POLICY#	STATUS	ISSUED	LAST REVISED	PAGE
10-06	Accepted	6/30/06	6/30/06	1 of 46

State of Rhode Island Department of Administration Division of Information Technology	TITLE	IT Security Handbook Operational Controls
	DRAFTED BY	Jim Berard

TABLE OF CONTENTS

1. PERSONNEL/USER SECURITY 2
   1.1. PURPOSE AND SCOPE 2
   1.2. BACKGROUND 2
   1.3. POLICY 2
   1.4. RESPONSIBILITIES 7
2. INCIDENT REPORTING 9
   2.1. PURPOSE AND SCOPE 9
   2.2. BACKGROUND 9
   2.3. POLICY/PROCESS 10
   2.4. RESPONSIBILITIES 13
3. EDUCATION, TRAINING AND AWARENESS 15
   3.1. PURPOSE AND SCOPE 15
   3.2. BACKGROUND 15
   3.3. POLICY 16
   3.4. RESPONSIBILITIES 18
4. SECURITY CONSIDERATIONS IN COMPUTER SUPPORT OPERATIONS 20
   4.1. PURPOSE 20
   4.1 BACKGROUND 20
   4.2. POLICY 21
   4.3. RESPONSIBILITIES 26
5. PHYSICAL/ENVIRONMENTAL SECURITY 27
   5.1. PURPOSE AND SCOPE 27
   5.2. BACKGROUND 27
   5.3. POLICY 27
   5.4. RESPONSIBILITIES 30
6. CONTRACTOR/VENDOR/PARTNER SECURITY 31
   6.1 PURPOSE 31
   6.1. BACKGROUND 31
   6.2. POLICY 31
   6.3. RESPONSIBILITIES 34
7. APPENDIX A 36
   7.1. ACRONYMS 36
8. APPENDIX B 37
   8.1. GLOSSARY 37
9. APPENDIX C 46
   9.1. REFERENCES 46

1. PERSONNEL/USER SECURITY

1.1. PURPOSE AND SCOPE

1.1.1. This section provides policy and guidance on implementing minimum requirements concerning the staffing of positions that interact with all Information Technology (IT) System resources; the administration of users on a system, including considerations for terminating user access; and special considerations that may arise when contractors or other non-agency individuals have access to the Agency IT System resources.

1.1.2. The policy contained in this section is mandatory for all organizational units, employees, contractors, and others having access to and/or using the IT System resources of the Agency.

1.2. BACKGROUND

1.2.1. Many important issues in computer security involve users, designers, implementers, and managers. A broad range of security issues relates to how these individuals interact with computers and the access and authorities they need to do their job. No IT System can be secured without properly addressing these security issues.

1.2.2. DoIT security policy..... requires that each system establish a set of "Rules of Behavior". The security required by the rules is only as stringent as necessary to provide adequate security for the system and the information it contains.

1.3. POLICY

1.3.1. **Staffing:** The Agency's agency staffing process involves, at a minimum, the following steps which apply equally to all users of the Agency's IT System resources:

1.3.1.1. Position definition. Identify and address security issues early in the process of defining a position. Once a position has been broadly defined, the responsible supervisor determines the type of computer access needed for the position. There are two general security rules to apply when granting access:

- Separation of duties. **NOTE:** This phrase refers to dividing roles and responsibilities so that a single individual cannot subvert a critical function. For example, in financial systems, no single individual shall normally be given authority to issue checks. Rather, one person initiates a request for a payment and another authorizes that same payment.

- Least privilege. **NOTE:** This phrase refers to the security objective of granting users only those accesses they need to perform their official duties.

1.3.1.2. Determining position sensitivity:

- Supervisors, with assistance from the CISO and Human Resources Management analyze all positions, establish their sensitivity level designation, and document them with a Position Sensitivity Level Designation.
- The Office Head, or designee (e.g., Director, Human Resources Management), signs the appropriate form.

1.3.1.3. The following positions will be designated no lower than moderate risk:

- Office and unit CISO(s) and alternates
- Individuals having either programmer privileges or the ability to create and add users and/or menus to establish file access for IT System resources that process sensitive data

1.3.1.4. Position descriptions must be written or annotated to reflect specific security responsibilities and position sensitivity levels. Within this context, "specific security responsibilities" refer to employee obligations to protect sensitive data and to use such data and information derived from it only in the execution of official duties.

1.3.1.5. All other individuals with IT System resource access (e.g., contractors, volunteers) must meet the requirements of government employees performing similar duties.

1.3.1.6. Screening – Background screening helps determine whether a particular individual is suitable for a given position.

- The appropriate investigation will be requested by the office to ensure the screening of all individuals (including non-the Agency individuals, (e.g. contractors, volunteers, work-studies) before they are granted access to sensitive data or are allowed to participate in the design, operation or maintenance of sensitive information systems.
- The level of screening required varies from minimal checks to a full background investigation depending on the sensitivity of the information to be handled or the risk and magnitude of loss or harm that could be caused by the position.
- It is more effective to use separation of duties and least privilege to limit the sensitivity of the position, rather than relying on screening to reduce the risk to the organization.
- The Emergency Preparedness and Administration Security Office have issued a "Security and Risk Designation, Appendix A", that establishes guidelines with regard to position sensitivity designation, risk levels and corresponding security investigation requirements.

1.3.1.7. Employee Training and Awareness

- Employees will be trained in the computer security responsibilities and duties associated with their jobs.
- For more training requirements, see Operations Handbook Section 3. "Education, Training, and Awareness".

1.3.2. **User Administration:** The Agency agencies must ensure effective administration of users' computer access to maintain system security, including user account management, auditing and the timely modification or removal of access.

1.3.2.1. User Account Management

- The Agency office management designates and records individuals authorized to issue access to IT System resources and data.
- The Agency Management, or their designee(s), sponsors user access for all users, including non Agency users and recommends access by the CIO. A written and signed request (electronic or paper form) for user access by management, or designee(s), constitutes management approval to initiate a request for access to any sensitive IT System resource. Management ensures that such requests meet the following criteria:
    - The request contains name, organization (or name of contracting company and contract number if applicable), location, purpose for access, and access requirements.
    - The individual must have an Agency need-to-know (i.e., access is an operational necessity) documented in the request.
    - The IT System security features have the capability to restrict the user's access to only information and/or functions appropriate for the authorized activities.
- The office CISO or designee reviews all approved requests.
- Requests for access to remote systems and networks not under the agency management control (i.e., Automation Center) must be routed through the CISO prior to approval.
- Access requirements to information systems by auditors, consultants, representatives of hardware and software vendors, communication company employees, volunteers, work-study students, and other members of the general public must meet or exceed those requirements established for the Agency employees.
- Procedures will be established at the Agency agencies that require all users to sign an "Access Notice" (electronic or paper copy) before actual computer access is granted.

- The rules of behavior cited in Circular A-130, Appendix III clearly delineate responsibilities and expected behavior of all individuals with access to the system. The rules:
  - State the consequences of inconsistent behavior or noncompliance.
  - Should be in writing and form the basis for security awareness and training.
  - Will be available to every user prior to receiving authorization for access to the system.
  - Will be incorporated into the "access notice" for each system.
- Each agency will establish procedures for identifying, managing (adding and deleting users), recording, and monitoring who has access to sensitive IT System resources.
- The process of distribution of access codes will be controlled by the CISO and may be delegated to a designee.
- If access codes cannot be issued directly to users, a secure method for delivery will be established.

1.3.2.2. **Audit and Management Reviews:**

- The Agency IT offices ensure that user access and privileges are reviewed at least every 90 days for appropriate level of access/continued need.
- Reviews examine the levels of access of each individual, conformity with the concept of least privilege, whether all accounts are still active, whether management authorizations are up to date, and whether required training has been completed.

1.3.2.3. **Temporary Assignments, In-house Transfers, and Terminations:**

- Access authorizations are typically changed under two types of circumstances: (1) change in job role, either temporarily (e.g., while covering for an employee on sick leave or training a new employee) or permanently (e.g., in-house transfer) and (2) termination.
- Although necessary, temporary access authorizations should be granted sparingly and monitored carefully, consistent with the need to maintain separation of duties for internal control purposes. The access must be removed promptly when no longer required.
- Permanent changes are necessary when employees change positions within an organization. In this case, the process of granting account authorizations described earlier will occur again. The Agency offices must establish a procedure to ensure that access authorizations of the prior position be removed.

- Terminations of a user's system access generally can be characterized as either "friendly" or "unfriendly." Security issues must be addressed in both situations.
  - Friendly termination can occur when an employee is voluntarily transferred, resigns, or retires. Security issues must be addressed in all situations. Local "friendly" termination procedures will include:
    - a. Removal of access privileges to all IT System resource accounts
    - b. Control of keys
    - c. Briefing on the continuing responsibilities for confidentiality and privacy
    - d. Return of property
    - e. Continued availability of data. In both the manual and the electronic worlds, this may involve documenting procedures or filing schemes, such as how documents are stored on the hard disk, and how are they backed up. Employees should be instructed whether or not to transfer important data from their PC to appropriate personnel before leaving. If cryptography is used to protect data, the availability of cryptographic keys to management personnel must be ensured.
  - Unfriendly termination may include situations when the user is being removed from duty or involuntarily transferred and there is a reasonable belief that IT System resources could be abused or misused. Local "unfriendly" termination procedures will include:
    - a. Termination of system access at the same time (or just before) the employees are notified of their dismissal or upon receipt of resignation.
    - b. When an employee notifies an organization of a resignation and it can be reasonably expected that it is on unfriendly terms, system access should be immediately terminated.
    - c. If applicable, during the "notice of termination" period assign the individual to a restricted area and function. This may be particularly true for employees capable of changing programs or modifying the system or applications.
    - d. In some cases, physical removal from the offices may be necessary.

1.4. RESPONSIBILITIES

1.4.1. **The Agency IT Manager** ensures that agencies within the network are in compliance with personnel security procedures as described in this section.

1.4.2. **Office Heads, and Regional Agency Directors**: ensure that ALL positions are assigned a proper sensitivity level designation based on information security criteria, such as computer related responsibilities, type of data to which the individual has access, a reasonable analysis of the risk, and principles of responsible management.

1.4.3. **Senior Management/Human Resources** analyze all positions, establish their sensitivity level designation, and document designation with a Position Sensitivity Level Designation. The Office Head or designee (e.g., Director, Human Resources) will sign the appropriate form.

1.4.4. **Human Resources**:

- Ensure that documentation for background investigations for identified positions are maintained in each employee's personnel file.
- Notify Agency CISO of all terminations and transfer of in-house employees.

1.4.5. **Supervisor or designee(s)**:

- Annually review the position description and performance standards with each employee occupying a position designated as sensitive.
- Discuss specific information security responsibilities with the employee.
- Discuss with the employee the consequences of noncompliance with those security responsibilities for the employee's particular position.
- Monitor temporary access authorizations and notify CISO when access should be terminated.

1.4.6. **The Agency Information Security Officer(ISO)/Alternate ISO**:

- Ensure access control procedures are in place for temporary access, permanent changes, and termination (friendly and unfriendly) of users. This will be confirmed by regular review and audit.
- Ensure that "rules of behavior" in accordance with DoIT policies and procedures have been established for all IT Systems.
- Ensure that "access notices/rules of behavior" have been reviewed and signed by all users prior to being granted access to the agency's IT Systems.

- Maintain "access notices/rules of behavior" for all individuals accessing the IT System resources.
- Maintain a list of all individuals granted system access, including remote access.
- Ensure that all positions have an established sensitivity level designation.

1.4.7. **Designee(s)** must distribute appropriate application menus and access privileges.

2. INCIDENT REPORTING

2.1. PURPOSE AND SCOPE

2.1.1. This section establishes mandatory procedures for IT Systems' security incident reporting within the Agency. It is designed to provide the Agency personnel the procedures for the proper response to an efficient and timely reporting of computer security related incidents, (e.g. major computer viruses, unauthorized user activity, and suspected compromise of the Agency data). These procedures are intended to meet required mandates of the Agency and to assist in the protection of the Agency IT System resources from unauthorized access, disclosure, modification, destruction, or misuse.

2.1.2. An IT System security incident reporting system is necessary to identify a violation or incident, assess damage as a consequence of a violation, record the violation or incident, investigate and report the incident, and use information to prevent future occurrences or violations. The reporting process outlined in these procedures is intended to detect and respond to IT System security incidents as they occur, assist in preventing future incidents through awareness, and when combined with existing IT System security procedures, augment the Agency IT System security controls.

2.1.3. The policy contained in this section covers all the Agency IT System resources whether maintained in-house or in the interest of the Agency. These policies are mandatory on all organizational units, employees, contractors, and others having access to and/or using the IT System resources of the Agency

2.2. BACKGROUND

2.2.1. Incident Response is a requirement of the Office of Management and Budget () Circular A-130, "Management of Federal Information Resources," Appendix III. Responding to computer security incidents is generally not a simple matter. This activity requires technical knowledge, communication and coordination among staff responding to the incident, and adherence to applicable the Agency policy. Incidents over the last few years indicate that, if anything, responding to incidents is increasingly more complex. Intrusions into machines are a serious concern, and increasing sophistication and collaboration among network attackers pose a considerable threat to the integrity of computing resources. Viruses will continue to occasionally infect the Agency computers, despite widespread availability of virus detection and eradication software.

2.3. POLICY/PROCESS

2.3.1. Security Incident Standards

2.3.1.1. An incident refers to a computer security problem arising from a threat. Computer security incidents can range from a single virus occurrence to an intruder attacking many networked systems, or such things as unauthorized access to sensitive data and loss of mission-critical data.

2.3.1.2. IT System security incidents to be reported and tracked can be categorized as follows (these types of acts are not all-inclusive):

- Circumvention of IT System security controls, safeguards and/or procedures
- Unauthorized access, use, disclosure, alteration, manipulation, destruction, or other misuse of data and AIS
- Theft, fraud, or other criminal activity committed with the aide of IT System resources
- Theft, loss or vandalism of IT System hardware, software or firmware
- Issues affecting confidentiality, integrity and availability of data
- Unauthorized downloading or copying of sensitive Agency information

2.3.1.3. **Examples** of specific reportable incidents which are to be reported under the six categories of incidents include (but are not limited to):

- Unauthorized access to or use of sensitive data for illegal purposes
- Unauthorized altering of data, programs, and IT System hardware
- Loss of mission-critical data
- Environmental damage/disaster (greater than $10,000) causing loss of IT System services or data, or which may be less than $10,000 in damage yet have affected the Administration's or staff office's capabilities to continue day-to-day functions and operations
- Major infection of sensitive systems or software by malicious code, i.e. virus, Trojan Horse, etc
- IT System perpetrated theft, fraud and other criminal computer activity;
- Telecommunications/network security violations, i.e., networks (including local area networks (LANs) and wide area networks (WANs)) which experience service interruptions that cause an impact to an indefinite number of end users

- Theft or vandalism of IT System hardware, software or firmware whose loss did or may affect the organization's capabilities to continue day-to-day functions and operations
- Unauthorized access to data when in transmission over communications media (e.g. sniffers)
- Loss of system availability impacting the ability of users to perform the functions required to carry out day-to-day responsibilities (e.g. denial of service attacks)
- Unauthorized access to and/or unauthorized use of the Internet

2.3.2. **Reporting Procedures**

2.3.2.1. The person observing or discovering the incidents, as defined above, advises their supervisor or the office ISO as soon as possible. The office CISO is responsible for recording and reporting security incidents. Additionally, those incidents which are determined to affect a agency's capability to accomplish critical functions, restrict the availability of a system or communications medium, i.e. LAN, WAN, etc., or result in a monetary impact to the agency, will be reported within 48 hours of the occurrence to the Agency Information Security Officer. Depending on the severity and the nature of the incident, the Agency CISO may also contact the Agency General Counsel, and the Office of the Inspector General (OIG), and FedCIRC.

2.3.2.2. Reportable IT System security incidents are recorded on a security incident form or log as developed by the office. Essential information about the security incident will be identified in as much detail as possible, at the time of occurrence. Some information may need to be added at a later time based on the investigation/closure of the incident. The following minimum information about a security violation or incident will be entered on the IT System security violation/incident form:

- Location of incident and organization filing report
- Reported by (Name, Title and Organization)
- Date and time of report filing
- Date and time of incident
- Details of incident (include names of personnel involved and description of the who, what, when, where, how, and why)
- The name and title of the person to whom the incident initially was reported
- Identification of whether the Inspector General or appropriate law enforcement organization has been notified
- Incident impact on day-to-day operations

- Action taken to contain the incident and resources required to correct the incident (in cases of system outage note what vendors have been contacted)
- Short-range corrective action, such as immediately removing a terminated employee's access privileges
- Long-range corrective actions, as necessary
- Estimated monetary damage
- Additional information, as appropriate

2.3.2.3. The information collected on the IT System security incident form is reported to the Agency Information Security Officer (ISO) in a confidential manner.

- Initial reports of serious incidents or violations may be reported by telephone.
- Reports may be sent by U.S. mail using the double-envelope method, couriers, or secured electronic mail or facsimile.
- Follow-up contact will be established with the reporting unit or office by the CISO, and tracking for each incident will be continued until final closure.
- Each office or unit ISO will be responsible for making the determination of whether the IT System security incident at their level is reportable based on the definitions provided in this procedure and ensuring that reports are filed with the Agency ISO.

2.3.2.4. **Protection of Report Information**: IT System security incident report information will be treated as sensitive information and safeguarded as equivalent to Privacy Act information. Access to IT System security incident information must be restricted and stored in a secured area.

2.3.3. **Tracking of IT System Security Incidents**

2.3.3.1. The ISSO is responsible for tracking IT System security violations and incidents for the Agency. Tracking includes monitoring each incident through final closure and maintaining a copy of the incident report for a period of three (3) years. The ISSO reports those security violations and incidents which threaten critical organization functions to the office of the e Agency Information Security Officer (ISO).

2.3.3.2. **Reporting of Security Incidents and Violations to the Media:** The Agency offices must refer questions from the media (e.g., newspapers, television, and radio) concerning IT System security violations or incidents to the Agency Public Affairs Office.

2.4. RESPONSIBILITIES

2.4.1. **Agency ISO**:

- Ensures that the Agency policy, procedures, and standards meet the Agency requirements outlined in the Agency's corresponding Handbook.
- Provides guidance and assistance to the Agency offices in preparing their IT System Security Incident Reporting policy, procedures, and standards to comply with the Agency policy.
- Provides assistance, upon request, and as needed, to the Agency offices in dealing with both the administrative and technical aspects of reportable IT System security incidents. The Agency Information Security Officer (ISO) is the initial point of contact for each office.
- Organize an incident response team, as needed, to assist sites with IT System security incidents.
- Report incidents that are determined to affect the Agency's overall capability to accomplish critical functions; restrict the availability of a system or communications medium; or result in a monetary impact to the Agency' s Information Resources Security Officer (ISO).

2.4.2. **The Office of the General Counsel**:

- Interprets laws, regulations, and directives applicable to the Agency IT System security activities, and specific to IT System incident occurrences and reporting of those occurrences.
- Renders legal advice and other legal services with respect to IT System security incidents.

2.4.3. **The Office of the Inspector General**:

- Investigates and audits major IT System security incidents when appropriate, and conducts criminal investigations, as warranted.
- Provides advice on coordinating an investigative process for IT System security incidents and reconciliation of those incidents.

2.4.4. **The Agency CIO**: The Agency CIO ensures that the provisions of this section are implemented at all agencies within the Agency.

2.4.5. **Office Heads, and Regional Agency Directors**:

- Implement the IT System security requirements at their office or agency.
- Ensure that the office or unit ISO investigates, reviews, and records IT System security incidents and notifies the Agency Information Security Officer when a reportable incident, as defined above, occurs.

2.4.6. **The Information Security Officer(ISO)/Alternate ISO**:

- Establishes the office IT System security incident reporting system.
- Logs, investigates, and reviews IT System security incidents and reports the incidents to the appropriate the Agency Information Security Officer.
- Establishes contact with the Agency incident response team when a reportable incident occurs as defined earlier in this section.

2.4.7. **Managers and Supervisors**:

- Implement the requirements of the unit's IT System security incident reporting procedures within their assigned areas of management control.
- Ensure that IT System security violations/incidents, occurring within their assigned area of management control, are reported to the appropriate agency ISO.
- Ensure on a regular basis that all assigned employees, contractors and other individuals, who develop, operate, administer, maintain, or use the Agency IT System resources understand they are responsible for reporting actual or suspected IT System security incidents to their immediate supervisor or office ISO.

2.4.8. **All the Agency Employees, contractors, and other individuals** with access to sensitive areas or IT Systems are responsible for reporting IT System security violations or incidents to their supervisor and/or ISO.

3. EDUCATION, TRAINING AND AWARENESS

3.1. PURPOSE AND SCOPE

3.1.1. This section provides policy and guidance for offices in establishing their security awareness and training program. To protect the integrity, confidentiality, and availability of information, the Agency offices will ensure that each person involved understands their roles and responsibilities and is adequately trained to perform them.

3.1.2. The procedures and responsibilities described in this handbook apply to all the Agency organizational units, employees, contractors, and others having access to and/or using the IT System resources of the Agency.

3.2. BACKGROUND

3.2.1. The Computer Security Act of 1987 (Public Law 100-235) requires that "each agency must provide for the mandatory periodic training in computer security awareness and accepted computer practices of all employees who are involved with the management, use, or operation of each Federal computer system within or under the supervision of that agency".

3.2.2. In accordance with the Computer Security Act of 1987, the National Institute of Standards and Technology (NIST) working with the U.S. Office of Personnel Management (OPM) was charged with developing and issuing guidelines for Federal computer security training. This requirement was satisfied by NIST's issuance of "Computer Security Training Guidelines" (Special Publication 500-172).

3.2.3. In January 1992, OPM issued a revision to the Federal personnel regulations making these voluntary guidelines mandatory. This regulation, 5 CFR Part 930, is entitled "Employees Responsible for the Management or Use of Federal Computer Systems" and requires Federal agencies to provide IT System security training as set forth in NIST guidelines.

3.2.4. In 1998, the Office of Management and Budget () Circular A-130, "Management of Federal Information Resources," Appendix III, "Security of Federal ITResources," re-enforced these mandatory training requirements and added additional requirements.

3.2.5. Due to the revision of Circular A-130, Appendix III, NIST issued a new publication in April 1998, which superseded Special Publication 500-172. This new publication, NIST Special Publication 800-16, "Information Security Training Requirements: A Role- and Performance-Based Model" presents a new conceptual framework for providing IT System security training. This publication is available on the Agency Information Security web site.

3.3. POLICY

3.3.1. IT System Security awareness training is required for:

- New employees within 60 days of hire
- All users on an annual refresher basis
- Whenever there is a significant change in the IT System security environment or procedures
- When an employee enters a new position that deals with sensitive information

3.3.2. Initial User Awareness Training

3.3.2.1. Each employee (the Agency employee, contractors, and all other individuals using IT System resources) must attend or receive some form (e.g. computer based training [CBT] or video) of initial IT System security awareness training prior to being granted access to the Agency systems. The user must understand the basic purpose of the Information Security Program and its implementation before IT System access is granted. At a minimum, the users must understand the following IT System security components:

- IT System Security Policy
- Confidentiality
- Password Security; Logging Off; Multiple Sign-Ons
- Appropriate IT System Security Behaviors
- Identification of CISO
- Malicious Software
- Email hoaxes
- Back-ups (where appropriate)
- Internet Use
- Software licensing
- Email manners
- Expectations of privacy
- Incident reporting
- Telecommunication Security

- Network Overview
- Remote sign-on
- Physical security
- Disposal of Sensitive Information
- Repercussions of misuse of IT System resources

3.3.3. Attendance at all security training will be documented for each employee and placed in the employee's personnel file.

3.3.4. Continuing Training

3.3.4.1. As part of an effective information security training program, the office or unit will also provide an ongoing security awareness program for all users. Awareness activities may include:

- Distribution of IT System security pamphlets and flyers
- Viewing of IT System security videos
- Dissemination of security posters throughout the agency
- Security articles in the site's newsletters, daily bulletins, web pages, etc

3.3.4.2. Each user is required annually to review the station information security policy and/or procedures

3.3.5. In addition to the initial orientation awareness training and ongoing security awareness activities, the user (e.g., employee, trainee, contractor, volunteer, etc.) will receive continuing training annually in additional aspects of information security as it relates to the requirements of the duties of the individual. Depending upon an individual's responsibilities, the following is a list of possible training subjects:

- Laws and Regulations
- IT System Security Program
- System Environment
- System Interconnection
- Information Sharing
- Sensitivity
- Risk Management
- Management Controls

- Acquisition/Development/Installation/Implementation Controls
- Operational Controls
- Awareness, Training, and Education Controls
- Technical Controls
- Contingency Plans
- Internet/Intranet

3.3.6. The supervisor will assess the need for appropriate information security training as the employee's position changes or is revised. Employees will be solicited for ideas on how to improve information security in the agency. NOTE: *Everyone should be encouraged to view information security as a positive procedural tool ensuring the* confidentiality, *integrity, and availability of the Agency IT System systems.*

3.3.7. The Agency's standard for developing and conducting IT System security awareness and training for the Agency employees is NIST's Special Publication 800-16, "IT Security Training Requirements: A Role- and Performance-Based Model".

3.4. RESPONSIBILITIES

3.4.1. **The Agency CIO:** Ensures that the provisions of this section are implemented at all agencies within the Agency.

3.4.2. **Office Heads, and Regional Agency Directors**:

- Ensure that their office has an information security training program that is effective, dynamically applicable, and documented.
- Ensure that information security is presented in a positive, cost-effective way.
- Participate in orientation and continuing education activities to emphasize support for the information security program.
- Ensure there is a method established office-wide to document IT System security training in each employee's personnel folder.

3.4.3. **The DoIT Chief Security Officer (CISO)**:

- Provides assistance and support to the ISOs within the Agency,
- Reviews the site's security awareness and training programs during scheduled security audits.

3.4.4. **Agency Information Security Officer(ISO)/Alternate Information Security Officer(AISO)**:

- Ensures that an information security orientation is presented during new employee entry processing.
- Maintains documentation of employee awareness and refresher training.
- Ensures that additional specialized training is provided as required. This will be accomplished by working with the supervisors, and with the assistance of the respective ISO, and the Agency.
- Monitors the Information Security Awareness Program and recommends policy and procedure. Specific information security responsibilities will be documented in each position description and consequences of noncompliance to information security procedures will be implemented according to current Human Resources directives concerning employee conduct.
- Distributes State provided information security training to the agency staff as it becomes available and works closely with supervisors to disseminate this information.

3.4.5. **Supervisors**:

- Ensure that employees who have functional responsibilities in information security areas (e.g., ISO and system administrators) are given the opportunity to attend security training lectures, courses, conferences, etc.
- Provide copies of the Agency IT system security policy and rules of behavior to the employee and discuss with the employee how they relate to the employee's specific position.
- Assess the need for appropriate information security training of an employee as assignments change or as a position is revised.

3.4.6. **Agency employees and other users**:

- Attend security orientation training and any other specifically assigned IT System security training, as required, to fulfill their role.
- Annually review the information security policy and rules of behavior appropriate to the use of the Agency IT.

4. SECURITY CONSIDERATIONS IN COMPUTER SUPPORT OPERATIONS

4.1. PURPOSE

4.1.1. This section provides guidance for computer support and operations. The primary goal of computer support and operations is the continued and correct operation of a LAN/WAN computer system. The closely linked goals of computer security are the availability, confidentiality, and integrity of systems.

4.1 *BACKGROUND*

4.1.2. Computer support and operations refers to everything required to run a computer system to include both system administration and tasks external to the system that support IT operation (e.g., maintaining documentation). The support and operation of any computer system is critical to maintaining the security of a system. Support and operations are routine activities that enable computer systems to function correctly. These include fixing software or hardware problems, loading and maintaining software, and helping users resolve problems.

4.1.3. The failure to consider security as part of the support and operations of computer systems is, for many Agencies, their Achilles heel. Agencies often undermine their expensive security measures because of poor documentation, old user accounts, conflicting software, or poor control of maintenance accounts. Also, agencies' policies and procedures often fail to address many of these important issues.

4.1.4. The important security considerations within some of the major categories of support and operation are:

- User support
- Software support
- Hardware support
- Configuration management
- Backups
- Media Controls
- Documentation
- Maintenance

4.2. POLICY

4.2.1. **User Support**

- (User Support Services) provides Agency user support. An important security consideration for user support personnel is the ability to recognize which problems are security related.
- System support and operations staff must be able to identify security related problems, respond appropriately, and inform appropriate individuals. A wide range of possible security problems exists. Some will be internal to the Agency applications, while others apply to off-the-shelf products. Additionally, problems can be software or hardware based.
- User support must be closely linked to the organization's incident handling capability. In many cases, the same personnel perform these functions.

4.2.2. **Software Security and Support Elements**

4.2.2.1. Controlling what software is used on a system.

- All executable software used on sensitive the Agency IT System resources must be obtained through authorized channels.
- Each system installation of the Agency-developed or off-the-shelf software must be reviewed and approved for determination of need and system compatibility, prior to installation. This includes software acquired by any other means (e.g., public domain software, bulletin board services, personally owned software, Internet obtainable freeware).
- Executable software authorized to run on an Agency IT System resource must be identified in the system's security plan.

4.2.2.2. Ensuring that software has not been modified without proper authorization.

- There must be no local modification of security software features.
- Willful and intentional modification of the Agency software for illegal or disruptive purposes or for personal gain is a crime. There will be no modifications of these programs except through authorized channels.
- Safeguards must be in place to detect and minimize inadvertent or malicious modification or destruction, or attempts to do so, of the Agency's IT System application software, operating system software, and critical data files. The safeguards will achieve the integrity objectives and be documented in the system's security plan. The level of protection will be commensurate with the sensitivity of the information processed.

- All approved software, regardless of source, will be scanned for viruses prior to use. Virus and malicious code (software) prevention and control measures will be employed on every Agency IT System resource to protect the integrity of the software and data.

4.2.2.3. Ensuring that software is properly licensed.

- Use of copyrighted software will comply with copyright laws and license agreements. See the Agency 802, Appropriate Use of the Agency Office Equipment, and the Agency 815, New Desktop Software Requests.
- The Agency licensed software may not be taken home without management approval.

4.2.3. Hardware Security and Support Elements

4.2.3.1. Hardware support will be under the direction of Agency User Support (or its equivalent) or DoIT Service Desk.

4.2.3.2. Security measures must be taken by all users to protect against theft and unauthorized use of IT System peripheral and communications devices, computers, and related items such as printers, disks, and software.

4.2.3.3. The removal of peripheral or communication devices from an agency for use off-site must be controlled. Appropriate documentation will be maintained of all IT System equipment and software removed from the agency, including the individual responsible for the equipment and the date(s) the equipment was removed and returned to the agency. NOTE: Remote off-site (e.g., dial-in) access to a computer system must be authorized

4.2.3.4. All physical security requirements (e.g., key and cypher lock hardware, security surveillance television equipment, room intrusion detectors), as identified in the risk analysis, which may be deemed necessary by the agency ISO to protect peripheral devices and microcomputers, will be compatible with and, when possible, integrated into the agency's security system.

4.2.3.5. Locks and access control procedures will be used to protect storage media containing sensitive data.

4.2.3.6. For those systems where virus protection is applicable, such protection must be current and enabled.

4.2.4. Configuration Management

4.2.4.1. Agencies must practice configuration management. Configuration management:

- Manages changes made to a system's hardware, software, documentation, and tests throughout the life of a system.

- Identifies, documents, and verifies the functional and physical characteristics of an IT System, recording its configuration, and controlling changes to the System and its documentation.
- Ensures that changes to the system do not unintentionally or unknowingly diminish security.

4.2.4.2. Configuration management will provide a complete audit trail of decisions and design modifications.

4.2.4.3. A Configuration management plan will include:

- A baseline that includes the controls for changes to IT System resources, including hardware, software, administrative requirements, documentation, and connectivity to another IT System or LAN.
- A current list of all components of the IT System (hardware, software, and their documentation).
- The configuration of the peripherals (printers, modems) and interconnections to other IT Systems (shared printers, file servers) and LANs.
- Listing of version releases of current software, information on batch files, environmental settings such as paths, and switch settings of machine components.

4.2.4.4. All the Agency IT Systems will employ configuration management at a level appropriate with the size, complexity, and sensitivity of the system.

4.2.5. Backups

4.2.5.1. Backup of IT System resources must be done on a periodic basis.

- Support and operations personnel backup major systems' software and data.
- Users of smaller systems are responsible for their own backups.
- Agencies may task support personnel with making backups periodically for smaller systems, either automatically (through server software) or manually.

4.2.5.2. Backups are critical to contingency planning and all users must be provided adequate awareness training on the importance of backing up data as well as the appropriate method for backing up their data, if this function is their responsibility.

4.2.5.3. Frequency of backups will depend upon how often data changes and how important those changes are.

4.2.5.4. Backup procedures must be periodically tested to ensure that copies work as intended..

4.2.5.5. Backups will be stored securely.

4.2.6. **Media Controls**. Media controls will be utilized to protect IT System resources. Media controls include a variety of measures to provide physical and environmental protection and accountability for tapes, disks, printouts, and other media. From a security perspective, media controls will be designed to prevent the loss of confidentiality, integrity, or availability of information, including data or software, when stored outside the system. This can include storage of information before it is input to the system and after it is output. The extent of media control depends upon many factors, including the type of data, the quantity of media, and the nature of the user environment. Physical and environmental protection is used to prevent unauthorized individuals from accessing the media. It also protects against such factors as heat, cold, or harmful magnetic fields.

4.2.6.1. **Marking/physical labeling.**

- Use labels to identify media with special handling instructions, to locate needed information, or to log media to support accountability. Identification is often by colored labels on diskettes or tapes or banner pages on printouts.
- If labeling is used for special handling instructions, users must be appropriately trained. The marking of IT System input and output is generally the responsibility of the user, not the system support staff. Typical markings for media could include Privacy Act Information or Joe's backup tape. In each case, the individuals handling the media must know the applicable handling instructions. For example, Joe's backup tape should be easy to find in case something happens to Joe's system. Also marking backup diskettes can help prevent them from being accidentally overwritten.

4.2.6.2. **Logging:** The logging of media will be used to support accountability. Logs can include control numbers (or other tracking data), the times and dates of transfers, names and signatures of individuals involved, and other relevant information. Periodic spot checks or audits may be conducted to determine that no controlled items have been lost and that all are in the custody of individuals named in control logs.

4.2.6.3. **Physical Access Protection**: As media can be stolen, destroyed, replaced with a look-alike copy, or lost, physical access protection must be utilized by agencies to protect their IT System resources. Physical access controls include locked doors, desks, file cabinets, or safes.

- If the media requires protection at all times, ensure the output data goes to a medium in a secure location (e.g., printing to a printer in a locked room instead of a general-purpose printer in a common area).
- Physical protection of media must be extended to backup copies stored offsite. Back-up copies will be accorded an equivalent level of protection to media containing the same information stored onsite. (Equivalent protection does not mean that the security measures need to be exactly the same. The controls at the off-site location are quite likely to be different from the controls at the regular site.)

4.2.6.4. **Environmental Protection:** Magnetic media, such as diskettes or magnetic tape, will be provided environmental protection, since they are sensitive to temperature, liquids, magnetism, smoke, and dust. Other media (e.g., paper and optical storage) will have different sensitivities to environmental factors and should be protected accordingly.

4.2.6.5. **Transmittal:** Media transferred within the agency and to outside elements must be secured during transmittal. Possible methods include sealed and marked envelopes, authorized messenger or courier, or U.S. certified or registered mail.

4.2.6.6. **Disposition:** Ensure that information is not improperly disclosed when media is disposed. This applies both to media that is external to a computer system (such as a diskette) and to media inside a computer system, such as a hard disk. The process of removing information from media is called sanitization. One of the following three techniques must be used by agencies in disposing of their media:

- Overwriting. Overwriting uses a program to write (1s, Os, onto the media. Common practice is to overwrite the media three times. Overwriting should not be confused with merely deleting the pointer to a file (which typically happens when a *delete* command is used). Overwriting requires that the media be in working order.
- Degaussing. Degaussing is a method to magnetically erase data from magnetic media. Two types of degaussers exist: strong permanent magnets and electric degaussers.
- Destruction. Destruction is shredding or burning.

4.2.6.7. **Documentation:** Documentation of all aspects of computer support and operations must be maintained to ensure continuity and consistency. Formalizing operational practices and procedures with sufficient detail helps to eliminate security lapses and oversights, gives new personnel sufficiently detailed instructions, and provides a quality assurance function to help ensure that operations will be performed correctly and efficiently.

- The security of a system must be documented. This includes many types of documentation, such as security plans, contingency plans, risk analysis, and security policies and procedures. Much of this information, particularly risk and threat analyses, has to be protected against unauthorized disclosure. Security documentation needs to be both current and accessible. Accessibility should take special factors into account (such as the need to find the contingency plan during a disaster).
- Security documentation must be designed to fulfill the needs of the different types of people who use it. Agencies should have locally developed *policy* and *procedures*. Policy is outlined in Section 1 of the the Agency IT System Handbook – Management Controls. Security procedure manuals are written to inform various system users how to do their jobs securely. A security procedures manual for

systems operations and support staff will address a wide variety of technical and operational concerns in considerable detail.

4.2.6.8. **Maintenance:** System maintenance requires either physical or logical access to the system. If someone who does not normally have access to the system performs maintenance, then a security vulnerability is introduced.

- Procedures must be developed to ensure that only authorized personnel perform maintenance. IT System technical support and maintenance work performed at the Agency agencies (on-site) must be supervised by or under the control of the Agency personnel knowledgeable in appropriate IT System operations.
- Automated (i.e., computer-connected) dial-up diagnostic maintenance of sensitive the Agency systems via remote communications between vendors and the Agency IT System resources is prohibited unless authorized by management in the system's accreditation. If authorized, authentication of the maintenance provider by the system prior to access is required.
- If a system has a maintenance account, it is critical to change factory-set passwords or otherwise disable the accounts until they are needed.

4.3. RESPONSIBILITIES

4.3.1. **Agency CIO:** Ensures that the provisions of this section are implemented at all agencies within the Agency.

4.3.2. **Agency ISO:** Ensures that the Agency policy, procedures, and handbooks reflect the Agency, Federal and generally accepted principles and practices for security IT Systems.

4.3.3. **Office Heads, and Regional Agencies Directors**: Ensure that adequate support and funding are provided to support their IT System functions and are ultimately responsible for the security for systems under their management control.

4.3.4. **Office, Library, and Regional CIOs**: Implement adequate computer support to the unit's systems and to the users.

4.3.5. **System Administrators:** Ensure that the controls described above are maintained for their assigned systems and are responsible for day-to-day operations.

4.3.6. **Information Security Officer (ISO)/Alternate Information Security Officer (AISO)**: Assist the support and operations staff in performing their duties and responsibilities as outlined in this section.

5. PHYSICAL/ENVIRONMENTAL SECURITY

5.1. PURPOSE AND SCOPE

5.1.1. This section provides policy and guidance to implement minimum requirements that will reduce the exposure of computer equipment to physical and environmental damage and assist in achieving an optimum level of protection for the Agency IT Systems.

5.1.2. The policy contained in this section covers all the Agency IT System resources maintained in-house or in the interest of the Agency. These policies are mandatory and apply to all organizational units, employees, contractors, and others having access to and/or using the IT System resources of the Agency.

5.1.3. This policy applies to all IT Systems currently in existence and any new automated technology acquired after the effective date of this policy document.

5.2. BACKGROUND

5.2.1. In the early days of computer technology, securing the system in a controlled environment with very limited access protected the computers and the information they processed. Although major changes in computer environments have occurred, physical security is still vitally important. Physical security measures are a tangible defense that must be taken to protect the agency, equipment, and information from theft, tampering, careless misuse, and natural disasters.

5.3. POLICY

5.3.1. Staff and equipment require a safe, secure, and technically sound physical environment. While it is necessary to comply with each of the areas addressed, appropriate adjustments or allowances may be made for the organization, physical plant, and any special requirements of the individual office or agency. Deviation from the minimum requirements must be annotated on the system risk assessment and the Office Head or Agency Director must be aware and acknowledge this deviation in the accreditation of the system.

5.3.2. There must be, at a minimum, a cipher lock or suitable substitute on each door to the computer room.

5.3.3. Only personnel who require access to perform their official duties will be permitted in the computer room.

5.3.4. A log will be kept of all personnel who were issued the combination/key to the computer room and the person will be required to sign for that combination/key.

5.3.5. The combination of a cipher lock will be changed frequently, especially when a person who was previously given the combination leaves the organization.

5.3.6. Keys or card keys will be returned to the Agency upon separation, transfer, or termination.

5.3.7. Loss of keys or disclosure of cipher key code will be reported to the ISO immediately.

5.3.8. A computer room access roster will be established.

5.3.9. There will be signs posted designating the room as a "Restricted Area".

5.3.10. Contract maintenance personnel and others not authorized unrestricted access but who are required to be in the controlled area, will be escorted by an authorized person at all times when they are within the controlled area.

5.3.11. All access to the computer room will be logged, and logs reviewed monthly by the ISO to determine if access is still required.

5.3.12. There shall be no signs to indicate that an information system is located in any particular building or area.

5.3.13. The main computer room should have certain structural physical security features. The computer room:

- Should be located in the center of the building
- Should not have windows
- The computer room walls should extend from true floor to true ceiling
- Failure to meet these requirements must be annotated in the risk assessment

5.3.14. Media used to record and store sensitive software or data will be labeled, protected, controlled and secured when not in use.

5.3.15. Physical access controls will also be implemented not only in the area containing system hardware, but also locations of wiring used to connect elements of the system, supporting services (such as electric power), backup media, communications closets, and any other elements required for the system's operation.

5.3.16. It is important to review the effectiveness of physical access controls in each area, both during normal business hours and at other times – particularly when an area may be unoccupied.

5.3.17. A computer room will have appropriate environmental security controls implemented, which include measures implemented to mitigate damage to IT System resources caused by fire, electrical surges and outages, water, and climate control failure.

5.3.17.1. **Fire and Smoke**

- Install smoke detectors near computer equipment – and check them periodically.
- Keep fire extinguishers in and near your computer rooms, and be sure all those with authorized access know where they are and how to use them.
- Enforce no smoking, no eating, and no drinking policies.
- Periodically hold fire drills.

5.3.17.2. Climate

- Keep all rooms containing computers at reasonable temperatures, following manufacturers recommendations.
- Keep the humidity level at 20-30 percent.
- Install gauges and alarms that warn you if the environmental controls are getting out of range. These alarms will be monitored at all times.
- Equip all heating and cooling systems with air filters to protect against dust and other particulate matter.

5.3.17.3. Water

- Protect your systems from the various types of water damage. Flooding can result from rain or ice buildup outside, toilet or sink overflow inside, or water from sprinklers used to fight a fire. Maintain plastic sheeting to protect the equipment if the sprinklers go off.
- Avoid locating computer rooms in the basement.

5.3.17.4. Electricity

- Connect all IT System resources to a non-interruptible power supply (UPS) that is tested periodically.
- Connect all critical IT System equipment to backup emergency generators.
- Install anti-static carpeting in each agency.

- Install a line filter on your computer's power supply. A voltage spike can destroy your computer's power supply.

5.4. RESPONSIBILITIES

5.4.1. **Agency ISO:** Ensures that the Agency policy, procedures, and handbooks reflect the Agency, Federal, and generally accepted principles and practices for the security of IT Systems.

5.4.2. **Agency CIO:** Ensures that the provisions of this section are implemented at all agencies within the Agency.

5.4.3. **Office Heads, and Agency Directors:**

- Ensure procedures are established for identifying and reporting suspected or actual breaches of physical security.
- Ensure that adequate funding is available for IT System physical and environmental controls for elements under their administrative control.
- **User Support**. Helps to develop, in cooperation with the ISO, physical access control procedures for the computer room and other restricted areas. Trains staff on the procedures established.
- **System Administrators.** Comply with access control procedures established for the computer room.
- **ISO/AISO**. Monitors access to the computer room and ensures that the physical access control procedures are established and followed.

6. CONTRACTOR/VENDOR/PARTNER SECURITY

6.1 *PURPOSE*

6.1.1. This section provides policy and guidance on implementing minimum security requirements for conducting the Agency business utilizing contracts, sharing agreements, and memorandums of understanding (MOUs) with companies, vendors, and other federal agencies.

6.1.2. The policy contained in this section covers all the Agency IT System resources maintained in-house or in the interest of the Agency. These policies are mandatory on all organizational units, employees, contractors, and others having access to and/or using the IT System resources of the Agency.

6.1.3. This policy applies to all IT Systems currently in existence and any new automated technology acquired after the effective date of this policy document.

6.1. BACKGROUND

6.1.1. The Agency is increasing the use of contractors and their services as well as entering into inter-agency agreements. This section covers in further detail some of the security requirements and controls that need to be addressed to ensure the confidentiality, integrity, and availability of the Agency's sensitive data and resources.

6.2. POLICY

6.2.1. **Contractor Personnel Security:**

6.2.1.1. Security requirements and specifications for hardware and software maintenance personnel contracted from commercial sources must be defined and approved prior to signing of contractual agreements.

6.2.1.2. Such requirements will vary depending upon the level of trust associated with the equipment or system to be maintained.

6.2.1.3. Maintenance contractors and their employees will be granted limited and controlled access to computer equipment and systems consistent with established security requirements. The access provided must be the MOST restrictive set of capabilities and privileges required to perform the work.

6.2.1.4. Access of contractors to the Agency's sensitive systems must be in the interest of the Agency.

6.2.1.5. Access must be limited to a specified timeframe appropriate to the task and then reviewed for possible termination.

6.2.1.6. The Agency management or their designees must officially sponsor all non-the Agency personnel accessing the Agency resources.

6.2.1.7. All contractors that have access to the Agency's sensitive systems and data must be required to meet the minimum the Agency security requirements outlined in Section 1 "Personnel Security".

6.2.1.8. Contractors must receive the same security training required for the Agency employees, including orientation and periodic security updates.

6.2.1.9. Contractors must indicate in writing that they have read and understand the Agency security requirements applicable to them.

6.2.1.10. Contract personnel who access the Agency IT System resources or data must have a background investigation. For questions concerning approval of contractor investigations, contact the Agency Security Office.

6.2.1.11. The following language is recommended for inclusion in contracts concerning background investigations:

> "The investigative history for contract personnel working under this contract must be maintained in the databases of either the Office of Personnel Management (OPM) or the Defense Industrial Security Clearance Organization (DISCO). Should the contractor use a vendor other than those identified by OPM or Defense Security Service (DSS) to conduct investigations, the investigative company must be certified by OPM/DSS to conduct contractor investigations.
>
> All costs associated with obtaining clearances for contractor provided personnel are the responsibility of the contractor. Further, the contractor will be responsible for the actions of all individuals they employ to work for the Agency under this contract. In the event that damages arise from work performed by contractor provided personnel, under the auspices of this contract, the contractor will be responsible for all resources necessary to remedy the incident."
>
> Contract personnel performing work under this contract shall satisfy all requirements for appropriate security eligibility in dealing with access to sensitive information and information systems belonging to or being used on behalf of the Agency. To satisfy the requirements of the Agency, a Minimum Background Investigation shall be conducted prior to performing work under this contract. The level of access and the individual's capability to perform work under this contract will be the determining factor in deciding if a higher investigative requirement is needed. The contractor shall ensure that those requirements are fully satisfied within 30 days of initiation of such investigations."

6.2.2. **Contracts/Sharing Agreements/Memorandum Of Understanding (MOU)**

6.2.2.1. All management, operational and technical security requirements outlined in the Agency's IT System Security Handbooks shall be included in contract specifications, as applicable, for the acquisition, maintenance, or operation of the Agency IT System resources.

6.2.2.2. All requirements outlined in Circular A-130, Appendix III, will be implemented.

6.2.2.3. Contracts, sharing agreements, and MOUs pertaining to IT System resources will be reviewed by the ISO for security implications prior to initiation of the contract. A separate section in the contract dealing with security issues will be incorporated, where appropriate.

6.2.2.4. If a potential risk to the Agency information resources exists, the ISO must be contacted for advice and documentation of risk.

6.2.2.5. Each the Agency office and agency must ensure that IT System contracts/agreements/MOUs documents include a written requirement that they (e.g., contractor) meet the minimal security clearance levels as outlined in the Agency's IT Systems Security Operations Handbook, Section 1 "Personnel Security".

6.2.2.6. Contracts must stipulate that the contractor will be held responsible for the cost of background investigations. Contractor personnel's background information must be maintained in the databases of either the Office of Personnel Management (OPM) or the Defense Industrial Security Clearance Organization (DISCO). Should the contractor use another vendor other than OPM or Defense Security Service (DSS) to conduct investigations, the investigative company must be certified by OPM/DSS to conduct contractor investigations.

6.2.2.7. Access to the Agency's network in the performance of contract duties and agreements must be outlined in the statement of work and included in the contract. Inbound access to the Agency's network must be secure and meet all requirements as outlined in the Agency's IT System Technical Handbook, Section 3, "Network and Communication Security". Additional costs for implementing a secure connection must be included in the contract, agreement, or MOU.

6.2.2.8. Following are paragraphs of contracting language that may be added to contracts, as required, to ensure that certain areas of security are addressed:

Records:

(Clause to be added if the contractor will have access to records protected by 38 U.S.C.

"Contractor personnel who obtain access to hardware or media which may manipulate or store any sensitive information protected under 38 USC, as defined by the Agency, must not access information unless absolutely necessary to perform their contractual

duties. Disclosure of any sensitive data obtained during the performance of the particular contractual duty is prohibited. Violation of these statutory provisions may involve imposition of criminal penalties."

System of Records:

"The Agency system(s) of records to which the contractor personnel will have access in order to maintain _____(system(s) to be deployed or maintained) is/are (insert title and identity code of the Agency system(s) of records involved).

System Security:

"The Contractor shall provide the Agency with full assurance that security measures have been implemented which are consistent with all the Agency, and other Federal standards and guidelines."

Procedures for User Access:

"Access requirements to the Agency information systems by contractors and contractor personnel shall meet or exceed those requirements established for the Agency employees as described in the Agency's IT System Security Policy the IT System Security Handbooks."

6.3. RESPONSIBILITIES

6.3.1. **Agency ISO:** Ensures that the Agency policy, procedures, and handbooks reflect the Agency, federal and generally accepted principles and practices for security IT Systems.

6.3.2. **Agency CIO**: Ensures that the provisions of this section are implemented at all agencies within the Agency.

6.3.3. **Office Heads, and Agency Directors**: Ensure that adequate contractual controls are implemented for all contracts, agreements, and procurements for which they hold responsibility and are ultimately responsible for the information security for systems in the area under their administrative control.

6.3.4. **CIO//ISO/AISO**

6.3.4.1. Ensures that all IT System security requirements (management, operational, and technical) are reviewed and documented prior to negotiating a contract, agreement, or MOU.

6.3.4.2. Provides security requirements to the procurement official for inclusion into the contract, agreement, or MOU.

6.3.5. **Procurement Official**

6.3.5.1. Ensures that the ISO reviews any contracts, agreements, MOUs pertaining to IT System resources for adequate security specifications and requirements.

6.3.5.2. Ensures the inclusion of a separate section in the contract dealing with information security issues, where appropriate.

6.3.6. **Contractors**

6.3.6.1. Comply with all the Agency and Federal security requirements.

6.3.6.2. Protect access codes from improper disclosure.

6.3.6.3. Access only authorized IT System applications and data necessary to perform approved activities. Access capability does not equate to authority (e.g., casual browsing of data is not permitted).

6.3.6.4. Notify the Agency contact when access or authority is no longer required for approved tasks.

6.3.6.5. Attend IT System security training as required by the Agency policy, regulations, MOUs, or sharing agreements.

6.3.6.6. Fund and obtain background investigations as required.

7. APPENDIX A

7.1. ACRONYMS

AISO	Alternate Information Security Officer
CIO	Chief Information Officer
DISCO	Defense Industrial Security Clearance Organization
DSS	Defense Security Service
NHT	Information Technology Services Division
ISO	Information Security Officer
LAN	Local Area Network
MOU	Memorandum of Understanding
NIST	National Institute of Standards and Technology
OIG	Office of the Inspector General
	Office of Management and Budget
OPM	Office of Personnel Management
ISO	Information Security Officer
WAN	Wide Area Network

8. APPENDIX B

8.1. GLOSSARY

Access Control	Security control designed to permit authorized access to an IT system or application.
Accreditation	A formal declaration by the Office Head that the IT is approved to operate in a particular security mode using a prescribed set of safeguards. Accreditation is the official management authorization for operation of IT and is based on the certification process, as well as other management considerations. The accreditation statement affixes security responsibility with the Office Head and shows that due care has been taken for security.
Authentication	Verification of the identity of a user, user device, or other entity, or the integrity of data stored, transmitted, or otherwise exposed to unauthorized modification in an IT.
Audit Trail	A record showing who has accessed a computer system and what operations he or she has performed during a given period of time. Audit trails are useful both for maintaining security and for recovering lost transactions.
Automated Information System(s) (AIS)	An assembly of computer hardware, software and/or firmware configured to collect, create, communicate, compute, disseminate, process, store, and/or control data or information.
Availability of Data	The state when data are in the place needed by the user, at the time the user needs them, and in the form needed by the user.
Backup	A copy of data and/or applications contained in the IT stored on magnetic media outside of the IT to be used in the event IT data are lost.
Certification	The comprehensive evaluation of the technical and non-technical security features of an IT and other safeguards, made in support of the accreditation process, that establishes the extent to which a particular design and implementation meet a specified set of security requirements.

Ciphertext	Form of cryptography in which the *plaintext* is made unintelligible to anyone, who intercepts it by a transformation of the information itself, based on some key.
Confidentiality	The concept of holding sensitive data in confidence limited to an appropriate set of individuals or organizations.
Configuration Management	The process of keeping track of changes to the system, if needed, approving them.
Contingency Plan	A plan for emergency response, backup operations, and post-disaster recovery maintained by an activity as a part of its security program that will ensure the availability of critical resources and facilitate the continuity of operations in an emergency situation.
COTS Software	Commercial Off The Shelf Software – software acquired by government contract through a commercial vendor. This software is a standard product, not developed by a vendor for a particular government project.
Data Integrity	The state that exists when automated data is the same as that in source documents, or has been correctly computed from source data, and has not been exposed to alteration or destruction.
Degaussing Media	Method to magnetically erase data from magnetic tape.
Default	A value or setting that a device or program automatically selects if you do not specify a substitute.
Dial-up	The service whereby a computer terminal can use the telephone to initiate and effect communication with a computer.
Encryption	The process of making information indecipherable to protect it from unauthorized viewing or use, especially during transmission or storage. Encryption is based on an algorithm and at least one key. Even if the algorithm is known, the information cannot be decrypted without the key(s).
Facsimile	A document that has been sent, or is about to be sent, via a fax machine.
Firewall	A system or cination of systems that enforces a boundary between

two or more networks.

Friendly Termination — The removal of an employee from the organization when there is no reason to believe that the termination is other than mutually acceptable.

Gateway — A bridge between two networks.

Hardware — Refers to objects that you can actually touch, like disks, disk drives, display screens, keyboards, printers, boards, and chips.

Identification — The process that enables recognition of a user described to an IT.

Internet — A global network connecting millions of computers. As of 1999, the Internet has more than 200 million users worldwide, and that number is growing rapidly.

Intranet — A network based on TCP/IP protocols (an internet) belonging to an organization, usually a corporation, accessible only by the organization's members, employees, or others with authorization. An intranet's Web sites look and act just like any other Web sites, but the firewall surrounding an intranet fends off unauthorized access.

Intrusion Detection — Pertaining to techniques, which attempt to detect intrusion into a computer or network by observation of actions, security logs, or audit data. Detection of break-ins or attempts either manually or via software expert systems that operate on logs or other information available on the network.

ISO/AISO — The persons responsible to the Office Head or Agency Director for ensuring that security is provided for and implemented throughout the life cycle of an IT from the beginning of the concept development plan through its design, development, operation, maintenance, and secure disposal.

Issue-specific Policy — Policies developed to focus on areas of current relevance and concern to an office or agency. Both new technologies and the appearance of new threats often require the creation of issue-specific policies (e.g., e-mail, Internet usage).

IT Security — Measures and controls that protect an IT against denial of and unauthorized (accidental or intentional) disclosure, modification, or destruction of ITs and data. IT security includes consideration of all

hardware and/or software functions.

IT Security Policy — The set of laws, rules, and practices that regulate how an organization manages, protects, and distributes sensitive information.

IT Systems — An assembly of computer hardware, software and/or firmware configured to collect, create, communicate, compute, disseminate, process, store, and/or control data or information.

LDAP — Short for Lightweight Directory Access Protocol, a set of protocols for accessing information directories. LDAP is based on the standards contained within the X.500 standard, but is significantly simpler. And unlike X.500, LDAP supports TCP/IP, which is necessary for any type of Internet access.

Least Privilege — The process of granting users only those accesses they need to perform their official duties.

Local Area Network — A short-haul data communications systems that connects IT devices in a building or group of buildings within a few square miles, including (but not limited to) workstations, front end processors, controllers, switches, and gateways.

Management Controls — Security methods that focus on the management of the computer security system and the management of risk for a system.

Modem — An electronic device that allows a microcomputer or a computer terminal to be connected to another computer via a telephone line.

Network — Two or more systems connected by a communications medium; a network is composed of a communications medium and all components attached to that medium whose responsibility is the transference of information.

Operating System — The most important program that runs on a computer. Every general-purpose computer must have an operating system to run other programs. Operating systems perform basic tasks, such as recognizing input from the keyboard, sending output to the display screen, keeping track of files and directories on the disk, and controlling peripheral devices such as disk drives and printers.

Operation Controls	Security methods that focus on mechanisms that primarily are implemented and executed by people (as opposed to systems).
Overwriting media	Method for clearing data from magnetic media. Overwriting uses a program to write (1s, Os, or a cination) onto the media. Overwriting should not be confused with merely deleting the pointer to a file (which typically happens when a "delete" command is used).
Password	Protected/private character string used to authenticate an identity or to authorize access to data.
Parity	The quality of being either odd or even. The fact that all numbers have parity is commonly used in data communication to ensure the validity of data. This is called parity checking.
PBX	Short for private branch exchange, a private telephone network used within an enterprise. Users of the PBX share a certain number of outside lines for making telephone calls external to the PBX.
Peripheral Device	Any external device attached to a computer. Examples of peripherals include printers, disk drives, display monitors, keyboards, and mice.
Port	An interface on a computer to which you can connect a device.
Port Protection Device	A device that authorizes access to the port itself, often based on a separate authentication independent of the computer's own access control functions.
RADIUS	Short for Remote Authentication Dial-In User Service, an authentication and accounting system used by many Internet Service Providers (ISPs). When you dial in to the ISP you must enter your username and password. This information is passed to a RADIUS server, which checks that the information is correct, and then authorizes access to the ISP system.
Real Time	Occurring immediately. Real time can refer to events simulated by a computer at the same speed that they would occur in real life.
Remote Access	The hookup of a remote computing device via communication lines such as ordinary phone lines or wide area networks to access network applications and information

Risk	The probability that a particular threat will exploit a particular vulnerability of the system.
Risk Analysis	The process of identifying security risks, determining their magnitude, and identifying areas needing safeguards. Risk analysis is a part of risk management.
Risk Management	Process of identifying, controlling, and eliminating or reducing risks that may affect IT resources.
Router	An interconnection device that is similar to a bridge but serves packets or frames containing certain protocols. Routers link LANs at the network layer.
Rules of Behavior	Rules established and implemented concerning use of, security in, and acceptable level of risk for the system. Rules will clearly delineate responsibilities and expected behavior of all individuals with access to the system. Rules should cover such matters as work at home, dial-in access, connection to the Internet, use of copyrighted works, unofficial use of Federal Government equipment, the assignment and limitation of system privileges, and individual accountability.
Security Incident	An adverse event in a computer system or the threat of such an event occurring.
Security Plan	Document that details the security controls established and planned for a particular system.
Security Specifications	A detailed description of the safeguards required to protect a system.
Sensitive Data	Any information, the loss, misuse, modification of, or unauthorized access to, could affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under Section 552a of Title 5, U.S. Code, but has not been specifically authorized under criteria established by an Executive order or an act of Congress to be kept classified in the interest of national defense or foreign policy.
Separation of Duties	A process that divides roles and responsibilities so that a single individual cannot subvert a critical process.

Server	The control computer on a local area network that controls software access to workstations, printers, and other parts of the network.
Smart Card	A credit-card-sized device with embedded microelectronics circuitry for storing information about an individual. This is not a key or token, as used in the remote access authentication process.
Software	Computer instructions or data. Anything that can be stored electronically is software.
Software Copyright	The right of the copyright owner to prohibit copying and/or issue permission for a customer to employ a particular computer program.
SPAM	To crash a program by overrunning a fixed-site buffer with excessively large input data. Also, to cause a person or newsgroup to be flooded with irrelevant or inappropriate messages.
System	Set of processes, communications, storage, and related resources that are under the same direct management control, have the same function or Mission objective, have essentially the same operating characteristics and security needs, and reside in the same general operating environment.
System Availability	The state that exists when required automated information s can be performed within an acceptable time period even under adverse circumstances.
System Integrity	The quality that a system has when it performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system.
System Administrator	The individual responsible for defining the system's operating parameters, authorized functions, and security requirements. This individual is usually the person who maintains the system on a day-to-day basis.
System Owner	The individual who is ultimately responsible for the function and security of the system.
TCP/IP	Transmission Control Protocol/Internet Protocol. The Internet Protocol is based on this suite of protocols.

Technical Controls	Security methods consisting of hardware and software controls used to provide automated protection to the system or applications. Technical controls operate within the technical system and applications.
Technical Security Policy	Specific protection conditions and/or protection philosophy that express the boundaries and responsibilities of the IT product in supporting the information protection policy control objectives and countering expected threats.
Telecommunications	Any transmission, emission, or reception of signals, writing, images, sound or other data by cable, telephone lines, radio, visual or any electromagnetic system.
Threat	Any circumstance or event with the potential to cause harm to a system in the form of destruction, disclosure, modification of data, and/or denial thereof.
Trojan Horse	Any program designed to do things that the user of the program did not intend to do, or that disguise its harmful intent. A program that installs itself while the user is making an authorized entry; and, then is used to break-in and exploits the system.
Unfriendly Termination	The removal of an employee under involuntary or adverse conditions. This may include termination for cause, RIF, involuntary transfer, resignation for "personality conflicts," and situations with pending grievances.
User	Any person who is granted access privileges to a given IT.
User Interface	The part of an application that the user works with. User interfaces can be text-driven, such as DOS, or graphical, such as Windows.
Virus	A self-propagating Trojan horse (a program that surreptitiously exploits the security/integrity of a program), composed of a mission component, a trigger component, and a self-propagating component.
Vulnerability	A weakness in automated system security procedures, technical controls, environmental controls, administrative controls, internal controls, etc., that could be used as an entry point to gain unauthorized access to information or disrupt critical processing.

Wide Area Network A physical or logical network that provides capabilities for a number of independent devices to communicate with each other over a common transmission-interconnected topology in geographic areas larger than those served by local area networks.

9. APPENDIX C

9.1. REFERENCES

Computer Security Act of 1987 (PL 100-235)

Circular A-123, Internal Control Systems

Circular A-130, Management of Federal Information Resources, Appendix III, "Security of Federal IT Systems".

Privacy Act of 1974 (PL-93-579) and Amendments

NIST SP 800-12, An Introduction to Computer Security; The NIST Handbook

NIST SP 800-14, Generally Accepted Principals and Practices for Securing IT Systems.

NIST SP 500-172, Computer Security Training Guidelines. This was replaced by 800-16. Should it be here instead?

the Agency IT Systems Security Handbook

the Agency Directive XXX, IT Systems Security Policy