protection for all information and information systems that collect, process, transmit, store, or disseminate information. The ISP must include as a minimum, adequate and appropriate levels of protection for all information system resources within the organization, including hardware, software, physical and environmental facilities that support information systems, telecommunications, administrative, personnel, and data.

FCC information and information technology (IT) resources must be protected in a manner commensurate with the sensitivity, value, and criticality of the assets involved. Such protection includes restricting access to information based on the need-to-know.

Management must devote sufficient time and resources to ensure that information is properly protected. FCC and information systems must be reviewed every three years or following a significant change to a system. Similarly, whenever a major security incident indicates that the security of information or information systems is insufficient, management must promptly take remedial action to reduce the FCC's exposure. Periodic timely reports reflecting the FCC's information security status and progress must be prepared and submitted to the OMB.

All FCC users must be provided with sufficient training and supporting reference materials to allow them to properly protect and otherwise manage FCC information assets. FCC training materials should communicate the importance of information security.

8. RESPONSIBILITIES

8.1 *Managing Director, FCC*

FCC's Managing Director shall designate a senior official to have the primary responsibility for managing the Commission's Information Security Program.

8.2 *Chief Information Officer (CIO), Information Technology Center (ITC)*

The Chief Information Officer shall perform the following duties:

- Assign and direct a person responsible for managing the FCC's Information Security Program.
- Evaluate and approve the resolution of issues related to information security.
- Designate a chief information security officer.
- Develop and maintain an agency wide information security program.
- Develop and maintain information security policies, procedures, and control techniques to address all applicable requirements, including those issued under FISMA section 3543, and Section 11331 of Title 40;
- Train and oversee personnel with significant responsibilities for information security with respect to such responsibilities; and
- Assist senior agency officials concerning their responsibilities of FISMA 3544 paragraph 2.

8.3 *Chief Information Security Officer (CISO), FCC*

The CISO is responsible for establishing, maintaining, directing, and coordinating implementation of this directive and for assisting FCC management and other FCC users with the development of procedures conforming to this and other related directives. Further, the CISO will ensure that appropriate technical and administrative safeguards are in place, and complied with, to ensure an adequate level of security for FCC information systems. To support this effort, the CISO shall:

- Carry out the CIO's information security responsibilities;
- Possess professional qualifications, including training and experience, required to administer the information security functions of CIO;
- Head an office with the mission and resources to assist in ensuring agency compliance with this section as the primary duties;
- Develop plans for providing adequate information security for networks, facilities, and systems or groups of information systems, as appropriate;
- Conduct periodic assessments of the risk and magnitude of the harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the agency;

- Develop overall Commission-wide Information Security policies and procedures that ensure compliance with current applicable laws and regulations;
- Conduct Certification and Accreditation (C&A) of major and minor FCC applications and general support systems to include certifying, as appropriate, that information system security and associated security safeguards comply with this directive, Federal regulations and related mandates prior to implementation in a production processing environment;
- Develop plans and procedures to ensure continuity of operations for information systems that support the operations and assets of the agency;
- Conduct periodic testing and evaluation of the effectiveness of information security policies, procedures, and practices, to be performed with a frequency depending on risk, but no less than annually as applicable by current laws and regulations of which such testing as outlined in FISMA 3544(b)(5);
- Refer to the Office of Inspector General cases of unauthorized use as appropriate;
- Maintain inventory of major information systems as outlined in FISMA sec. 305;
- Develop a process for planning, implementing, evaluating and documenting remedial action to address any deficiencies in the information security policies, procedures, and practices of the agency; and
- Develop reporting structure to monitor occurrences of security breaches, incidents, issues, and threats; and
- Review and approve or deny user requests to reconfigure desktop security settings.

8.4 ITC, Network Operations Group

The Network Operations Group (NOG) will assist with the implementation of this directive and its policy and standards. To support this effort, NOG shall:

- Coordinate with the CISO to establish and maintain procedures, which will ensure the security and integrity of respective FCC information systems. Procedures should provide adequate safeguards for processing and storing sensitive data and limiting access to systems, therein;
- Document event(s), and immediately notify the CISO, whenever a known or possible breach of IS security occurs;

- Take all reasonable steps to ensure that information processed, stored or in transit on FCC computer systems is kept secured while on the FCC network;
- Ensure that all file server system management account passwords adhere to Federal mandates and guidelines (Presidential Directives, NIST, OMB, and best practices), and that passwords are provided only to persons with a bona fide need-to-know;
- Establish written file and database server backup policies and procedures and ensure that they are followed;
- Periodically review FCC computer system servers and workstations to ensure that only authorized software is installed; and
- Oversee and maintain the FCC IT Change Control Board (CCB) process to ensure all changes to the FCC network infrastructure are reviewed, tested, and approved before implementation.

8.5 *ITC, Network Development Group*

The Network Development Group (NDG) will assist with the implementation of this directive and its policy and standards. To support this effort, NDG shall:

- Develop and implement appropriate administrative and technical procedures to conform to this directive, and other related Federal regulations, and FCC directives and policies;
- Compile and maintain a FCC computer system topology diagram which clearly illustrates the entire network, including server locations, communication links, firewalls, and all other related network components maintained by the ITC;
- Process change control requests and report results to CCB;
- Ensure that all system routers and firewall passwords are changed at a minimum of every 90 days, or more frequently as required, and that passwords are provided only to persons with a bona fide need-to-know;
- Coordinate with the CISO in the development and testing of contingency plans, and provide assistance on the conduct of network risk analyses;
- Identify and recommend security solutions and safeguards for use on the FCC Network in order to avert or minimize potential security vulnerabilities;

- Ensure that system audit logs and other available system management reports are accumulated and reviewed. Activities that show potential misuse should be forwarded to the CISO for consideration;
- Maintain the operation of ITC-managed firewalls, routers, and other network devices, and implement appropriate security policies on firewalls and ITC managed routers; and
- Ensure the integrity and security of ITC-managed firewalls and routers.

8.6 *ITC, Applications Integration Group*

The Applications Integration Group (AIG) will assist with the implementation of this directive and its policy and standards. To support this effort, AIG shall:

- Provide Bureau/Office assistance to develop application(s) and database(s) that comply with this directive and other related federal mandates and policies;
- Provide assistance to the CISO to ensure that appropriate security reviews are conducted on FCC applications and servers prior to being utilized in a production environment;
- Ensure the security and integrity of production servers, databases and Internet application servers under AIG control;
- Configure systems to meet security requirements; and
- Periodically review production systems to verify compliance with security requirements and fix any discrepancies.
- Submit change requests to the Change Control distribution list. The requests are then added as an item for review at the next Change Control meeting.

8.7 *Bureau/Office Application Custodians/Managers*

Application Custodians/Managers are those Bureau/Office representatives who have the responsibility to manage respective sensitive and mission critical applications, databases, and/or information systems. Application Managers should comply with and implement the policies, standards and goals of this directive. They are also responsible for ensuring the development, administration, monitoring, and enforcement of internal controls, application systems security plans and continuity of operations plans, and incident reporting processes. Bureau/Office Custodians/Managers should contact the CISO or designee for technical support in the development and implementation of their policies, standards, and goals, as needed. To support the effort, Bureau/Office Managers shall:

- Identify sensitive and mission critical systems, applications and databases, and files within their functional control and inform ITC of such information;
- Ensure that respective computer systems are used exclusively by authorized FCC users for the performance of official Commission business and that equipment is secured to prevent unauthorized use and theft;
- Ensure that Sensitive and Privacy Act data are only released outside of the Commission with the approval of the Performance Evaluation and Records Management (PERM) Privacy Officer;
- In accordance with OMB M-06-16, *Protection of Agency Sensitive Information*, monitor user requirements to ensure that only required system access privileges are granted to perform current job responsibilities. Authorize controlled physical removal of personally identifiable information when required for job performance;
- Ensure that respective computers systems follow the system backup policy;
- Develop a System Security Plan, in concert with the ISP, for applications for which they are responsible;
- Work with the CISO to ensure that required level of Information Security is put in place for each application, including contacting the CISO at appropriate points in the Systems Development Life Cycle (SDLC);
- Report any and all security incidents to the CISO or designee;
- Monitor respective systems for potential misuse and security threats;
- Authorize access to computer resources (FCC Form A-200) and perform a review of user access privileges every 6 months;
- Educate managers and users on control and protection requirements for computer systems and information;
- Implement Interagency Security Agreements, Memorandums of Agreement, and Memorandums of Understanding documents with external entities which their systems share data in accordance with NIST Special Publication 800-47; and
- Monitor compliance with established FCC security directives, Federal regulations and other applicable mandates, and periodically review control processes.

8.8 *OMD, Performance Evaluation and Records Management*

The OMD, Performance Evaluation and Records Management (PERM) office is responsible for overall coordination of the Commission's programs mandated by 44 USC 3101 et seq (Records Management), the Freedom of Information Act (FOIA) as amended, the Privacy Act of 1974 (PA) as amended, and the section of the E-Government Act of 2002 requiring Privacy Impact Assessments. Each of these programs may, and often do, impact information security activities across all FCC information system platforms. To carry out its coordination responsibilities, PERM is responsible for ensuring that the policies and procedures identified in the following Commission directives are appropriately implemented by the parties identified:

- FCC INST 1110.1 - Records Management
- FCC INST 1113.1 - FCC Privacy Act Manual
- FCC INST 1179.1 - Freedom of Information Act Requests

8.9 *Security Operations Center, Administrative Operations*

The Security Operations Center, Administrative Operations is responsible for:

- Arranging background checks for FCC users in sensitive computer related positions as required by applicable regulations;
- Ensuring adequate physical security for locations containing FCC information systems and communications devices used to support the FCC information technology function; and
- Granting badge access to key FCC and ITC spaces based on need-to-know criteria and management approval, and
- Coordinating efforts with Law Enforcement entities on security breaches, incidents, issues, and threats.

8.10 *Contracting Officer*

The FCC Contracting Officer shall:

- Ensure that qualified persons are assigned as Contracting Officers Technical Representatives (COTRs) for each task involving the management, development, or modification of FCC computer systems and information, therein; and
- Ensure that each Statement of Work (SOW) and task order comply with this directive and other related FCC and federal mandates and that all SOWs issued on behalf of the FCC include criteria to require compliance with this directive and related FCC and federal mandates.

8.11 Contracting Officers Technical Representative (COTRs) Responsibilities

The COTR shall:

- Ensure that each Statement of Work (SOW) regarding information systems and information solicitations contain appropriate language to ensure compliance with this directive and related FCC and federal mandates; and
- As deemed necessary, select an onsite Contractor Representative (to fill the role of Contractor Security Representative) who shall:
 - Coordinate all information system security procedures through the COTR;
 - Ensure compliance with all FCC's information security directives, and related Federal regulations and mandates; and
 - Maintain a current list of names and telephone numbers for or off-site contractors working on FCC contracts, which require access to FCC information systems. In addition, ensure that a copy of each listing is provided to the CISO.

8.12 Assistant Bureau Chief for Management (ABC) Responsibilities

Each ABC shall:

- Coordinate with CISO to manage FCC users signing Rules of Behavior, FCC Form A-201.

8.13 Authorized Network/Workstation System Users

An informed, educated, and alert user is a crucial factor in ensuring the security of FCC's information systems and sensitive information resources. To support this effort, users shall:

- Be aware of, and understand responsibilities to comply with this and related FCC directives;
- Recognize the accountability for all activity taking place with the assigned userID and associated account(s);
- Use FCC information system resources only for lawful and authorized FCC business purposes, and access FCC computer systems and information only when a bona-fide business purpose exists;
- Ensure that computers are not used to generate or send harassing or slurring messages, or similar graphical images;

- Change passwords on assigned accounts every 90 days, at a minimum.
- Use a password protected Screen Saver when leaving a logged-in workstation unattended;
- Comply with safeguards, policies, and procedures that prevent unintentional or deliberate access to FCC information systems by unauthorized persons;
- Comply with the terms of software licenses and only install licensed software that is authorized for use at the FCC (see Section 18.1.1 Installing Non- FCC Standard Software on FCC Computers;
- Ensure that appropriate forms pertaining to FCC information systems access and use of resources are completed and submitted;
- Promptly report known or suspected unauthorized use of computer resources, disclosure of user ID's and/or passwords, or violations of this directive to the CISO; and
- Attend annual mandatory FCC Information Security Awareness Training.
- Not reconfigure desktop security settings without approval from the CISO.

9. MAINTENANCE

The FCC Information Security Program policy is intentionally written at a high level and is intended to be generic enough to apply across the FCC. Over time, additional controls and standards will inevitably be required. These will be added, as needed, according to priorities, legislative, or other legal requirements. The additions will be accomplished through published policy papers which will be available on the ISP web page until the next revision of this document, at which time they will be incorporated, if still applicable.

10. PENALTIES

Disciplinary actions for noncompliance with this policy will be handled in accordance with FCC Human Resource Personnel policies. In the case of a serious offense where a formal action may be taken, supervisors should consult with the Office of Inspector General and the Human Resources Office immediately.

11. SEPARATION OF DUTIES

In order to prevent anyone from having end-to-end control over any sensitive, critical, or financial process, all FCC Bureau/Office's (B/O) must maintain a clear separation of duties in positions of authority over matters of security, payroll, budget, and personnel in accordance with MC-006, Separation of Duties Policy 2. The objective is to prevent anyone from having end-to-end control over any sensitive, critical, or financial process such that they could initiate a fraudulent transaction, approve its execution, and subsequently eliminate any record of the

action. Where separation of duties cannot be implemented, controls must be established to monitor activities in an effort to mitigate risk of inappropriate actions.

12. PERSONNEL SECURITY AND SUITABILITY REQUIREMENTS

As mandated by Executive Order 12968, Executive Order 10450, OPM, 5 CFR 731, and HSPD-12 the FCC must conduct personnel security and suitability investigations. Each FCC User will be classified as a High, Moderate, or Low Risk according to level of access to the respective systems. Background checks will be conducted to ensure compliance with Federal Mandates.

- FCC management must incorporate the security functions for the individual role within the position description.
- Users must successfully pass a minimal background check and sign an FCC Form A-201, Rules of Behavior form before system administrators grant them access on any FCC system.
- For each Federal employee and contractor, the background investigation required will be commensurate with the sensitivity level assigned to the position.
- Default Privileges. FCC employee access privileges must be assigned such that only those capabilities necessary to perform their assigned tasks are granted.
- User Separation. Where control systems provide the ability to separate the activities of different users, these facilities must be implemented. For example, systems must employ individual User IDs and passwords to differentiate the activity, communications, and files of different users.

13. USER ACCOUNTABILITY

Users are responsible for all actions and activities performed using their userID on FCC networks, systems, and applications. Accountability is fundamental because many security services and mechanisms rely on the accurate identification of individuals and computing resources.

- Each user shall have a unique individually assigned User ID and user-assigned logon password.
- Computer users interacting within the FCC computing and communications environment must be uniquely identified and held accountable for actions they perform.
- Multi-user systems must maintain logs of processing activity to facilitate transaction tracking to an identifiable individual or entity. Accounts shared by multiple personnel require approval by the CISO.
- Except where required for specifically authorized batch and other systems IDs, individual passwords must never be shared or revealed to anyone else besides the authorized user.

13.1 Password Controls

The following are standards on password use and construction for access to FCC computer systems:

- Users forgetting their password and requiring the password to be reset, will report to the Computer Resource Center (CRC) and show their badge for proper identification, prior to the CRC resetting their password;
- Remote users requiring password-reset will call the CRC and provide appropriate identification;
- Passwords must contain at least twelve alphanumeric characters including special character(s);
- Passwords may not be reused within a twelve month period;
- A unique userID and password (only known by the user), must be used to access FCC computer systems;
- User passwords should be changed at least every 90 days;
- System Administrator passwords should be changed at least every 60 days; and
- A new password must be established, and the user must immediately contact their supervisor or COTR and the Information Security Officer when a password has been, or is believed to have been, compromised.

14. INFORMATION SECURITY PROGRAM

FCC ISP shall establish an information security program that includes processes where FCC information systems within their scope of authority are reviewed, tested, evaluated and certified and accredited. These processes are required by Federal regulation. The processes must be an independent validation and verification of security controls, documented, and determines potential risk, security baselines are being met and to ensure appropriate, cost-effective safeguards are incorporated on all new and existing systems, networks, and facilities. The minimum requirements for performing risk assessments on computing systems, networks, and facilities are as follows:

14.1 Information Security Categorization Assessment

System Owner's must conduct an information security categorization assessment during the initiation phase of a system's life cycle. The type of information collected, processed, and stored shall be identified and categorized, at a minimum, using criteria outlined in National Institute of Standards and Technology (NIST) Federal Information

Processing Standards (FIPS) 199. The results determine the impact to the agency should the information be compromised, which in turn indicates the minimal security controls required to protect the information.

14.2 Selection of Security Controls

Applications, and systems, should meet the minimal security control baselines recommended by NIST. Exceptions will be considered on a case by case basis by the FCC's Information Security Officer. Where possible, all computer and network security measures should be simple and easy to use, administer, and audit. For all business application systems, systems designers and developers must consider security from the beginning to the end of the system's life cycle.

15. ACCESS TO FCC NETWORKED RESOURCES

FCC network security requirements must be balanced against the needs of client agencies to legitimately access FCC networked resources. To protect internal resources, and prevent spoofing, firewalls should enable extensive management control over the availability of services, unauthorized access, and IP address translation. (For Remote Access or Telecommuting Security, see FCCNet Remote Access IT Security Requirements, Version 1.1)

15.1 Mandatory Controls

The following operational guidelines shall not be violated:

- Firewalls shall be employed to deny all services except those specifically granted;
- TCP/IP address spoofing controls shall be activated at all times;
- Ping and WWW requests from un-trusted networks shall not be honored;
- New firewall modification requests (e.g., conduits) shall be made in writing, verified, and approved by the Change Control Board (CCB);
- Firewalls shall be configured to log traffic of a suspicious nature. The log shall be reviewed daily. Incident reports shall be generated as necessary;
- Firewall security logs shall be protected such that no individual user can write to or modify the contents of log files, regardless of the storage media involved. Firewall security logs shall be backed-up with sufficient frequency to ensure that no security log is ever overwritten before being archived. *Firewall security log archives (tapes or other media) shall be retained for a period of no less than 180 days;*

- Unauthorized intrusions into the FCC internal network by trusted sources may result in the immediate termination of the conduit (access path). The decision to terminate connectivity is at the discretion of the FCC CIO or the designated deputy;
- Two firewall administrators (one primary and one secondary) shall be appointed at each FCC site and shall be responsible for upkeep and maintenance of the firewall(s). Individuals assigned the task of firewall administration must have proficient hands-on experience with networking concepts, design, and implementation to ensure the firewall is configured correctly and administered properly. Firewall administrators should receive periodic training on the firewalls in use and in network security principles and practices; and
- Firewall administration is allowed only from within the FCC internal network.

15.2 VPN - Specific Security Requirements

The Virtual Private Network (VPN) point is a common connection point for approved business partners' wide area networks or remote FCC staff users. It allows Bureaus and Offices to exchange appropriate information with external business partners, government or commercial, over a virtual private network Internet connection. The following requirements apply to the VPN environment:

- a. The FCC network must have the proper security controls in place to restrict inappropriate and unauthorized access to and from the VPN. These controls are enacted by configuring network hardware and software to deny access to all traffic to and from the VPN unless expressly permitted. At a minimum, firewalls or routers with access control lists must be used to secure the connection. Using "stateful" firewalls is highly recommended.
- b. Access control lists (firewall rules) must be actively managed and be very specific to limit the traffic flow to meet specific business needs. The reason(s) for any rules that provide access to internal FCC resources from the VPN must be documented. The documentation must be included in the FCC network (FCCNET) security plan.
- c. All computing resources accessing or accessible from the VPN must be fully patched and properly configured to reduce the risk of compromise. Tools such as the Microsoft Baseline Security Analyzer or the Center for Internet Security scoring tool must be used on a regular basis (at least annually) to verify the security configuration on the computers. As with other security weaknesses, the FCC is responsible for managing and remediation of vulnerabilities. Remote components not meeting the baseline patch and configuration requirements will not be allowed to connect to the FCC network through the VPN.

15.3 *Operational Requirements*

Any client or other entity requesting access through an FCC firewall or the VPN must complete a *Network Access Request* before modifications are made to the security parameters of the affected firewall(s). The completed request will contain requesting client point of contact information, client network information, and a brief explanation of why the access is required. The request must be approved through the change control process.

It is important that the operational procedures for firewalls and the configurable parameters be well documented, maintained current, and kept in secure locations (including off-site copies for disaster recovery purposes).

15.4 *Modems/ISDN/DLS Connections*

Modems/ISDN/DLS connections to office desktop PCs are not permitted except in rare instances that must be approved on a case-by-case basis, based on business need and an assessment of risk. Mobile and telecommuting computers (i.e. desktops, laptops, notebooks) are an exception to this rule; however, use should be documented through the user's appropriate Bureau/Office and NOG. FCC user needing to make connections with remote computers must route their connections through the FCC network.

Modems in the server environment may exist only for purposes of vendor troubleshooting, etc., must only be activated for specific times when vendor software maintenance or trouble-shooting has been scheduled. Such modems require the vendor to logon with a User ID and password, regardless of the platform involved. Device default User ID and passwords are not authorized and must be changed meeting ID and password requirements (when capable). The vendor ID shall be limited to only those directories, files, programs, and services required for them to perform maintenance and trouble-shooting. All online activity by vendors shall be logged in the system security log files. When the maintenance or trouble-shooting session is completed, the modem must be disabled to prevent its use by anyone else including the vendor.

15.5 *Wireless Security*

Transmission of sensitive information using any wireless device is generally prohibited. Transmitting FCC sensitive information is allowed only when necessary, by secured means and through officially approved channels. FCCINST 1139, *Management of Non-Public Information* states, unauthorized disclosure of non-public information is prohibited by the Commission's rules, and those rules set forth the procedures under which non-public information may be publicly disclosed.

- All FCC-owned desktops, laptops, and other networking devices must be configured to only maintain one IP address at a time. This is to prevent unauthorized bridging of networks by hosts with multiple interfaces.

- Laptops without an active wireless connection may be synchronized with an FCC computer while it is logged into the local area network.
- Laptops with an active wireless connection may not maintain wireless connectivity (e.g., be connected to the internet or to a wireless service) while the laptop is connected to an FCC-managed computer that is connected to the network.
- If the wireless capability can be disabled, the laptop may be connected while the service is disabled.
- If the wireless connection cannot be disabled, the laptop cannot be synchronized to an FCC-managed computer that is physically connected to the FCC network. The computer must be physically unplugged from the network before synchronization with the laptop can begin.

15.6 Establishing Networks

FCC users must not establish electronic bulletin boards, LANs, modem connections to existing internal networks, or other multi-user systems for communicating information without the specific approval of FCC management. Firewalls will be used to control communications between internal FCC networks and external (e.g., public Internet, vendors, other Government agencies, and Bureaus/Office etc.) networks.

15.7 Non-FCC Issued Equipment Internal Network Access Policy

Contractors and/or vendors are only allowed to connect non-FCC issued equipment to the FCC network once permission has been granted. The Bureau/Office must designate a person to be the Point of Contact (POC). The POC acts on behalf of the Bureau/Office, and is responsible for those portions of this policy that pertain to it.

All non-FCC issued equipment connecting to the internal FCC network will go through a security review by ISP. The reviews are to ensure that all access matches the business requirements, the principle of least access is followed, that the operating system contains all the latest security patches, and that local workstation anti-virus and anti-spyware definitions are current. Network traffic of the equipment may be monitored while it is connected to the internal FCC network. Additionally, if a vendor is troubleshooting an application, they will be accompanied and watched by the Bureau/Office POC while performing the task. In no case will the Bureau/Office POC rely upon the vendor to protect FCC's network or resources.

Change Control for Internal Network Connectivity and Access

Request for internal network connectivity for non-FCC issued equipment must be accompanied by a valid business justification, and is subject to security review. This should be implemented via the FCC change management process. The Bureau/Office is responsible for notifying ISP if there is a material change in the originally provided information so that security and connectivity evolve accordingly.

Terminating Access

When access is no longer required, the BO POC must notify ISP.

Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

16. PHYSICAL SECURITY & COMPUTER EQUIPMENT HANDLING

The offices and work areas where FCC computer systems are located must be physically secured at all times. FCC Information systems must be physically protected commensurate with the sensitivity and criticality of data processed. Offices and rooms or buildings, such as data centers, must use appropriate devices to enforce physical access control. To prevent unauthorized attempts to intercept and capture traffic across transmission lines, wiring closets and other areas that contain network cabling and electric power service cables must be secured at the same level as the areas housing the systems hardware.

Access control lists will be reviewed and updated on a periodic basis. A procedure will be implemented to immediately deny access to individuals who are terminated or, at the discretion of management, are the subject of adverse personnel actions. Encryption, fiber optic cable, or (in the case of copper wire) a protected distribution system composed of sealed conduit, will be used when the risk of interception of sensitive data is great. Laptop computers, PDA, Blackberries, and other portable computing devices, and magnetic or optical media that contain Non-Public-Highly Sensitive/Restricted or "Non-Public-For Internal Use Only" data, shall not be left unattended, in plain view, in vehicles, hotel rooms, or uncontrolled offices. It is recommended that each bureau and office management establish controls that include any or all of the following:

16.1 Critical and High Value Equipment

Wherever possible, LAN, Internet, client, servers, or other high value equipment supporting FCC applications must be housed in areas or enclosures that offer a high degree of physical access control. These areas shall be protected by surveillance-class camera and audio recording monitoring appliances cameras and electronic entry controls. Only those hardware maintenance or system administrators who require physical access in order to perform their duties should have keys, cipher-lock codes, or cardkey permissions to access these areas.

16.2 Area Access Controls

FCC users have a responsibility to create and maintain a secure work environment, and to protect the computer assets used to fulfill business activities. Only authorized FCC users should have access to areas where computer resources, processing sensitive or mission critical FCC information, are housed. Authorization to controlled areas should be granted, and removed when applicable, on a "need- to-access basis." Access to

offices and work areas, where FCC information and computer resources are located, should be controlled in a manner that permits access only to authorized persons. System-provided mandatory *Screen Saver* and associated password are imposed for each user of FCC computer resources.

16.3 *Equipment Custodian and Relocation*

The primary user of IT equipment (including backup tapes), is considered to be a custodian for the equipment. If the equipment has been damaged, lost, stolen, borrowed, or is otherwise unavailable for normal business activities, a custodian must promptly inform the involved FCC Bureau Chiefs and the property manager. Microcomputer equipment must not be moved or relocated without the knowledge and approval of the involved Bureau Chief and ITC's Network Operations Group (NOG). It is important that secure methods be employed to safeguard equipment and the information it may contain during relocation; therefore, all relocations shall be coordinated through NOG.

16.4 *Preventing Information or Hardware Theft*

Information and computer equipment must be protected against theft. Loss of certain information, if not properly backed-up, can require significant effort to recreate. Significant repercussions may ensue if the lost information is subject to FOIA or Privacy Act compliance or has a business or economic impact. It is recommended that Bureaus and Offices management select and implement security controls that employ any or all of the following measures to prevent theft:

- *Do not* store critical or sensitive data, files, or programs on any workstation's local drive. Rather, store such information on the local file server (e.g. N:\ Drive, My Documents folder). As deemed necessary by each user, periodically backup any files stored on the local computer's drive to diskette and store in a safe and secure location.

- Work and storage areas housing computer resources should have locked doors, cabinets, or desks in use. When computer hardware storing sensitive or mission critical information is not secured by a locked door, it should be secured with equipment enclosures and/or lock-down devices. Accessory equipment like modems and external disk drives should be secured in a similar fashion.

- Implement the use of federal government approved encryption to protect sensitive or mission critical information on computing resources that may be susceptible to theft or loss.

- Adhere to the other guidance provided in FCCINST 1139, *Management Of Non-Public Information* for business sensitive correspondence, other printed information and magnetic media.

16.5 *Removable Information Media*

Removable media (e.g., Thumb Drives, external storage devices, tapes, CD-ROM, DVD, Zip disks, floppy diskettes, etc.) allow for the storage of large amounts of sensitive data vital to the FCC mission. Depending on the potential exposure of information residing on removable media, managers should establish any or all of the following controls:

- Ensure that FCC users understand the significance of sensitive information contained on removable media. Additionally, advise FCC users of their responsibility to protect information on removable media as protection of this information would be required in other formats.
- For information that must be stored on removable media; implement the use of federal government approved encryption to protect sensitive or mission critical information that may be susceptible to theft or loss. For information stored on removable media that is removed from or accessed outside the agency or is stored at a remote site, federal government approved encryption is required.
- Discard hard-copy information in a secure manner that prohibits the information from being retrieved and made use of by unauthorized persons.
- Develop procedures to ensure that sensitive information is not stored on diskettes unless the diskettes are properly labeled and stored in a lockable unit in an access-controlled environment.

16.6 *Mobile Device Security*

Mobile, also called portable, devices consist of small computing devices that have the ability to store, exchange and process a significant amount of data while providing convenience and productivity gains. These devices include, but are not limited to, notebook computers, tablet PCs, Personal Digital Assistants (PDA), and mobile phones. With mobile computing resources there are increased risks of theft and loss of information. The Security guidelines outlined in the Management of Non-Public Information (FCCINST 1139) and Privacy Act Manual (FCCINST 1113.1) are particularly binding when using mobile devices. Specific precautions should be taken in the transmission and storage of sensitive FCC information on mobile devices. For the issuance and use of mobile devices:

- FCC staff shall be provided and be familiar with this directive;
- The CISO shall approve all mobile device types deployed;
- FCC will provide mobile devices to FCC users for "Official FCC Use Only";
- Users shall only use the mobile devices for "Official FCC Use Only";

- FCC mobile devices supporting the capability shall, when technically feasible:
 - Have approved anti-virus software installed and maintained;
 - Have access controls that allow for passwords in accordance with this document;
 - Have controls to restrict the device to be home to more than one network, including WiFi, Bluetooth, and infrared, while connected to the FCCNET; and
 - Have an inactivity time out capability requiring user re-authentication.
 - Install anti-theft hardware on equipment deemed as critical or high risk.
- All FCC sensitive data on mobile devices must be encrypted in accordance with OMB Memorandum M-06-16;
- An inventory of mobile devices and peripherals assigned to Bureau and Office (B/O) employees must be maintained to ensure that all pertinent information is included in the Master FCC Inventory database;
- Ensure FCC inventory labels are properly affixed prior to issuance;
- Provide FCC users with emergency contact information;
- *Do not* use FCC mobile devices to generate, send or store harassing material, pornography or similar text, video, or sound files;
- *Do not* process or store Classified National Security information on FCC mobile devices;
- Users should not connect FCC issued computing devices to non-FCC networks or Internet service providers (ISP) without properly configured anti-virus and firewall software;
- Return mobile and other peripheral devices to assigning office when requested; and
- Attend Security Awareness Training provided by the FCC ITC.

16.7 Personal Use of FCC Office Equipment

FCC users may use FCC office equipment only for official business or as otherwise authorized by the FCC. Refer to the FCC Information Security Program Policy, which authorizes limited personal use of certain FCC property under circumstances including, but not limited to when it occurs on non-business time, does not interfere with official business, is not a commercial gain activity or is otherwise prohibited, and the expense to the FCC is negligible.

The following limited personal uses of FCC office and library collections are hereby authorized for all users. Supervisors should be consulted before authorizing any personal use of FCC office equipment if there is any question whether such use is appropriate under the terms of this FCC Information Security Program Policy.

Office Equipment

FCC users are allowed limited use of office equipment for personal uses that involve only negligible expense to the FCC (such as electricity, sheets of paper, ink, and ordinary wear and tear) and do not interfere with official business. For purposes of this policy, office equipment includes copy machines, computers, printers, and fax machines. FCC users may not use official stationery, envelopes, or postage for personal purposes under any circumstances. Copy machines, fax machines, and printers are for official business; however, personal use of less than ten pages per week is permissible on occasion. Color copiers and color printers when used to print in color are excluded from this policy at this time due to high associated costs. Loading personally owned software (such as tax preparation programs, computer games, etc.) on FCC machines is prohibited.

16.8 *Personally Owned Equipment*

FCC users who bring non-FCC issued equipment (e.g., computers, computer peripherals, computer software, cell phones, PDAs, etc.) into FCC facilities may not connect such items to the FCC network without CIO approval.”

16.9 *Environmental Considerations*

The Computer Room and wiring closets contain, in most cases, the highest concentration of support equipment and information used at the FCC. FCC Information systems will be environmentally protected commensurate with the sensitivity and criticality of data processed. Environmental protection includes heating, ventilation, and air-conditioning systems (HVAC); water supplies; uninterruptible power supplies (UPS); and fire detection and suppression systems.

To reduce the damage done by electrical power problems, all microcomputers, or other IT resources, in FCC spaces should use surge suppressers. Those IT resources with critical production applications must also have uninterruptible power supplies (UPS) or must be plugged into circuits supplied by an UPS system. Drinking and eating is discouraged in the immediate vicinity of computers and related peripherals.

17. SYSTEM ACCESS CONTROLS

The Computer Resource Center (CRC) staff and the CISO have established procedures, which, in conjunction with appropriate request forms, will allow personnel to access FCC information system resources. Each user profile and access authorization must be supported by appropriate request forms. It is vital to the security of FCC information systems that users only request access to data and systems for which a need-to-access exists. FCC Form A-200, Computer

System Application Access Assignment must be properly completed and submitted to the CRC or ISP to obtain access to the FCC network.

17.1 Access Control

All FCC-managed computers should possess the capability to prevent unauthorized access through connected terminals, consoles, or end-user workstations by locking the workstation or disabling a session.

Password-controlled screensavers should be set to automatically activate after no more than 15 minutes of user inactivity. However, if FCC sensitive information resides on the computer, a manual keyboard lock function should also be used to secure the machine immediately when the user leaves the terminal, console, or workstation.

IMPORTANT NOTE: Any access methodology that uses stronger authentication than passwords can be used in lieu of, or in conjunction with, traditional password controls required by this policy.

17.2 User Identification and Authentication

Accountability cannot be ensured through identification alone. Identities must be verified or authenticated. Authentication mechanisms must NOT be bypassed. Both User IDs and passwords are required mechanisms for FCC multi-user systems and for single-user systems having the capability. Misrepresenting, obscuring, suppressing, or replacing a user's identity on an FCC-managed computer system is forbidden. To support this process the following standards should be followed by FCC users:

- Each user must have a unique userID/password to access FCC computer systems;
- Under normal circumstances, the userID or password must not be shared with anyone. Only in emergency situations should this be considered and then only to your supervisor. When this has occurred the user must change the password immediately upon the next login;
- UserIDs must be rendered unusable when not being used for training or maintenance tasks and administered through a secure and documented process; and
- Automatic login scripts for system access must not contain the login passwords.

17.3 Password Handling

- Passwords should be stored with one-way encryption, where only the user has the ability to know the password, and should be used on all FCC systems.
- Password history will be set to disallow the 10 previously used passwords.

- ITC System Administrators are required to disable a userID if a password attempt threshold of three failed login attempts is exceeded. Account locked-out duration is 15 minutes.
- In rare instances when certain specialized passwords, private keys, or access codes are distributed via mail or similar distribution systems, they must be sent separately from UserIDs. These items must be sealed in an opaque envelope marked with the following markings: "FCC Highly Sensitive/Restricted". This envelope must then be enclosed in a Special Attention FCC envelope.
- Developers must not endeavor to construct separate mechanisms for collecting passwords or User IDs unless such mechanisms can be proven to maintain the security and integrity of the system.
- Vendor-supplied default passwords must be changed, whenever technologically feasible, before being placed into operational status.

17.4 Emergency IDs

Emergency logon passwords for critical FCC systems must be sealed in an opaque envelope marked "Non-Public-Highly Sensitive/Restricted." The envelope must further be marked with sufficient system-specific information to ensure they are not inadvertently opened. The envelope should be placed in a secure storage area. Emergency passwords may only be used by authorized persons outside normal work hours. Each FCC installation must provide documentation detailing the circumstances and procedures for the use of emergency passwords, if they are used. Emergency passwords must be changed whenever they have been used and should be changed as outlined based on type of account and roles.

17.5 Application/Database Controls

Controls should be implemented to ensure the integrity of FCC information systems.

- Access control software and/or network operating system security software should be kept current.
- When technically possible, logs must be maintained to monitor system usage, and used to establish accountability for changes to data and programs.
- Ensure that software license agreements are adhered to, and as required, ensure that software-metering mechanisms are in place and used to monitor software use.
- Ensure that network applications installed on FCC system servers are designated as execute-only or read-only, as necessary.

- Updates and changes to applications/databases must be thoroughly tested, and certified and accredited prior to the deployment into the FCC production environment.

18. FCC INTRANET SECURITY

18.1 Respecting Intellectual Property Rights

Although the Intranet is an informal internal communications environment, the laws for copyrights, patents, trademarks, and the like still apply. To uphold these rights, and also to ensure the quality and security of the Intranet, material posted to the FCC Intranet must comply with the following:

- If material to be posted originates outside the FCC, written permission from the originator must first be obtained and the originator must be given appropriate credit;
- Copyright infringement, sensitive information disclosure, libel, defamation of character, and other possible legal issues must be avoided;
- Material accuracy, timeliness, and relevance to FCC business must be confirmed;
- All Web pages must be tested for security and operational problems before being released for FCC-wide use;
- FCC sensitive information must be protected on Intranet servers according to the level of sensitivity involved;
- All information posted to the FCC Intranet must have a designated "owner" (responsible manager). Contact information for this owner should be indicated on the page where the information appears;
- Unless approved in advance by the FCC CIO and explicitly noted on the Intranet Web page in question, all content posted to the FCC Intranet is the property of the FCC and the United States Government;
- The FCC Intranet is for the exclusive use of authorized persons. Unlike the Internet, information on the Intranet may be disseminated only to authorized persons. FCC users must not forward information appearing on the Intranet to third parties without obtaining the approval of the information owner; and
- The responsible group of each Information System must preauthorize the addition of new Intranet servers before they are connected to the internal FCC network.

18.2 *Bulletin Board System*

The FCC electronic Bulletin Board System (BBS) is provided as a supplemental system to "pin-up" bulletin boards found throughout the hallways and in the break rooms within FCC spaces. Appropriate use of the BBS facility include posting such notices as:

- Carpools: Information for those interested in car-pooling with other FCC employees; and/or
- Lost & Found: Information regarding a lost or found item.

Refer to the FCC Bulletin Board System policy for further guidance.

18.3 *Monitoring*

The FCC monitors usage of the BBS to make sure that only authorized uses of the FCC BBS will occur. Appropriate audit and investigative efforts may result from inappropriate or unauthorized use.

19. INFORMATION SECURITY MANAGEMENT

Securing information systems demands strong safeguards, effective countermeasures, and well-designed processes that are constantly reviewed for proper administration. Most systems security weaknesses are related to people and inadequate or improper security management.

Two critical systems security management issues are the management of system and network configurations, and problem resolution. Configuration management ensures there is a documented, repeatable process for tracking security features, safeguards, and countermeasures in automated systems as installed and operated, as well as detecting, reporting, and resolving security problems across the enterprise. This is particularly critical in network environments.

Security management includes responsibilities for monitoring access attempts and taking steps to prevent unauthorized intrusions. Physical security controls protect hardware and software from physical damage. Local Area Network (LAN), servers, and communications hardware must be isolated from unauthorized physical access by locked doors or cabinets. Only systems and security administration personnel should have access to servers and communications equipment.

Secure operation and implementation of systems requires accurate and up-to-date user, administration, and operational documentation. The FCC is responsible for developing, distributing, and maintaining documentation that is unique to the processing and business needs of the FCC, and which is needed to establish and maintain a secure computing and communications environment. Security awareness and training are ongoing management responsibilities. FCC users must be aware of, and understand their responsibilities for securing FCC-managed computer and communications assets.

FCC management must:

- Ensure that security and funding for IT security will be an integral part of each phase of System Development Life Cycle (SDLC) for each system. The SDLC process shall include, but not be limited to, a determination of data sensitivity, system security requirements, system boundaries and interconnections, risk assessments, and provisions for the disposal of data when the system is replaced or retired;
- Establish, fund, staff, and maintain a formal FCC-wide program for Certification and Accreditation (C&A) of all FCC information systems in accordance with OMB Circular A-130 (Appendix III), and NIST Special Publication 800-37;
- Ensure that all FCC-managed information systems undergo a C&A before they are allowed to process production data. Systems must go through the C&A process at least every three years or when a significant change is made to the system;
- Develop, document, and implement an Interim Authority to Operate (IATO) process, in accordance with NIST guidance, to be applied to any FCC-managed computer system that has not yet been fully certified and accredited with an Authority to Operate (ATO) or has had significant vulnerabilities discovered during the certification process. Any information system within the FCC that has not been subjected to the formal C&A process must have an IATO approved by the FCC CIO before being allowed to process production data;
- Develop, maintain, and enforce a process for requesting access to the various FCC computing platforms. This process must provide detailed written procedures regarding who can submit requests to add, modify, or remove user access to FCC - managed computer systems for both internal and external clients. The access request process must provide adequate identification and contact information for users, and must specify what applications, systems, and information they may access. The process must provide permanent electronic or hardcopy documentation of all access requests for all users, such that an individual's access history can be retrieved as needed for audit and tracking purpose;
- Develop and maintain current documentation in the form of standards, procedures, charts and diagrams that explain how hardware, software, and application systems are to be installed, maintained, used, backed up, restored, and secured. Every FCC network, major application (MA) and general support system (GSS) must have detailed documentation addressing these areas of concern. Documentation should be written in sufficient clarity and detail that a skilled FCC user who is unfamiliar with a system or application could, in an emergency situation, manage the operation and maintenance of the system or application. Organization charts and network diagrams must be kept current and distributed to appropriate staff as often as necessary to ensure users can perform their assigned duties with the assurance that their documentation is accurate;

- Review, on a regularly recurring basis, lists of users and their associated network or system access privileges. These reviews will be the basis for requesting security administrators to modify user access levels, including removal of access for individuals because of changes in job responsibilities, transfers to other functional Bureaus/Offices or changes in employment status such as termination, retirement, etc.;
- Develop a System Security Plan (SSP) during the initiation phase for each system in accordance with NIST Special Publication 800-18. All FCC Major Applications and General Support Systems must have an SSP that reflects the security controls for interfaces and boundary issues of all interconnected systems. Each SSP must include system categorization, asset valuation, and rules of behavior tailored to the security requirements of the particular system;
- Review and update the SSPs for MAs and GSSs at least every three years or whenever a significant change is made in a system's configuration. SSPs must be reviewed and certified by the CISO;
- Establish computer support and operations as a part of the FCC security program. Computer support and operations planning will address loading and executing new software; use of system utility software; authorizations required for system changes; software license management; configuration management; file backups; media controls; and documenting security support sufficiently to ensure consistency and continuity. Computer support and operations also includes establishing a help-desk to assist users in identifying security problems, issuing the proper response, and informing the appropriate individuals;
- Develop and implement procedures to ensure sensitive printed, electronic or other removable media is not lost, stolen, misplaced, or accessed by unauthorized persons. The procedures will address the control of output, access to system printers, and marking and disposing of media in accordance with the FCC Management of Non-Public Information Policy;
- Establish procedures for the maintenance, service, and repair of system hardware and software. The procedures for hardware maintenance should address background checks for unsupervised and unescorted contractor maintenance personnel; procedures for escorting non-cleared maintenance personnel on FCC premises; and sanitization of storage media before removal for off-site repair;
- Establish and document a change control process for each system. The change control process will include documenting and testing all changes before modifying the IT system so that new vulnerabilities are not introduced. Update system configuration documents, such as the SSP, risk assessment, and contingency plan accordingly;

- Establish procedures to ensure software installed on IT systems complies with copyright laws and is incorporated into the system's Life Cycle Management (LCM) process;
- Designate in writing the assignment of data ownership responsibilities (e.g., Data Custodians) for FCC and client agency databases, master files, and other shared collections of information. Such assignments should also identify individuals or groups authorized to originate, modify, or delete specific types of information found in these collections of information;
- Identify in writing the assignment of platform and application security administration responsibilities. Concurrent with this responsibility is the requirement that all individuals who are assigned security-related responsibilities must be provided with security and job-specific training designed to ensure they can perform their duties in an accurate and timely manner;
- Reevaluate at least annually, the computer and information access privileges granted to users. As user job duties change, privileges must be reevaluated. Managers are responsible for promptly reporting significant changes in their staff's computer-related duties or employment status to FCC Network Operations Group (NetOPs). Records must be kept current and reflect all the computer systems for which users have IDs; and
- When a user vacates a position, both computer-resident files and paper files must be promptly reviewed by his or her supervisor to determine:
 - a. If the files should be retained,
 - b. Who should become the custodian of files that are retained, and
 - c. The appropriate method(s) to be used for disposing of files that are not retained.

19.1 Software Management

Software used on FCC computers must be properly licensed. Unlicensed software is not authorized for use on FCC computers. In addition, software must be pre-authorized for installation on local computer drive(s) by completing Form A-202, FCC Computer System Personally-Owned Software Certification before installation. Users are not authorized to place software, which has been licensed for individual use, on any shared drive.

- 19.1.1 Installing Non-FCC Standard Software on FCC Computers. At times, FCC users may be required to use computer software programs, which are not readily available at the Commission. Computer resources, including system disk space, are limited agency assets. In order to maximize the use of FCC computer resources, the

group(s) managing the system(s) must be aware of what is loaded on their respective system(s). FCC managers also have the responsibility to ensure that software loaded on Commission computer systems is properly licensed. To support this effort, users must obtain authorization prior to installing software on their local drives by completing the Form A-202, FCC Computer System Personally-Owned Software Certification, and submitting the form to the Computer Resource Center for processing. Conditions which will be considered prior to approving a request include:

- Is the software in question intended for official FCC business?
- Is the software only to be loaded on the user's local computer drive(s)?
- Have the software diskettes been scanned for computer viruses?
- Will the software encumber related FCC computer resources?

19.1.2 Single License Software - FCC users should ensure that single license software programs are not loaded on shared system drives. All software deemed to have been loaded without proper approval on system shared drives may be purged from the system after notice has been given to the user(s).

19.1.3 Copying Software from FCC Computer Systems - Users of FCC computer resources are *not* authorized to copy software from the system. Users requiring a copy of the software loaded on FCC computer systems for a remote PC should contact the Computer Resource Center for assistance.

19.1.4 Upgrading Software - As necessary, software will be upgraded to most recent version, provided funding is available. When previous versions of software are no longer installed on FCC computer systems or individual PCs, appropriate actions should be taken to ensure destruction of the old version, ensuring the software is no longer useable.

19.2 *Unauthorized Software*

No exceptions to this policy will be issued. Do not submit Form A-202, FCC Computer System Personally-Owned Software or the FCC Power User Account Certification Form requesting installation for the types of software applications listed below.

19.2.1 Games - Users of FCC computer resources are *not* authorized to load games software on FCC provided computer systems.

19.2.2 Peer-to-Peer Computing (P2P) – In accordance with OMB M-04-26, *Personal Use Policies and "File Sharing" Technology*, FCC users are prohibited from using P2P because of the risks associated with File-Sharing technologies such as the following:

- Installation of malicious code;
- Exposure of sensitive or personal information;
- Susceptibility to cyber-security attack;
- Denial of service;
- Its use or installation violates sections of this policy;
- Impermissible personal use of computer resources; and
- Installing non-FCC standard software on FCC computers.

19.2.3 Instant Messaging (IM) – The FCC prohibits the use of IM applications, and its use by a user or its installation violates sections of this policy. IM poses both privacy and security threats to FCC networks.

- Impermissible Personal Use of computer resources;
- Installing Non-FCC Standard Software on FCC Computers; and
- All violations must be reported to the FCC Information Security Program (ISP) phone number at (202) 418-1818 and e-mail address csp@fcc.gov.

19.3 *Service Level Agreements (SLAs) and Security Service Agreements (SSAs)*

The FCC negotiates formal arrangements (ie., SLAs) documenting the services the FCC agrees to provide to the client. SLAs must include a Security Services Agreement (SSA), either in the body of the main agreement, or as an addendum. The SSA clearly documents what security services the client can expect from the FCC and what security behavior and practices the FCC expects from the client organization in the areas of:

- Security programs and practices.
- Security education and awareness at all levels of the organization.
- Cooperation in the area of security incident alerts,
- Compliance with OMB Circular A-130, Appendix III, and
- Any other documented expectations on behalf of the signatories of the SLA/SSA.

- 19.3.1 Establishing and Maintaining Technical Expertise - All administrators of FCC computing platforms (e.g., WAN perimeter hardware and software, LAN hardware and software, application servers and software, or other production FCC computing devices) shall be provided with sufficient training to ensure the integrity of all FCC computing platforms and systems.

IMPORTANT NOTE: For the purposes of this document, the term “administrators” shall include any individual who is responsible for the configuration, security, patch management, software installation and maintenance, backing up of data, and other daily technical management of an FCC computing device or system. Administrators may be full-time, part-time, temporary, or contract employees.

The focus of training received by administrators must include training on:

- How to configure systems correctly and securely.
- How to ensure systems are always maintained at the latest patch levels.
- Best practices for the specific IT resources being administered or implemented.
- How to audit security logs and to recognize unauthorized or suspicious activity.
- How to ensure IT resources are operating correctly.

Technical administrators of FCC IT resources must receive specialized technical training on new IT resources before the resources are placed into a production environment. A training waiver may be obtained by the manager of a new IT resource, providing the new resource is similar enough in design and function to other IT resources already in use, or providing the administrative staff have prior experience with the new resource.

- 19.3.2 Wide Area Network (WAN) Perimeter Security - The FCC shall plan, design, and implement the hardware, software, and monitoring capabilities needed to ensure the security of the perimeter of the FCC WAN. All points of entry into the FCC network must be hardened, maintained, and monitored to prevent unauthorized access, and vulnerability to denial of service or other potentially IT security-destructive attacks from external or internal sources. The FCC must maintain a *Bureau Perimeter Security Plan (BPSP)* that details network defenses [DMZ (demilitarized zone), firewalls, etc.] and configurations to provide protection for the FCC mission against intrusion.

- 19.3.3 Information Integrity - FCC IT systems that employ routable protocol devices will contain intrusion detection systems (IDS)/intrusion prevention systems (IPS). The IDS/IPS will be installed on boundary protection devices, such as routers or firewalls, to detect network intrusions and potential breaches in progress. Additionally, IDS/IPS will be installed on multi-user systems to detect intrusions on hosts, including servers that are located on wireless local area network segments and servers that are directly accessible from a network outside FCC security administration boundaries.
- 19.3.4 Penetration Testing and Vulnerability Assessment - For the purposes of this policy, the term "penetration testing" shall be construed to include any manual or automated process applied by approved and knowledgeable persons against any FCC network or computer system for the purpose of scanning or otherwise testing for operating system, configuration, or other weaknesses or vulnerabilities that could be exploited to gain unauthorized access to an FCC network or system. Penetration testing may involve the use of tools and other approved mechanisms, either internal or external to an FCC ITC, under tightly controlled circumstances and with the prior written approval of the FCC CIO.

Penetration Testing will be conducted on a regularly scheduled basis, on selected systems and networks and should involve program managers and information owners responsible for the mission activities supported by the subjected system. Isolated systems (those not connected to external networks through routable protocol features or supporting dial-in capability) do not require penetration testing. Test plans and detailed procedures will be developed, reviewed, and approved by the FCC CIO before testing at any FCC ITC. The penetration testing team will complete nondisclosure agreements before the testing and all test data, including logs, files, and passwords will be returned. No copies will be made of information. FCC ITC will take precautionary measures, such as the issuance of formal rules of engagement, to ensure the testing does not interrupt routine customer processing or create an exposure to the system.

19.3.5 Lessons Learned and Mitigation

As soon as possible following the conclusion of penetration testing on any FCC network or system, ITC management will schedule a meeting of all participants together, with members of installation IT Security management, and with other concerned persons such as program managers and system owners. These meetings will be used to present lessons learned from the penetration testing, and to discuss methods and techniques for mitigating any residual risks found. Risk mitigation shall be accomplished based on issues of cost-benefit and on management's willingness, to accept a certain amount of residual risk.

Care shall be taken to thoroughly document:

- Penetration testing results
- Vulnerability assessment results
- Lessons learned
- Management decisions regarding mitigation measures
- When mitigation will be implemented
- Who will be responsible for the implementation
- What the expected level of residual risk will be

20. RESOURCE CLASSIFICATION

Bureaus/Offices are required to determine and notify ITC of which, if any, applications/databases controlled or utilized within that Bureau/Office are considered sensitive or support a function considered critical to the successful operation of the FCC.

20.1 Sensitive/Mission Critical Applications

Oversight for computer data and associated resources resides with the Bureau/Office requesting the purchase of the peripheral(s) or development of the application and/or data. Bureau Chiefs and Office Directors should assign ownership to an appropriate Division, Branch, or any functional entity within that Bureau/Office.

Information Systems and applications that process, store or transmit FCC owned information must be identified and use protections appropriate to the highest level of sensitivity of information processed by or contained within the system. It is the responsibility of each Bureau/Office to identify their applications that are considered sensitive or mission critical and to provide sufficient justification for that determination based on business need.

The following criteria should be considered to determine the sensitivity and/or related mission critical nature of applications and data processed at the FCC:

- Follow guidelines set forth in NIST FIPS 199;
- Information protected under the Privacy Act of 1974 and protected from release under the Freedom of Information Act (FOIA);
- Information which is critical to an agency's ability to perform its mission;
- Financial management data on systems that process electronic funds transfers, control inventory, issue checks, control accounts receivables and payables, etc.;

- An application that can produce ad-hoc reports with aggregated information that may be considered sensitive in nature; and
- An application with information that falls within one of the categories identified within FCCINST 1139, *Management of Non-Public Information*.

20.2 *Safeguarding FCC Data (Sensitive/Mission Critical Data and Non-Sensitive Data)*

Each FCC Bureau/Office shall be responsible for ensuring that all forms of media containing FCC data originated or processed by the Bureau/Office is handled and disposed of in a manner commensurate with the criteria established in this and other FCC directives. FCC users should ensure that sensitive data is not stored on shared drives accessible by the general FCC user community. Sensitive data should be stored on network devices that have access granted only to appropriate staff. In addition, users should not store sensitive data on their local drives. If sensitive data is stored on removable media it should be appropriately labeled, encrypted, protected, and accounted for. Refer to FCC Policy #OC-009, *Protection of Sensitive Agency Information*.

20.3 *Sharing Sensitive and Other Data with Others Outside the FCC*

It is the policy of the FCC that sensitive information is only releasable by authorized Bureaus/Offices within the FCC. Further, users must take precautions to restrict the release of electronic or other removable media containing sensitive information and receive written authorization from their supervisor as needed.

Processing of FCC Data - FCC data may be processed by another Government agency, or a contractor. However, the application and agency processing FCC data shall:

- Adhere to the information security policies in OMB Circular A-130 and FISMA unless more stringent policies or regulations apply at the agency where the information is being processed;
- Follow the standards and guidelines promulgated by NIST;
- Complete a security assessment of the facility within the previous three years;
- The Contracting Officer will consult the CISO for security assistance, as required;
- The COTR will monitor contractor compliance with FCC's Information Security Assurance Program Directive and policies; and

- The COTR will maintain all documentation provided by the outside organization.

20.4 *Certification & Accreditation of Information Systems/Applications/Appliances*

Prior to implementation all applications or appliances created and utilized to process FCC data are to undergo testing to verify that the required administrative and technical IT security safeguards are operationally adequate and the results of the design review and system tests are fully documented and maintained. Application and appliances owners must ensure this testing is conducted, receiving an authority to operate (ATO) or an interim authority to operate (IATO) prior to deploying the application to production. Testing of applications shall be in accordance with NIST SP 800-37 and SP 800-53 guidance. System owners with applications external to the FCC, but processing FCC data, shall ensure that applications are tested by the external agency or an approved third party in accordance with these requirements.

Risk Assessment Cycle

A risk assessment must be performed on all major applications and general support systems at specific times within the lifecycle of the application or system. This should occur before approval of the design specifications for a new system and at least once every three years or whenever a significant change occurs to a production system (e.g., adding a LAN; changing from batch to on-line processing; adding dial-up or digital signature capabilities, etc.).

Security Test and Evaluation

Security Test and Evaluation (ST&E) activities validate that security controls implemented on an information system meet the security requirements for the system and the information. An ST&E will be conducted on all FCC major applications and general support systems prior to moving into production and at least every three years thereafter or whenever a significant change occurs.

In accordance with OMB A-130, recertification occurs whenever an application is modified significantly or every three years. Recertification of external systems processing FCC data must be completed by the external organization.

All application owners must ensure that their applications undergo periodic security reviews in an effort to evaluate the effectiveness of the application's security controls. This should be done depending on risk associated to the system, but not less than annually.

21. BUSINESS CONTINUITY AND DISASTER PLANNING

All Federal agencies are required to have in place a viable Business Continuity Plan (BCP) to ensure the performance of essential functions during any emergency situation that may disrupt normal operations. A BCP provides a controlled response that minimizes damage and restores operations as quickly as possible.

FCC Bureau's and Office's (B/O), to include Field Offices, shall develop Business Continuity Plans (BCP)s for all time-sensitive FCC-managed computer systems, applications, and business processes, hereafter referred to as "system". Such plans must be written in sufficient detail so that persons unfamiliar with the system (or systems) could execute the plans and be successful in recovering the system (or systems) involved.

A Disaster Recovery Plan (DRP) shall be required to establish procedures for the recovery of the FCC Headquarters Information Technology (IT) infrastructure and automated services functionality following a disruption.

21.1 Business Continuity and Disaster Planning

Business Continuity and Disaster Planning for FCC IT systems must include, as a minimum:

- A determination of system sensitivity to down time.
- System restoration priorities. This should be reevaluated at least annually.
- Automated Systems: A program of regular back-ups of systems, data, and the documentary materials necessary to operate and maintain them.
- Non-Automated Systems: A program of maintaining time-sensitive/critical documents and hardcopy records for off-site storage.
- Review and update the plan at least annually.
- Annual testing of the plan.

21.2 Plan Integration

The B/O Business Continuity and Disaster Recovery Plans must be an integral and integrated part of the overall agency plan. Interdependencies between Bureaus, Offices and Field Offices must be clearly identified in their respective plans so that there are no surprises in the event of a disaster.

22. INFORMATION CONFIDENTIALITY, INTEGRITY, AND AVAILABILITY

All information protection and handling activities at the FCC are intended to be consistent with generally accepted privacy ethics, standard business practices, public law, FCC 1139 Directive, Management of Non-Public Information, and FCCINST 1131, Information Security Manual.

FCC management must make reasonable efforts to:

- Ensure that all privacy information maintained by the FCC is accurate, timely, relevant, and complete;
- Ensure that all privacy information is used only as intended and that precautions to prevent misuse are both effective and appropriate;
- Establish appropriate controls to ensure that privacy information is disclosed only to those who have a legitimate business need;
- Establish and maintain sufficient controls to ensure that all FCC information is free from a significant risk of undetected inappropriate alteration; and
- Consistently apply an Information Classification label or marking. Refer to FCCINST 1139, *FCC Management of Non-Public Information* for guidance relating to identification, marking, handling and disposal of FCC sensitive information.

23. AWARENESS, TRAINING, AND EDUCATION

It is FCC policy that each FCC user having access to computer resources receive FCC information security awareness training. The training generally includes topics of information system security basics, acceptable computer practices, and an overview of information security policies and procedures.

23.1 *Orientation Training*

Each new user of FCC computer systems shall be provided training materials promulgated by the Information Security Program which outline responsibilities on safe computer practices. This training should occur within the first 30 days of beginning employment.

23.2 *Annual Training*

Users are required to take an annual training program, which is meant to enhance users' knowledge of good security practices while operating FCC information systems through material promoted by the Information Security Program.

23.3 *Quarterly Awareness and Training*

This refresher training may fulfill the requirement for annual training for FCC users and is open to all FCC employees and contractors.

23.4 *Specialized Training*

Key IT Staff, designated by the CISO, with significant security related responsibilities are required to take specialized training quarterly. This training should provide security awareness through advance topics relative to the key IT staff's responsibilities.

24. ACCESS PRIVILEGES AND PERMISSIONS

Each FCC Bureau/Office and field office is responsible for determining the level of permissions required for each user. If an employee transfers between FCC Bureaus/Offices or functional groups, old privileges and permissions must be removed and replaced by those required by the new job responsibilities. The gaining organization is responsible for requesting new access authorities by completing FCC Form A-200, FCC Computer System Application Access Assignment based on the requirements of the new job, and having the person complete a new FCC Form A-201, Rules of Behavior.

24.1 *Privileged Access and Users*

Special system privileges, such as the ability to examine the files of other users without permission, reset passwords, add or delete user accounts, etc., must be restricted to only those individuals directly responsible for system management or security. Activities of privileged users should be audited in complete detail and the audit logs maintained for a period of at least six months. System privileges must not be granted without documented management approval on the FCC Power User Approval Form. This form may be obtained from the ISP office or the corporate Intranet, and will be filed with the ISP once signed.

24.2 *Temporarily Modifying System(s) Access*

Users must complete and submit Form A-200, FCC Computer System Application Access Assignment to the CRC to modify system access.

25. INTERNET ACCESS AND USE

Internet access is provided to every FCC user as a resource to directly facilitate work. FCC reserves the right to monitor websites accessed. Refer to FCC Internet Access Policy for detailed information on appropriate use of the Internet, and examples on impermissible uses.

It is the user's responsibility to exercise good judgment when accessing Internet sites and avoid sites that might cause embarrassment to the FCC.

FCC users may make some personal purchases through the Internet, but only during non-business time. When making personal purchases, users must:

- Not use a Government credit card;
- Not incur any expense to the Government (e.g., request separate billing to the FCC, etc.); and
- Have purchases delivered to a non-Government address.

25.1 Public Representations

All FCC users declaring an affiliation with the FCC must also clearly indicate that the opinions expressed are their own and not those of the FCC or the United States Government. Likewise, if an affiliation with the FCC is provided, political advocacy statements and product/service endorsements are also prohibited.

To avoid libel, defamation of character, and other legal problems, any and all declared affiliations with the FCC via an Internet message or posting must refrain from harassing, annoying or alarming other persons.

Care must be taken to properly structure comments and questions posted to mailing lists (listservs), public news groups, Usenet, and related public postings on the Internet. Before posting any material, users must consider whether the posting could cause legal or public relations problems for the FCC. Consequently, users should be reserved rather than forthcoming with information relating to or about the FCC, its mission, or its clients.

25.1.1 Internet Security - All information obtained from the Internet should be considered suspect until confirmed by separate information from another source. There is no quality control process on the Internet.

25.1.2 Virus Checking - All non-text files (databases, software object code, spreadsheets, formatted word processing documents, etc.) downloaded from non-FCC sources via the Internet must be screened with virus detection software before being used. Whenever an external provider of software is not trusted, downloaded software should be tested on a stand-alone non-production machine that has been recently backed up. Downloaded files must be decrypted and decompressed before being screened for viruses. Separately, the use of digital signatures to verify that unauthorized parties have not altered a file is recommended; but this does not assure freedom from viruses.

- 25.1.3 Push Technology - Automatic updating of software or information on FCC-managed computers via background "push" Internet technology is prohibited due to the potential to cause system operability problems. There are limited exceptions to this rule. The exceptions must be documented and approved through the change control board.
- 25.1.4 Spoofing Users - Identity confirmation is ideally performed via digital signatures or digital certificates; but in cases where these are not available, other means such as letters of credit, third party references, and telephone conversations may be used.
- 25.1.5 User Anonymity - Misrepresenting, obscuring, suppressing, or replacing a user's identity on the Internet or any FCC electronic communications system is forbidden. The user name, E-mail address, organizational affiliation, and related information included with messages or postings must reflect the actual originator of the messages or postings. Anonymous FTP log-ins, except via web browsers are NOT permitted.

25.2 Confidentiality

- 25.2.1 Information Exchange - In keeping with the confidentiality agreements signed by all employees, FCC software, documentation, and all other types of internal information must not be sold or otherwise transferred to any non-FCC party for any purposes other than those business purposes expressly authorized by FCC management.
- 25.2.2 Posting Materials – FCC users must not post unencrypted FCC material (software, internal memorandums, policies, etc.) on any publicly accessible FCC computer unless the posting has been reviewed and approved by the FCC OMD Web Development group, in accordance with the FCC *Information Security Program*.
- 25.2.3 Message Interception - Wiretaps, sniffers, and other types of message interception are straightforward and frequently encountered on the Internet. Accordingly, FCC sensitive information including source code must not be sent over the Internet unless it has first been encrypted by approved methods.
- 25.2.4 Security Parameters - Credit card numbers, telephone calling card numbers, fixed logon passwords, and other security parameters that can be used to gain access to FCC information systems services must not be sent over the Internet in readable form.

25.2.5 Restriction on “Persistent Cookies.” - FCC Web sites and pages operated by FCC users or by contractors on behalf of the FCC should not use “Persistent Cookies” in accordance with OMB M-99-18, the Privacy Policies and Data Collection on Federal Web Sites and stated in FCC Privacy Policy.

25.3 Access Control

25.3.1 User Authentication - All users wishing to establish a real-time connection with an FCC internal computer via the Internet must first authenticate themselves at the FCC firewall, VPN device, or multi-factor authentication system before gaining access to the FCC internal network.

Protection of Authentication-Related Data - FCC ITC must employ data integrity and validation controls to provide assurance that authentication data (e.g., password files, User ID files, user permission files, etc.) are protected sufficiently so that only authorized persons may make changes to the data (e.g., users may change their password, administrators may change user permissions when authorized to do so, etc.). System-generated security logs must track all accesses to user authentication data at the level of UPDATE or higher. Unusual or suspicious changes must be investigated and resolved.

25.3.2 Internet Service Providers - With the exception of telecommuters and mobile computer users, FCC users must not employ personal Internet Service Provider (ISP) accounts and dial-up lines to access the Internet with FCC-managed computers. Instead, all Internet activity must pass through FCC firewalls or ITC approved devices so that access controls and related security mechanisms can be applied.

26. ELECTRONIC MAIL

The FCC Electronic Mail (e-mail) facility offers FCC users an efficient way to communicate with others inside, and outside (via Internet) the FCC using Commission computer systems. FCC e-mail is provided for use to accomplish day-to-day business activities. FCC provided e-mail is intended for official and authorized purposes only. E-mail users must exercise common sense, good judgment, and propriety in the use of this FCC resource because messages could be taken out of context and lead to inappropriate or potentially damaging conclusions.

Authorized FCC e-mail users *are not* permitted to forward FCC e-mail or attachments to personal accounts managed by public e-mail or Internet access service providers where the information might be compromised. Further, FCC users *are not* authorized to use the e-mail system to send sensitive Commission information via the Internet where information might be intercepted. Refer to the FCC Electronic Mail Policy for further instruction.

26.1 *Distribution Protocol*

Whenever possible, FCC users should limit the distribution of e-mail to the smallest group possible in order to eliminate unnecessary resource congestion. If an inappropriate e-mail is brought to the attention of the CISO, the "sender" will be directed to retract the message by either the e-mail Postmaster or the Information Security Officer. The Postmaster will retract inappropriate or unauthorized e-mail if the "sender" is not available.

Important Note: An e-mail message sent to the "*Everyone*", or similar group, reaches approximately 2,500 FCC employees and contractors causing a significant burden on the FCC.

26.2 *Inappropriate Use of Electronic Mail*

The activities below constitute "Improper Use of FCC E-Mail Systems" and are prohibited:

- Any personal use that causes congestion, delay, or disruption of service to any FCC system, i.e. file attachments;
- The creation, copying, transmission, or retransmission of chain letters or other unauthorized mass mailings regardless of the subject matter. ;
- For activities that are illegal, inappropriate, or offensive to fellow users or the public. Such activities include, but are not limited to, profanity, slander, harassing language, hateful speech or material that ridicules others on the basis of race, creed, religion, color, sex, disability, national origin, sexual orientation, and other such language is as inappropriate in E-mail as in any other medium;
- The creation, viewing, storage, copying, or transmission of sexually explicit or sexually oriented materials;
- The creation, viewing, storage, copying, or transmission of materials related to gambling, illegal weapons, terrorist activities, and any other illegal activities or activities otherwise prohibited, etc.;
- 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, and sale of goods or services);
- Use for engaging in any outside fund-raising activity, endorsing any product or service, participating in any lobbying activity, or engaging in any prohibited partisan political activity;

- Use for posting agency information to external newsgroups, bulletin boards, or other public forums without authority. 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;
- The unauthorized transmission or distribution of any controlled information including computer software and data that includes Privacy Act or other sensitive information;
- The unauthorized transmission or distribution of copyrighted or trademarked documents or materials with other intellectual property rights (beyond fair use) such as proprietary data or export controlled software or data; and
- Knowingly and willfully transmitting malicious code via E-mail such as viruses, worms, or other programs used for exploiting systems.

26.3 Proprietary, Sensitive, or Confidential Information

FCC users who have access to proprietary or highly sensitive information, including information that is protected under the Privacy Act of 1974 are responsible for protecting the sensitive or confidential information to which they have access. Unencrypted E-mail is not a secure medium for transmitting sensitive or confidential information. Unless authorized to do so, E-mail may not be used to send messages that contain confidential, sensitive, or private information about an individual.

26.4 Ethical Conduct

Employee must not use or permit the use of their position or title or any authority associated with public office in a manner that could reasonably be construed to imply that the agency sanctions or endorses their personal activities.

26.5 Retention of E-Mail Messages

Users are responsible for managing the number of E-mail messages in their own mail box, copying and filing official E-mail records into the appropriate paper filing system, and deleting those messages that do not constitute records.

26.6 Archiving

Storing E-mail messages in a network directory or on a local hard drive is not an acceptable records storage method because the records are not easily accessible to other users. The E-mail archiving feature should only be used for storing "personal" copies of reference documents, not for the storage of official E-mail records. Official E-mail records must be printed in paper and filed in the agency paper filing system.

26.7 *Freedom of Information Act (FOIA) Considerations*

E-mail messages may contain information that *must* be disclosed to the public, upon request. E-mail messages that are the subject of active FOIA requests or appeals procedures may not be deleted or otherwise disposed of even if they constitute records and are authorized for destruction by an approved records schedule.

26.8 *Examination of Stored Information*

At any time and without prior notice, FCC management reserves the right to examine archived E-mail, private file directories, hard disk drive files, and other information stored on FCC information systems. Such examinations are typically performed to assure compliance with internal policies, support the performance of internal investigations, and assist with the management of FCC information systems.

26.9 *Improper Use of FCC Computing Resources*

Unauthorized or improper use of FCC computing resources could result in disciplinary action (Misuse or abuse of FCC computing resources may also result in the loss or limitation on use of such equipment (e.g., revocation of User IDs or suspension of access privileges). Refer to the FCC Information Security Program Policy on Limited Personal Use of FCC Office Equipment for further instruction.

- Users are prohibited from using FCC computing resources, including e-mail for personal uses except as authorized by this Policy; Further,
- Users are prohibited from using FCC computing resources, at any time, for activities that are:
 - Illegal (e.g., gambling (5 CFR 735.201));
 - Inappropriate or offensive to colleagues or the public, such as the use of sexually explicit material or materials that ridicule others on the basis of race, creed, religion, color, sex, disability, age, national origin, or sexual orientation;
- Users are prohibited from using FCC computing resources at any time for any outside fund-raising activity, endorsing any product or service, participating in any lobbying activity, or engaging in political activities;
- Users are prohibited from using FCC computing resources at any time, including the Internet to:
 - Make purchases for personal commercial gain activity; and

- Present their personal views in a way that would lead the public to interpret it as an official position. This includes posting to external news groups, bulletin boards, or other public forums;
- Users are not authorized to remove FCC property from FCC premises for personal use; and
- Users are prohibited at any time from using “push” technology on the Internet or other continuous data streams, unless they are directly associated with the user’s job. Push technology from the Internet means daily, hourly, or continuous updates via the Internet (e.g., news, stock quotes, weather, and similar information). Continuous data streams could degrade the performance of the entire network.

27. INCIDENT HANDLING

When security incidents occur, the FCC must respond quickly and effectively. The FCC's Computer Incident Response Team (CIRT) has been charged to act as the Commission's focal point for mitigating the impact of computer related information security incidents. As required, the team acts to prevent or minimize the impact of an attack against computer operations at the FCC. During an actual Information Security incident, CIRT members will be expected to devote whatever time and expertise is required to bring the incident to a satisfactory closure with minimal damage and impact to the FCC.

All security incidents, including breaches of personal identifiable information (PII) will be handled in accordance with established procedures. Refer to the US CERT *Concept of Operations for Federal Cyber Security Incident Handling* and the FCC Desk Reference Guide, *Computer Security Incident Response Guide*, OC-290.

FCC users must promptly report all suspected or known security incidents to the appropriate help desk, supervisor or to their manager. When appropriate, the CISO shall activate the CIRT to investigate, contain, and control an incident. Although all incidents are to be reported, the level to which an incident is raised is a judgment call resting with the FCC CISO. The extent of the investigation and reporting will be determined by the impact and severity of the incident.

The FCC ISP, in conjunction with the CIRT and the system administrator(s), is responsible for completing an Incident Response Report and forwarding it to the FCC CISO and as applicable, to the US-CERT.

The default status of any and all security-related information that the FCC CIRT receives must be protected as Non-Public-For Internal Use Only. During the investigation of extremely sensitive security incidents, all information about the incident will be limited to only those individuals with a need to know. Only after proper review and approval will such information be made available for release.

28. COMPLIANCE

The FCC is responsible for establishing an auditable process to document, track, and monitor compliance of its computer systems, applications, and network elements with the requirements of this Policy. Compliance requirements for FCC-managed computer systems are as follows:

28.1 *New Systems*

All computer systems, computer-based tools, computer applications, and network elements acquired or developed after the publication date of this Policy must comply with the requirements for security detailed herein.

28.2 *Existing Systems*

Computer systems, computer-based tools, computer applications and network elements currently in use by the FCC must comply with the security standards detailed herein, to the extent permitted by the technology involved, business risk, cost of conversion, and complexity of change.

28.3 *Noncompliance*

Any computer systems, applications, or network elements, existing or future, failing to comply with the requirements of this policy must be documented by the responsible organization, signifying knowledge and acceptance of risks associated with areas of noncompliance.

28.4 *Variances*

FCC Bureau/Office can request system variances for requirements in this document that may be too costly or technically infeasible to implement. All requests for variances must be submitted in writing to the FCC Chief Information Officer (CIO), and Chief Information Security Officer (CISO). Requests must include the following information:

- A description of the system(s) for which a variance is being requested. This should include all pertinent information necessary to clearly identify the system(s), such as brand name, model, exact physical location, operating system(s) in use, applications supported, number of users, etc.
- A description of the security variance(s) being requested. This should include an explanation why the requirement(s) cannot be met, what alternative measures will be used to compensate for any vulnerabilities resulting from the variance, and a target date when the variance will no longer be required. Requests for variance(s) from the requirements of this Policy must be approved by the FCC and must be updated annually. Copies of approved variances must be sent to the Bureau/Office heads.

29. AUTHORITIES


This policy replaces all previously published FCC Information Security-related policies except for installation-specific or platform-specific documents designed to address security issues unique to the installation or platform for which it was written, so long as those documents meet or exceed the minimum requirements of this Policy.

The authority behind the FCC Information Security Policy includes Public Laws, Executive Branch Directives, Federal Standards and other policies that provide direction and guidance concerning security planning. This Information Security Policy establishes the FCC IT Security Program in compliance with:

- The Privacy Act of 1974;
- The Freedom of Information Act, as amended;
- The Paperwork Reduction Act;
- The Computer Fraud and Abuse Act of 1986;
- OMB Circular A-130, Appendix III, Security of Federal Information Resources;
- National Institute of Standards and Technology (NIST) Special Publications addressing IT security;
- Federal Information Security Management Act (FISMA), (Public Law (P.L.) 107-347);
- OMB M-06-16, Protection of Agency Sensitive Information;
- FCCINST 1113.1, Privacy Act Manual;
- FCCINST 1139, Management of Non-Public Information;
- NIST Federal Information Processing Standards Publications (FIPS PUBS)
- Office of Personnel Management's (OPM) guidance on personnel security as they relate to IT resources;

The FCC Information Security Policy is specifically designed to address risks to data, data processing systems, and networks. In doing so, this Policy may overlap with other FCC policies such as those relating to building security, ethics, business continuity, etc. While the intention is to complement related policies, it is possible that conflicts may exist. Such cases should be reported to the policy document owners for resolution. Federal, legal, regulatory, and statutory

requirements will always take precedence over this policy. This policy is intended to be technically generic. Installation and platform-specific policies, standards, and procedures must be developed and implemented at the FCC Bureau and Office levels, to ensure compliance with the word and intent of this policy.


Anthony J. Dale
Managing Director

- FCC Computer System Application Access Assignment, Form A-200
- FCC Computer System Rules of Behavior, Form A-201
- FCC Computer System Personally-Owned Software Certification, Form A-202
- FCC Computer Systems Separation Clearance, For A-203
- Definitions
- References

Stocked By:
Performance Evaluation and Records Management

30. DEFINITIONS

- a. Access - 1. The ability to enter a secured area. 2. A specific type of information between a subject and an object that results in the flow of information from one to the other.
- b. Access Control - An entire set of procedures performed by hardware, software, and administrators to monitor access, identify users requesting access, record access attempts, and grant or deny access based on pre-established rules.
- c. Adequate security - security commensurate with the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of information. This includes assuring that systems and applications used by the agency operate effectively and provide appropriate confidentiality, integrity, and availability, through the use of cost-effective management, personnel, operational, and technical controls.
- d. Alphanumeric - A contraction of *alphabetic* and *numeric*, that indicates a combination of *any* letters, numbers, and special characters.
- e. Application - means the use of information resources (information and information technology) to satisfy a specific set of user requirements.
- f. Availability - That aspect of security that deals with the timely delivery of information and services to the user.
- g. Backup - Applies to data, equipment or procedures that are available for use in the event of failure or loss of normally used data, equipment or procedures. The provision of adequate backup capability and facilities is important to the design of data processing systems in the event of a system failure that may potentially bring the operations of the business to a virtual standstill.
- h. Computer Incident Response Team (CIRT) - Act as the Commission's focal point for mitigating the impact of computer related information security incidents, and acts to prevent or minimize the impact of an attack against computer operations at the FCC.
- i. Computer Log-in - A simple procedure occurring at the beginning of a session at a workstation in which the host asks the user for identification. At the FCC, login refers to two separate authorization codes: userID, and password.
 - 1. UserID is the authorization code used to verify that FCC users are entitled access to FCC computer resources, and to identify the specific resource(s) used; and
 - 2. Password is a unique secret word selected by each user that is associated with a particular user ID. The Passwords primary function is to protect the userID from unauthorized use. A non-display mode is used when the password is entered to prevent disclosure to others.

- j. Computer Security - Technological and managerial procedures applied to computer systems to ensure the availability, integrity, and confidentiality of information managed by the computer system.
- k. Data Integrity - A measure of data quality. Integrity is high when undetected errors in a database are few. Complete data integrity is the assurance that is input to the computer today will be there tomorrow, unchanged in any way.
- l. Bureau/Office Manager - Any FCC Bureau/Office representative who acts as the application/database or system focal point for management.
- m. General Support Systems - Are those interconnected set of information resources under the same direct management control which share common functionality. A system can be, for example, a local area network or an agency-wide backbone.
- n. Hardcopy - Medium of data, either input or output, in paper form such as printouts, reports, screen prints, memoranda, checks, etc. generated as a result of the use of FCC computer system resources.
- o. Information Security Program (ISP) - Computer Security Program (CSP) has been renamed to ISP.
- p. Instant Messaging - Introduces IT security risks by allowing for the potential dissemination of significant sensitive information in a manner similar to speaking on a telephone. During registration to IM services, users are requested to fill out personal profiles with key identifying information which is placed in an Internet directory that can be viewed by all. The directory can be searched by name, date of birth, gender, and interests. A type of communications service that enables you to create a private chat room with another individual in order to communicate in real time over the Internet.
- q. Major Application - An application that requires special attention to security due to the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application. Note: All Federal applications require some level of protection. Certain applications, because of the information in them, however, require special management oversight and should be treated as major. Adequate security for other applications should be provided by security of the systems in which they operate.
- r. Mission Critical Data - Is any electronic data which supports the collection, transfer, or disbursement of funds, or Commission activities mandated by statute or treaty, the interruption of which would cause significant economic or social harm to licensees or the public.
- s. Non-FCC Issued Equipment - A device belonging to an entity that is not a formal or subsidiary part of FCC. This includes all portable, removable devices such as notebooks, USB drives, iPods, Smartphones, and PDAs.

- t. Peer-to-Peer Networking – Allows internet users to share files housed on individual computers. A type of network in which each workstation has equivalent capabilities and responsibilities. Peer-to-peer networks are generally simpler, but they usually do not offer the same performance under heavy loads.
- u. Removable Media - An information storage medium that can be removed from an information creation device such as a computer. Examples are diskettes, tapes, cartridges, optical disks, and external disk drives.
- v. Sensitive Information - Is that which requires various degrees of protection due to the risk and magnitude of loss or harm, which could result from accidental or deliberate disclosure, alteration, or destruction. This data includes records protected from disclosure by the Privacy Act, as well as information that may be withheld under the Freedom of Information Act, Non-Public—Highly Sensitive/Restricted and/or Non-Public—For Internal Use Only. Computer "hard copy" is considered, for purposes of this directive, a computerized record, and may contain "sensitive" data.
- w. Zero-day Exploit – An exploit that takes advantage of a vulnerability on the same day that the vulnerability becomes known.

31. REFERENCES

- a. Public Law 99474, Subject: "Computer Fraud and Abuse Act of 1986." The act provides for unlimited fines and imprisonment of up to 20 years if a person "intentionally accesses a computer without authorization or exceeds authorized access and, by means of such conduct, obtains information that has been determined...to require protection against unauthorized disclosure...." It is also an offense if a person intentionally accesses "a Federal interest computer without authorization and, by means of one or more instances of such conduct alters, damages, or destroys information...or prevents authorized use of such computer...or traffics any password or similar information...if such computer is used by or for the Government or the United States."
- b. OMB Circular No. A123, Revised, Subject: "Internal Control Systems." Requires heads of government agencies establish and maintain effective systems of internal control within their agencies that, in part, safeguard its assets against waste, loss, unauthorized use, and misappropriation. Among other things, the circular specifies that periodic security reviews be conducted to determine if resources are being misused.
- c. OMB Circular No. A127, Subject: "Financial Management Systems." This Circular prescribes policies and procedures to be followed by executive departments and agencies in developing, operating, evaluating, and reporting on financial management systems.
- d. OMB Circular No. A130 "Management of Federal Information Resources," Appendix III "Security of Federal Automated Information Resources." Requires federal agencies to implement a program and develop physical, administrative, and technical controls to safeguard personal, proprietary, and other sensitive data in automated data systems. OMB Circular A130 also requires that periodic audits and reviews be conducted to certify or recertify the adequacy of these safeguards. In addition, it makes agency heads responsible for limiting the collection of individually identifiable information and proprietary information to that which is legally authorized and necessary for the proper performance of agency functions, and to develop procedures to periodically review the agency's information resources to ensure conformity.
- e. 5 CFR Part 2635.1112, "Standards of Ethical Conduct for Employees of the Executive Branch." Use of Government Property Personnel shall protect and conserve Government property, including equipment, supplies and other property entrusted to them. Use of Government Information Personnel shall not use, or allow use of, official information obtained through performance of duties to further a private interest if such information is not available to the general public.
- f. 5 USC 552, Freedom of Information Act (FOIA) of 1974, As Amended. FOIA requires agencies to make available, on its own initiative, certain types of records and disclose any other record to a requestor unless a specific exemption under FOIA, of which there are nine, applies.

- g. 5 USC 552a, Privacy Act of 1974, As Amended. The basic provisions of the act are to protect the privacy of individuals. An agency is prohibited from disclosing personal information contained in a system of records to anyone or another agency unless the individual (about whom the information pertains) makes a written request or gives prior written consent for third party disclosure (to another individual or agency).
- h. 40 United States Code 1452, Clinger-Cohen Act of 1996. This Act links security to agency capital planning and budget processes, establishes agency Chief Information Officers, and recodifies the Computer Security Act of 1987.
- i. Paperwork Reduction Act of 1995. This Act linked security to agency capital planning and budget processes, established agency Chief Information Officers, and re-codified the Computer Security Act of 1987.
- j. Federal Information Processing Standards (FIPS) Pub. 102, Guideline for Computer Security Certification and Accreditation. This guideline describes how to establish and how to carry out a certification and accreditation program for computer security.
- k. Federal Information Processing Standards (FIPS) Pub. 199, Standards for Security Categorization of Federal Information and Information Systems. This publication establishes security categories for both information¹ and information systems. Security categories are to be used in conjunction with vulnerability and threat information in assessing the risk to an organization.
- l. Federal Information Security Management Act of 2002 (Title III of -Gov)
- m. GAO/AIMD-12.19.6, Federal Information System Controls Audit Manual (FISCAM). The FISCAM methodology provides guidance to auditors in evaluating internal controls over the confidentiality, integrity, and availability of data maintained in computer-based information systems.
- n. Presidential Decision Directive 63, "Protecting America's Critical Infrastructures." This directive specifies agency responsibilities for protecting the nation's infrastructure; assessing vulnerabilities of public and private sectors; and eliminating vulnerabilities.
- o. NIST Special Publication 800-18, Guide for Developing Security Plans for Information Technology Systems. This publication details the specific controls that should be documented in a security plan.
- p. NIST Special Publication 800-37, Guide for the Security Certification and Accreditation of Federal Information Systems. The purpose of this publication is to provide guidelines for the security certification and accreditation of information systems supporting the executive agencies of the federal government.

- q. NIST Special Publication 800-47, Security Guide for Interconnecting Information Technology Systems. The purpose of this publication is to provide guidance for planning, establishing, maintaining, and terminating interconnections between information technology (IT) systems that are owned and operated by different organizations, including organizations within a single federal agency.
- r. NIST Special Publication 800-53, Recommended Security Controls for Federal Information Systems. The purpose of this publication is to provide guidelines for selecting and specifying security controls for information systems supporting the executive agencies of the federal government. The guidelines apply to all components of an information system that process, store, or transmit federal information.