Department of Veterans Affairs
Washington, DC 20420

VA Handbook 6500
Transmittal Sheet
September 18, 2007

Information Security Program

1. REASON FOR ISSUE: To provide specific procedures and establish operational requirements to implement the Department of Veterans Affairs (VA) Directive 6500, Information Security Program dated August 4, 2006.

2. SUMMARY OF CONTENTS/MAJOR CHANGES: This handbook provides the specific procedures and operational requirements to implement *VA Directive 6500, Information Security Program*, to ensure Department-wide compliance with the Federal Information Security Management Act of 2002 (FISMA), 44 U.S.C. §§ 3541-3549, and the security of VA information and information systems administered by VA, or on behalf of VA. This handbook applies to all VA organizations, Administrations, their employees and contractors working for, or on behalf of the VA.

3. RESPONSIBLE OFFICE: The Office of the Assistant Secretary for Information and Technology (OI&T) (005).

4. RELATED DIRECTIVE: VA Directive 6500, Information Security Program.

5. RESCISSIONS: VA Directive 6504, Restriction on Transmission, Transportation and Use Of, and Access To, VA Data Outside VA Facilities, dated June 7, 2006, and VA Directive 6601, Removable Storage Media dated February 27, 2007.

CERTIFIED BY:

/s/

Robert T. Howard
Assistant Secretary for Information and Technology

BY DIRECTION OF THE SECRETARY OF VETERANS AFFAIRS

/s/

Robert T. Howard
Assistant Secretary for Information and Technology

Distribution: Electronic Only

TABLE OF CONTENTS

PARAGRAPH **PAGE**

Information Security Program Handbook

1. PURPOSE.

a. This handbook establishes the foundation for VA's comprehensive information security program and its practices that will protect the confidentiality, integrity, and availability of information created, processed, stored, aggregated, and transmitted by VA's information systems and business process.

b. This handbook provides the minimum mandatory security control standards for implementation of VA Directive 6500, Information Security Program.

c. This handbook also provides the criteria to assist management in making governance and integration decisions for VA's various security programs.

2. SCOPE.

a. The security policies, procedures, and controls in this handbook apply to all VA employees, contractors, researchers, students, volunteers, representatives of Federal, State, local, or Tribal agencies, and all others authorized access to VA facilities, information systems or information in order to perform a VA authorized activity.

b. The requirements in this handbook and appendices apply to all VA or contractor-operated services and information resources located and operated at contract facilities, at other government agencies that support VA mission requirements, or any other third party utilizing VA information in order to perform a VA authorized activity.

c. The VA National Rules of Behavior provide the responsibilities and expected behavior of all individuals (end users) with authorized access to VA's information and information systems.

d. The security controls apply to all information resources used to carry out the VA mission. For example, the controls apply to desktop PC workstations, laptop computers, other portable devices, servers, network devices, office automation equipment (such as copiers and fax machines with communication capabilities), and operated by or on behalf of VA.

e. This handbook applies to the security of all information collected, transmitted, used, stored, or disposed of, by or on behalf of VA.

f. The Office of Information and Technology (OI&T) will develop and disseminate additional directives, handbooks, memoranda, notices and best practices to implement these procedures, or institute additional requirements to maintain the information assurance program.

3. UTILIZATION OF THIS HANDBOOK AND APPENDICES.

a. This handbook establishes specific minimum security procedures, processes and responsibilities for the implementation and operation of VA's information security program. The information security program is designed to protect VA's information systems, all VA information and telecommunications resources from unauthorized access, use, disclosure, modification, or destruction. These requirements comply with established Federal information

security laws and regulations, including the Information Security Subchapter III of Chapter 57 of Title 38, U.S.C., Federal Information Security Management Act of 2002 (FISMA) (44 U.S.C. §§ 3541-3549), Office of Management and Budget (OMB) Circular A-130 and its appendices, the Administrative Simplification provisions of the Health Insurance Portability and Accountability Act (HIPAA), The Privacy Act of 1974 (as amended) and the National Institute of Standards and Technology (NIST) Federal Information Processing Standards (FIPS) and Special Publication (SP) guidance.

b. This handbook provides Operating Units (see definition in Appendix A) with a security policy foundation from which to operate and maintain their overall facility or program offices' information security programs. This handbook provides the information security responsibilities for individuals with authorized access to VA information and information systems.

c. *Appendix A* contains terms and definitions used throughout this handbook.

d. *Appendix B* contains a list of abbreviations/acronyms used throughout this handbook.

e. *Appendix C* contains the legal authorities upon which this handbook is based.

f. *Appendix D* contains the current minimum applicable security control requirements for VA information and information systems promulgated by NIST under FISMA including *FIPS 200, Minimum Security Requirements for Federal Information and Information Systems*, and NIST SP *800-53, Recommended Security Controls for Federal Information Systems*. This appendix provides specific procedures for the individuals [Information Security Officers (ISOs), Chief Information Officers (CIOs), system administrators, system developers, contractors, etc.] who must comply with VA information security policy based upon FISMA and the corresponding security controls for the specific information systems under their control. The controls in this appendix are broken down based on the impact level of the system. This document and its appendices will be updated when required.

g. *Appendix E* is a chart that provides the *VA Control Parameter Definitions: Configuration Standards* for the information system security controls provided in *Appendix D*. This chart details the various VA defined security controls by user level and security categorization (impact level) of systems.

h. *Appendix F* provides the password management policy for information systems operated by or on behalf of VA.

i. *Appendix G* is the VA approved National Rules of Behavior that will be utilized throughout VA. The National Rules of Behavior contains responsibilities and expected behavior of all individuals (end users) with access to VA's information and information systems.

4. BACKGROUND/OVERVIEW

a. The E-Government Act (PL 107-347), passed by Congress and signed into law by the President in December 2002, recognized the importance of information security to the economic and national security interests of the United States. Title III of the E-Government Act, FISMA, emphasized the need for all Federal agencies to develop, document, implement, and maintain an enterprise-wide program to provide an integrated security program to protect

Federal information and information systems that support the Federal Government's mission. Specifically, FISMA directed all federal agencies to follow specific security guidance and implement specific requirements issued by NIST in its FIPS and SP documents. Specifically, VA is required within its FISMA security program to implement NIST FIPS 199 and 200 to:

(1) Categorize VA information systems based on the sensitivity of the information, the mission criticality of the business process for which information systems provide support and the levels of risks faced; and

(2) Use security requirements in FIPS 200, and NIST SP 800-53.

b. With the diverse nature of VA's information systems, Operating Units may find it necessary, on occasion, to specify and employ compensating security controls. A compensating control for an information system may be employed by an Operating Unit only under the following conditions:

(1) The Operating Unit selects the intended compensating control(s) and determines if they are equivalent to the security control requirements in Appendix D;

(2) The Operating Unit provides a justification in the system security plan for how the compensating control provides an equivalent or greater security capability or level of protection for the information system; and

(3) The Operating Unit assesses, tests, and formally accepts the risk associated with employing the compensating control in the information system. Compensating controls should provide equivalent protection and when they do not, they should only be used temporarily until the requirements in Appendix D and the NIST specified control can be procured and implemented. If the compensating control provides greater security capability than required by Appendix D, the compensating control must be compatible with, and not adversely affect the operation of other information systems within VA. The use of compensating security controls should be reviewed, documented in the system security plan and must be approved by the authorizing official for the information system prior to implementation. The authorizing official's designated representative may examine compensating controls when provided for review and approval as part of the security control assessment plan for new systems prior to operation and also in the final certification and accreditation package reviewed to support an Authority to Operate (ATO) for both new and currently operating systems.

c. System Owners/Information Owners/Program Managers must identify any proposed deviations from the mandatory practices of this handbook and request a waiver (including compensating controls) in writing to the ADAS for OCS. Approved waivers must be documented as part of the appropriate system security plan(s) that cover the system(s) operating under the waiver. Identical systems under the same management authority and covered by one system security plan require only one waiver request. Requests for an Information Security Program Policy Waiver must:

(1) Cite the specific mandatory practice(s) for which the waiver is requested;

(2) Explain the rationale for the requested waiver;

(3) Describe compensating controls to be in place during the period of the requested waiver until systems are compliant with this policy; and

(4) Provide an action plan, with target dates, for compliance.

d. The transmission of requests must be secured in a manner commensurate with the risk of harm of disclosure of the content (e.g. control vulnerabilities). OCS will decide whether to approve or deny a waiver request or request additional information in support of the waiver request within 30 calendar days of receipt. If OCS takes longer to make the decision on a requested waiver, OCS will notify the originating office and provide an estimated date for decision. The lack of response within 30 calendar days is not an approval of the waiver request. The decision letter must either:

(1) Approve the waiver and state all of the conditions, if any, for operating the information system under the waiver, including any waiver expiration date;

(2) Deny the waiver and state the bases for the denial; or

(3) Request any additional information needed to make the decision on the waiver request.

e. Operating Unit Chief Information Officers may appeal the OCS waiver decision in writing to the VA CIO.

f. If a compensating control waiver is denied by the VA CIO, the VA CIO will determine, using a risk based decision, the actions required of the System Owner. Based on the risk, the CIO may require the System Owner to take actions such as shutting down the system, using another compensating control, or providing a mandatory date for compliance.

g. Violations of *VA Directive 6500*, *Information Security Program* and this handbook may result in disciplinary action, up to and including dismissal and legal action against the offending employee(s) or researchers, consistent with law. A violation of this handbook may result in denial or termination of access to VA information and VA systems. Additionally, violations of this handbook may also result in a denial of an ATO, suspension of funding, and/or information system shut down.

5. INFORMATION SECURITY RESPONSIBILITIES

a. *VA Directive 6500, Information Security Program* describes the responsibilities for VA Senior Officials, Information Owners, Information system users, and the Office of the Inspector General (OIG). Each subordinate directive and/or handbook issued by OCS in support of the VA Information Security program will include definitive roles and responsibilities related to the security control family addressed and may delineate additional responsibilities as necessary to protect VA information and information systems.

b. Additional roles and responsibilities with significant information and information security responsibilities necessary for implementing the VA Information Security Program include the following:

(1) Deputy Assistant Secretary for Information Protection Risk Management Under the IT Single Authority the VA CIO has created the DAS IPRM which has authority over:

(a) VA enterprise cyber security budget

(b) Associate Deputy Assistant Secretary for Cyber Security

(c) Associate Deputy Assistant Secretary of Privacy and Records Management

(d) Associate Deputy Assistant Secretary for Risk Management and Incident Response;

(e) Director, Business Continuity

(2) Associate Deputy Assistant Secretary for Cyber Security carries out the responsibilities of the Associate Deputy Assistant Secretary for Cyber and Information Security under 38 U.S.C. § 5723(c) and the Senior Information Security Officer of the Department. This position is responsible for carrying out the responsibilities of the Assistant Secretary for Information and Technology under 44 U.S.C. 3544. These responsibilities include:

(a) Establishing, maintaining, and monitoring Department-wide information security policies, procedures, control techniques, training, and inspection requirements as elements of the Department information security program;

(b) Issuing policies and handbooks to provide direction for implementing the elements of the information security program to all Department organizations;

(c) Approving all policies and procedures that are related to information security for those areas of responsibility that are currently under the management and the oversight of other Department organizations;

(d) Ordering and enforcing Department-wide compliance with and execution of any information security policy;

(e) Establishing minimum mandatory technical, operational, and management information security control requirements for each Department system, consistent with risk, the processes identified in standards of the National Institute of Standards and Technology, and the responsibilities of the Assistant Secretary to operate and maintain all Department systems currently creating, processing, collecting, or disseminating data on behalf of Department information owners;

(f) Establishing standards for access to Department information systems by organizations and individual employees and to deny access as appropriate;

(g) Directing that any incidents of failure to comply with established information security policies be immediately reported to the Assistant Secretary;

(h) Reporting any compliance failure or policy violation directly to the appropriate Under Secretary, Assistant Secretary, or other key official of the Department for appropriate administrative or disciplinary action;

(i) Reporting any compliance failure or policy violation directly to the appropriate Under Secretary, Assistant Secretary, or other key official of the Department along with taking action to correct the failure or violation;

(j) Requiring any key official of the Department who is so notified to report to the Assistant Secretary with respect to an action to be taken in response to any compliance failure or policy violation reported by the Assistant Secretary;

(k) Ensuring that the CIOs and ISOs of the Department comply with all cyber security directives and mandates, and ensuring that these staff members have all necessary authority and means to direct full compliance with such directives and mandates relating to the acquisition, operation, maintenance, or use of information technology resources from all facility staff;

(l) Establishing the VA National Rules of Behavior for appropriate use and protection of the information which is used to support Department missions and functions;

(m) Establishing and providing supervision over an effective incident reporting system;

(n) Submitting to the Secretary, at least once every quarter, a report on a deficiency in the compliance with subchapter III of chapter 35 of title 44 of the Department or any Administration, office, or facility of the Department;

(o) Reporting immediately to the Secretary on any significant deficiency in the compliance described by paragraph (n); and

(p) Providing immediate notice to the Secretary of any presumptive data breach.

(3) Associate Deputy Assistant Secretary of Privacy and Records Management is responsible for:

(a) Providing guidance and procedures for protecting personally identifiable information (PII) as required by the Privacy Act of 1974;

(b) Tracking and auditing of VA privacy complaints;

(c) Providing oversight and guidance for VA compliance with applicable privacy laws, regulations and policies;

(d) Advising the ADAS for Cyber Security and the CIO in privacy-related matters;

(e) Coordinating with Federal oversight agencies and VA management regarding privacy violations and their resolution, as required;

(f) Establishing VA requirements and providing guidance regarding the development, completion, and updating of Privacy Impact Assessments (PIA);

(g) Ensuring that Privacy Awareness Training is provided and available for VA employees, contractors, volunteers, and interns;

(h) Assisting system owners in conducting PIAs as required;

(i) Coordinating with OCS and the ISO community to ensure reasonable privacy safeguards are in place as required by Health Insurance Portability and Accountability Act (HIPAA), or other Federal privacy statutes;

(j) Coordinating and assisting ISOs with privacy related issues; and

(k) Coordinating with facility ISOs and/or Network ISOs to ensure that privacy and information system security policies complement and support each other.

(4) Associate Deputy Assistant Secretary for Risk Management and Incident Response is responsible for:

(a) Evaluating, monitoring, and assigning risk values, and builds impact assessments of the internal risk environment from an employee, information systems, internal control, and research and development perspectives;

(b) Working with other IT organizations to establish risk action plans and works with stakeholders to implement;

(c) Working with IT governance structure to incorporate management approval of risk acceptance;

(d) Facilitating the Information Resolution Core Team (IRCT), which is made up of all security entities in VA, to review, discuss and provide resolution in nationwide VA incidents;

(e) Facilitating building into the organization risk tolerance and evaluates the information sources, risk management system, and mitigation techniques for efficiency, effectiveness, and opportunities for improvement;

(f) Responding to incidents and events, which could cause an interruption to or reduction in the quality of that service, and identifies the root cause(s) of the incidents/events in order to mitigate the same or similar events from impacting service in the future;

(g) Establishing and maintaining a formal incident response capability. Provides pertinent information on incidents to the appropriate organizations;

(h) Providing pertinent information on incidents to the appropriate organizations;

(i) Evaluating, monitoring and coordinating data breach quarterly reports. These data breach reports are provided to Congress by the Secretary of Veterans Affairs;

(j) Developing guidance and assisting in the identification, implementation, and maintenance of enterprise-wide information identity protection and risk assessment policies and procedures in coordination with stakeholders;

(k) Executing initial and periodic information identity risk assessments and conducts related on-going compliance monitoring activities in coordination with other compliance and operational assessment functions.

(5) Director, Business Continuity is responsible for:

(a) Working closely with IT and other business units to develop program initiatives to meet the requirement to develop and maintain an enterprise business continuity program to ensure a state of readiness in the event of a disaster or business disruption;

(b) Managing the planning, design, and maintenance of business continuity program projects and ensuring compliance with industry standards and regulatory requirements;

(c) Managing, guiding, and directing business continuity preparedness through business centered teams; reviews team plans to ensure compliance; monitors plan development; evaluates plan changes and updates;

(d) Providing business and technical guidance to senior and executive staff, subcontractors, business continuity team members and enterprise staff relative to business continuity;

(e) Managing, and resolving all business continuity problems involving one or more IT or business units, systems or functions;
(f) Overseeing the process of defining business continuity problems and implementing solutions

(6) Deputy Assistant Secretary for Security and Law Enforcement is responsible for:

(a) Processing background investigations as required;

(b) Developing and implementing *VA Directive and Handbook 0710, Personnel Suitability and Security Program*;

(c) Conducting an annual physical security survey in accordance with *VA Directive and Handbook 0730, Security and Law Enforcement;*

(d) Establishing physical security standards and practices (VA Directive and Handbook 0730, Security and Law Enforcement); and

(e) Disseminating guidance and direction to the field security and law enforcement staff, as required, to assist implementation of these security policies and procedures.

(7) Deputy Assistant Secretary for Human Resources Management is responsible for:

(a) Providing guidance based on VA's HR policy to field supervisors and managers regarding personnel actions or other actions to be taken when employees have violated information security practices, laws, regulations, policies, and rules of behavior; and

(b) Providing advice to field supervisors and managers regarding appropriate information security-related performance standards and position descriptions for employees who are authorized to access any information system(s).

(8) Deputy Assistant Secretary of Acquisition and Logistics is responsible for:

(a) Providing acquisition guidance and procedures to VA contracting officers (COs) and contracting officer technical representatives (COTRs) to facilitate implementation of VA's information security program for information systems implemented within the Department;

(b) Providing VA guidance to ensure that security requirements and security specifications are explicitly included in information systems and information system support service acquisition contracts;

(c) Providing VA guidance to ensure that contracts contain the language necessary for compliance with FISMA and 38 U.S.C. 5721-28 and provide adequate security for information and information systems used by the contractor;

(d) Providing VA guidance to ensure that contracts for services include appropriate background investigation requirements; and

(e) Providing VA guidance to ensuring that contractors have the appropriate background investigation on record in accordance with VA Directive and Handbook 0710.

(f) Ensuring that Contracting Officers (COs) consult with appropriate ISOs.

(9) Director, Oversight and Compliance Management Division in OI&T is responsible for:

(a) Ensuring VA compliance with FISMA and 38 U.S.C. 5721-28 and other related security, privacy, and record management requirements promulgated by NIST, OMB, and VA information and information security policies;

(b) Validating the remediation of Plans of Action and Milestones (POA&M) identified in the Security Management and Reporting Tool (SMART) database; and

(c) Ensuring VA systems that have undergone a security certification and accreditation are continuing to operate at their accredited level of risk by repeating a selection of security control assessment tests.

(10) VA Network Security Operations Center (VA NSOC) is responsible for:

(a) Identifying, validating and managing all information and information system incidents (security and privacy) reporting and response efforts;

(b) Ensuring information security incidents are assigned a risk severity level rating;

(c) Approving and managing all VA information and information systems incident response efforts based on VA NSOC standard operating procedures or as directed by the guidance of the VA OI&T or the United States Computer Emergency Readiness Team (US-CERT);

(d) Providing central coordination and incident response functions for all security and privacy events impacting and affecting the Department of Veterans Affairs;

(e) Coordinating with outside agencies such as the US-CERT;

(f) Working directly with the OIG to support any activity necessary;

(g) Tracking the progress of event activity and performing all necessary documentation of incident progress;

(h) Reporting all privacy related incidents to the US-CERT within one hour of discovery of event;

(i) Generating Situation Reports, trending reports suitable for upper management review, final Incident Reports and Lessons Learned briefings for major incidents; and

(j) Actively monitoring all VA network intrusion detection sensors, firewall alerts, network operations and security logs for abnormal activity, attempted intrusions or compromises and other manners of security alerts that may be generated, and follow up as appropriate to prevent security incidents from occurring or developing into major security events.

(11) Authorizing Official (AO) is the VA CIO and senior management official authorized to assume the responsibility and accountability for operating an information system at an acceptable level of risk. The AO is involved with Certification & Accreditation (C&A) of VA systems and is responsible for:

(a) Authorizing operation of an information system;

(b) Issuing an interim authorization to operate (IATO) for an information system under certain terms and conditions; and

(c) Denying authorization to operate the information system, or if the system is already operational, halt operations after consulting with the system owner if unacceptable security risks exist.

(12) Authorizing Official Designated Representative (AODR) is the AO's designated representative, to act on his/her behalf in coordinating and carrying out the necessary activities required during the security accreditation of an information system. The AODR responsibility has been assigned to the Deputy Assistant Secretary for Information Protection and Risk Management. In addition, the AODR can be empowered by the AO to perform the following:

(a) Making decisions with regard to the planning of the security certification and accreditation activities;

(b) Providing an IATO extension in the event local system management can show they are providing continuous monitoring and show security due diligence but need up to an additional six months to accommodate corrective actions due to contracting needs or other reasonable accommodations. Any needs over six months or for second requests must be in the form of a recommendation to the AO;

(c) Accepting and approving system security plans; security control assessment plans, and assists the AO by recommending a system operations risk determination;

(d) Reviewing all final security certification and accreditation packages and making decision recommendations to the AO on issuance of an IATO, Authority to Operate (ATO), or Denial of Authority to operate.

(13) Certification Agents (CA) are appointed by OCS, part of the Certification and Accreditation (C&A) process and responsible for:

(a) Conducting or overseeing security certification testing;

(b) Ensuring security control assessment testing meets minimum levels of assurance;

(c) Recommending corrective actions to the AO to reduce or eliminate vulnerabilities identified as a result of the controls testing for the information system; and

(d) Providing an independent security controls assessment based on testing results and providing an honest opinion of whether the system is operating at an acceptable level of risk, taking into consideration system and information sensitivity and the timely completion of control deficiency remediation plans as outlined in the POA&M.

(14) Information Systems Owners (Regional Directors) are responsible for the overall procurement, development, integration, modification, daily operations and maintenance of VA information and information systems, including:

(a) Ensuring that each system is assigned a system owner, that the system owner is responsible for the security of the system, and that the system owner meets the following qualifications:

(1.) General support systems: An individual knowledgeable in the information technology used in the system and in providing security for such technology.

(2.) Major Applications: A management official knowledgeable in the nature of the information and process supported by the application and in the management, personnel, operational, and technical controls used to protect it. This official shall assure that effective security products and techniques are appropriately used in the application and shall be contacted when a security incident occurs concerning the application.

(b) Ensuring compliance with Federal security regulations and VA security policies;

(c) Ensuring the development and maintenance of system security plans and contingency plans in coordination with local information owners, the local system administrators, the information system security officers, and functional “end user” for nationally deployed systems;

(d) Reviewing and updating the system security plan on an annual basis and when a significant change to the system occurs;

(e) Reviewing, updating and testing the system contingency plan on an annual basis and when a significant change to the system occurs;

(f) Developing and maintaining an “ IT system Configuration/Change Management Plan”;

(g) Ensuring that system users and support personnel receive required security training;

(h) Assisting the local system administrators in the identification, implementation, and assessment of common security controls;

(i) Ensuring risk assessments are accomplished every three years, reviewed/updated annually, and when there is a major change to the system, re-evaluating sensitivity of the system, risks, and mitigation strategies with the assistance of other VA officials with significant information and information system responsibilities;

(j) Ensuring a security certification and accreditation of the information system is completed prior to operational deployment and re-certified/accredited at a minimum every three years, or whenever a major change occurs;

(k) Ensuring each decision to utilize compensating controls, waive security controls, or enhance the recommended security controls of the information system are fully documented and approved as a risk-based decision and included in the "Approval to Operate" package forwarded to the Certifying Official;

(l) Assisting other VA officials with significant IT responsibilities in remediating and updating the POA&M identified during the certification and accreditation process, periodic compliance validation reviews, and the FISMA annual assessment to reduce or eliminate system vulnerabilities;

(m) Ensuring continuous monitoring activities are being performed that re-tests a subset of controls from each system's security certification and accreditation security control assessment test procedures;

(n) Notifying the responsible VA ISO, VA NSOC and/or the OIG of any suspected incidents immediately upon identifying that an incident has occurred and assisting in the investigation of incidents, as necessary.

(o) Ensuring compliance with the Enterprise and Security Architecture throughout the system life cycle.

(p) Conducting PIAs as required.

(15) Department Information Owners in accordance with the criteria of the Centralized IT Management System are responsible for the following:

(a) Providing assistance to the Assistant Secretary for Information and Technology regarding the security requirements and appropriate level of security controls for the information system or systems where sensitive personal information is currently created, collected, processed, disseminated, or subject to disposal;

(b) Determining who has access to the system or systems containing sensitive personal information, including types of privileges and access rights;

(c) Ensuring the VA National Rules of Behavior is signed on an annual basis and enforced by all system users to ensure appropriate use and protection of the information which is used to support Department missions and functions;

(d) Assisting the Assistant Secretary for Information and Technology in the identification and assessment of the common security controls for systems where their information resides; and

(e) Providing assistance to Administration and staff office personnel involved in the development of new systems regarding the appropriate level of security controls for their information.

(16) Under Secretaries, Assistant Secretaries, and Other Key Officials in accordance with 44 U.S.C. 3544 and 38 U.S.C. § 5723(e), are responsible for the following:

(a) Implementing the policies, procedures, practices, and other countermeasures identified in the Department information security program that comprise activities that are under their day-to-day operational control or supervision;

(b) Periodically testing and evaluating information security controls that comprise activities that are under their day-to-day operational control or supervision to ensure effective implementation;

(c) Providing a plan of action and milestones to the Assistant Secretary for Information and Technology on at least a quarterly basis detailing the status of actions being taken to correct any security compliance failure or policy violation;

(d) Complying with the provisions of subchapter III of chapter 35 of title 44 and other related information security laws and requirements in accordance with orders of the Assistant Secretary for Information and Technology to execute the appropriate security controls commensurate to responding to a security bulletin of the VA-NSOC, with such orders to supersede and take priority over all operational tasks and assignments and be complied with immediately;

(e) Ensuring that all employees within their organizations take immediate action to comply with orders from the Assistant Secretary for Information and Technology to mitigate the impact of any potential security vulnerability, respond to a security incident, or implement the provisions of a bulletin or alert of the VA-NSOC and ensuring that organizational managers have all necessary authority and means to direct full compliance with such orders from the Assistant Secretary;

(f) Ensuring the VA National Rules of Behavior is signed and enforced by all system users to ensure appropriate use and protection of the information which is used to support Department missions and functions on an annual basis.

(g) Communicating this policy to all employees in their organizations and evaluating the security and privacy awareness activities of each organization in order to set clear expectations for compliance with security and privacy requirements and to ensure adequate resources to accomplish such compliance;

(h) Developing mechanisms for communicating, on an ongoing basis, each workforce member's role and responsibilities specific to information security and privacy policies and practices that will enhance our security and privacy culture; and

(i) Ensuring that all employees in their respective organizations receive required security and privacy training.

(17) Program Directors/Facility Directors, through the ISO, are responsible for:

(a) Providing the necessary support to the Information Security Program in their organizations and ensuring that the facility meets all the information security requirements mandated by Executive and VA policy and other federal legislation (e.g., FISMA, HIPAA);

(b) Ensuring ISOs are fully involved in all new projects concerning the development or acquisition of systems, equipment, or services including risk analysis, security plans, request for proposals (RFPs), and other procurement documents that require the ISO's participation.

(c) Ensuring that respective staff, with defined FISMA security roles, provide the ISO (in a timely manner) the information required to complete the quarterly FISMA reporting to OI&T and OMB.

(d) Ensuring all POA&M corrective actions are taken by their respective staff.

(18) Information Security Officers (ISOs) are the agency officials' assigned responsibility by OI&T Field Operations and Security to ensure that the appropriate operational security posture is maintained for an information system or program. The VA ISOs are responsible for:

(a) Ensuring compliance with Federal security regulations and VA security policies;

(b) Managing their local information security programs and serving as the principal security advisor to system owners regarding security considerations in applications, systems, procurement or development, implementation, operation and maintenance, disposal activities (i.e., life cycle management);

(c) Assisting in the determination of an appropriate level of security commensurate with the impact level;

(d) Coordinating, advising, and participating in the development and maintenance of information system security plans and contingency plans for all systems under their responsibility;

(e) Ensuring risk assessments are accomplished every three years, reviewed/updated annually, and when there is a major change to the system, re-evaluating sensitivity of the system, risks, and mitigation strategies with the assistance of other VA officials with significant information and information system responsibilities;

(f) Verifying and validating, in conjunction with the system owners and managers, that appropriate security measures are implemented and functioning as intended;

(g) Working with the system owner and manager, repeating a selected sub-set of security control certification and accreditation security control assessment test procedures, as it pertains to the information systems at the site, to ensure that controls remain in place, operating correctly and producing the desired results. Controls most apt to change over time must be included and these tests and results must be documented to support the continuous monitoring program;

(h) Participating in security self-assessments, external and internal audits of system safeguards and program elements, and in certification and accreditation of the systems supporting the offices and facility under their area of responsibility;

(i) Assisting other VA officials with significant IT responsibilities (i.e., system managers, contracting staff, human resources staff, police) in remediating and updating the POA&M identified during the certification and accreditation process, periodic compliance validation reviews and the FISMA annual assessment reporting;

(j) Notifying the VA NSOC and/or the OIG of any suspected incidents within one hour of identifying that an incident has occurred and assisting in the investigation of incidents, if necessary;

(k) Maintaining cooperative relationships with business partners or other interconnected systems;

(l) Monitoring compliance with the security awareness and training requirements for each employee/contractor;

(m) Coordinating, monitoring and conducting periodic reviews to ensure compliance with the National Rules of Behavior requirement for each system information user;

(n) Serving as the primary point of contact for security awareness and training within their area of responsibility;

(o) Coordinating with the facility Privacy Officer for the assurance of reasonable safeguards as required by the HIPAA Privacy Rule, HIPAA Security Rule, or other federal privacy statutes;

(p) Working with the facility Privacy Officer to assure information security and privacy policies complement and support each other; and

(q) Notifying OI&T staff to add, change, suspend, or revoke access privileges in a timely manner when a user under his/her supervision or oversight no longer requires access privileges or he/she fails to comply with this policy.

(19) Local Program Management: Must determine whether Federal employees and contractors require information system access in the accomplishment of the VA mission. Specifically, the managers and/or supervisors are responsible for:

(a) Ensuring that all users are adequately instructed, trained, and supervised on IT security and information protection issues.

(b) Ensuring their offices and staff are in compliance with Federal security regulations and VA security policies;

(c) Determining the Federal employee's or contractor's "need to know" before access is granted. Access to any VA information or information system must not be authorized for a person who does not have a need for access to the system in the normal performance of his/her official duties;

(d) Ensuring users under his/her supervision or oversight comply with this policy and pursue appropriate disciplinary action for noncompliance;

(e) Ensuring users under his/her supervision or oversight complete all security and privacy training requirements;

(f) Ensuring users under his/her supervision or oversight review and sign the VA National Rules of Behavior on an annual basis;

(g) Notifying system administrators and ISO of new users per locally approved procedures;

(h) Notifying system managers and ISO to revoke access privileges in a timely manner when a user under his/her supervision or oversight no longer requires access privileges or he/she fails to comply with this policy;

(i) Authorizing remote access privileges for personnel and reviewing remote access user security agreements on an annual basis, determined by the date of authorized agreement for remote access, at a minimum to verify the continuing need for access, and the appropriate level of privileges;

(j) Ensuring appropriate background investigations (BIs) are initiated and verified on all Federal employees and contractors under their supervision through the VA Security and Investigations Center;

(k) Notifying responsible ISOs if BIs are unfavorable until further determination of fact;

(l) Ensuring employees report any suspected incidents immediately upon discovery to management officials and ISOs;

(m) Assisting other VA officials with significant information system responsibilities in the remediation and updating of the POA&M identified during the certification and accreditation process, periodic compliance validation reviews and the FISMA annual assessment reporting to reduce or eliminate system vulnerabilities;

(n) Notifying the responsible ISO of any suspected incidents immediately upon discovery and assisting in the investigation of incidents if necessary.

(20) Local CIOs/System Administrators/Network Administrators are responsible for day to day operations of the systems. The role of a system administrator must include security of Local Area Network (LAN) or application administration and account administration. The system/network administrator is responsible for:

(a) Ensuring compliance with Federal security regulations and VA security policies;

(b) Assisting in the development and maintenance of information system security plans and contingency plans for all systems under their responsibility;

(c) Participating in risk assessments every three years, review/update annually, or when there is a major change to the system to re-evaluate sensitivity of the system, risks, and mitigation strategies;

(d) Participating in self-assessments, external and internal audits of system safeguards and program elements, and in certification and accreditation of the system;

(e) Evaluating proposed technical security controls to assure proper integration with other system operations;

(f) Identifying requirements for resources needed to effectively implement technical security controls;

(g) Ensuring the integrity in implementation and operational effectiveness of technical security controls by conducting technical control testing and security control assessments (SCA);

(h) Developing system administration and operational procedures and manuals as directed by the system owner;

(i) Evaluating and developing procedures that assure proper integration of service continuity with other system operations;

(j) Notifying the responsible ISO of any suspected incidents within one hour upon discovery and assisting in the investigation of incidents if necessary;

(k) Reading and understanding all applicable training and awareness materials;

(l) Providing information on users and/or the system in support of any reports or documents necessary for oversight and C&A;

(m) Reading and understanding all applicable use policies or other rules of behavior regarding use or abuse of the Operating Unit's information system resources; and

(n) Understanding which systems, or parts of systems, for which they are directly responsible (e.g., network equipment, servers, LAN, etc.), the sensitivity of the information contained in these systems, and the appropriate measures to take to protect the information;

(o) Periodically repeating selected security control assessment test procedures from the systems security certification and accreditation to ensure the systems controls continue to operate effectively at the proper levels of assurance per NIST guidance and over the life cycle of the system; and

(p) Assisting other VA officials with significant IT responsibilities in the remediation and updating the POA&M identified during the certification and accreditation process, periodic compliance validation reviews and the FISMA annual assessment reporting to reduce or eliminate system vulnerabilities.

(21) Contracting Officers (COs)/ Contracting Officer's Technical Representatives (COTRs) are responsible for:

(a) Ensuring that security requirements and security specifications are explicitly included in information systems and information system support service acquisition contracts;

(b) Ensuring that contracts contain the security language necessary for compliance with FISMA and 38 U.S.C. 5721-28 and provide adequate security for information and information systems used by the contractor, including the requirement for signing the National Rules of Behavior, when applicable;

(c) Ensuring contracts for services include appropriate background investigation requirements; and

(d) Ensuring that contractors have the appropriate background investigation on record in accordance with VA Directive and Handbook 0710.

(e) Assisting other VA officials with significant IT responsibilities in the remediation and updating the POA&M identified during the certification and accreditation process, periodic compliance validation reviews and the FISMA annual assessment reporting to reduce or eliminate system vulnerabilities.

(22) Local HR Staff/Security and Law Enforcement Staff are responsible for implementing specific security role based functions and are responsible for the following:

(a) Complying with all Department information security program policies, procedures, and practices that pertain to their specific positions;

(b) Assisting other VA officials with significant IT responsibilities in the remediation and updating the POA&M identified during the certification and accreditation process, periodic compliance validation reviews and the FISMA annual assessment reporting to reduce or eliminate system vulnerabilities; and

(23) Users of VA Information and Information Systems are responsible for complying with the VA National Rules of Behavior (Appendix G).

6. POLICY AND PROCEDURES

a. Management Controls

(1) Risk Management

(a) **Policy**: VA will implement security control measures to sufficiently manage, reduce and/or eliminate risks and vulnerabilities to a reasonable and appropriate level of compliance with all federal security statutes.

(b) **Procedure**:

1. Risk Assessments: The Operating Unit is responsible for conducting accurate and thorough risk assessments to identify potential risks, vulnerabilities and threats to the confidentiality, integrity, and availability of sensitive information held by VA in accordance with *NIST SP 800-30, Risk Management Guide for Information Technology Systems*. The assessments will review the Operating Unit's information systems, information, users, assess the probability of occurrence for potential losses and their effect, and recommend cost effective measures to reduce the Operating Unit's exposure to potential threats such as physical destruction or theft of physical assets; loss or destruction of information and program files; theft of information; theft of indirect assets; and delay or prevention of computer processing. A mission/business impact analysis will also be conducted.

a. Every risk assessment is made up of three components: facility risk assessment, identification of systems, and system risk assessment. System owners perform risk assessments for all information systems that are owned and operated by the facility, business partners or contractors, regardless of their location.

b. Risk assessment methodology encompasses ten primary steps. They are:

(1) The ISO, IT managers, and system managers form a risk management team;

(2) System characterization;

(3) Threat identification;

(4) Vulnerability identification;

(5) Control analysis;

(6) Likelihood determination;

(7) Impact analysis;

(8) Risk determination;

(9) Control recommendations; and

(10) Results documentation.

c. Each facility and/or Operating Unit will maintain current information/list on known system vulnerabilities, system flaws, or weaknesses that could be exploited by the threat sources. To ensure standardization and completeness of assessments, the facility or Operating Unit will use the Office of Cyber Security's approved risk assessment tool. The risk management team will collaborate to answer the multi-user system and facility questionnaires. A risk factor is calculated, weaknesses are identified, and a risk level is assigned.

2. Risk Mitigation: The ISO will review the risk assessment reports and recommendations and work with the information system managers, system administrators, and facility staff to mitigate the risks that are currently solvable. These mitigation decisions, additional procedures (if applicable) and responsibilities assigned will be documented and maintained by the ISO. The risk management team conducts a follow-up analysis to determine whether the security requirements and changes made adequately mitigate the vulnerabilities. The outstanding risks will be presented to the facility Director and the facility CIO for their review and action. The Director and CIO may accept the risks, provide necessary resources to mitigate the risk immediately, temporarily accept the risk and define future plans for risk mitigation, or disapprove use of the system. The decisions by the Director and the CIO will be maintained on file by the ISO. If additional funding for hardware, software, or services are needed to adequately protect information and reduce risks, the following issues should be considered:

a. Compatibility of the information system solution to the intended environment;

b. The sensitivity of the information;

c. The facility's security policies, procedures and standards;

d. Other requirements such as resources available for operation, maintenance, and training.

e. Costs.

3. On-going Evaluations: Risk assessments will be completed at least every three years and reviewed/updated annually by the appropriate risk management team or after a significant audit finding, or when the information system experiences significant enhancement or modification. Some examples of significant enhancements or modifications include change in operating system, change in hardware, change in the overall operating environment, and major system upgrades.

(2) Information Security Categorization

(a) **Policy:** VA information owners are responsible for analyzing their specific VA program/mission information and determining the security category. These categories provide a framework for evaluating the information's value and the appropriate controls required to protect it. VA has defined three basic security categories of information and additional handbooks may be issued to further categorize as appropriate and if necessary. These categories will enable information that requires security to be consistent, whether in a mainframe, client/server, workstation, file cabinet, desk drawer, waste basket, or in the mail. All information must be categorized by the information owner into one of the categories defined by VA. VA information owners are responsible for analyzing their specific VA program/mission information using the three security objectives for information, referred to as CIA:

(1) Confidentiality;

(2) Integrity; and

(3) Availability and determining the impact level on VA and for veterans if there is a breach of security that affects these three security objectives.

(4) There are three levels of potential impact on VA or veterans should there be a breach of information security (i.e., a loss of confidentiality, integrity, or availability (CIA)). They are low, moderate, and high. The impact level for each information type is needed to determine the level of protection required for the information and the security categorization of the system in which it resides. Per FIPS 199, an information type is a specific category of information (e.g., privacy, medical, proprietary, financial, investigative, contractor sensitive, security management) defined by an organization or, in some instances, by a specific law, Executive Order, directive, policy, or regulation.

(b) **Procedure:** VA has categorized VA information into the following three categories for security purposes:

(1) **VA Sensitive Data/Information** – See VA Sensitive Data/Information in the definitions in Appendix A for VA's formal definition as defined by Public Law 109-461. To further define, sensitive information is information that requires protection due to the risk of harm that could result from inadvertent or deliberate disclosure, alteration, or destruction of the information. The term includes information whose improper use or disclosure could adversely affect the ability of VA to accomplish its mission. Sensitive information within VA includes the following types of information: Sensitive Personal Information (SPI), and Regulatory/Program Specific Information (defined below). Information regarded as sensitive should be labeled as SENSITIVE. The impact level of sensitive information is high.

(a) Sensitive Personal Information (SPI) – also referred to as personally identifiable information (PII) or individually identifiable information. Refers to any information about an

individual maintained by an agency, including any information which can be used to distinguish or trace an individual's identity, such as their name, social security number, date and place of birth, mother's maiden name, biometric records, or any information that is linked or linkable to an individual. Education, financial transactions, medical history, and criminal or employment history are included. Individually identifiable health information, protected health information, and privacy-protected information are also included in this category. Below is additional clarification of these terms.

(1) Individually identifiable information – Individually-identifiable information is any information, including health information maintained by VHA, pertaining to an individual that also identifies the individual and, except for individually-identifiable health information, is retrieved by the individual's name or other unique identifier. Individually-identifiable health information is covered regardless of whether or not the information is retrieved by name.

(2) Individually identifiable health information - Individually-identifiable health information is a subset of health information, including demographic information collected from an individual, that is (1) Created or received by a health care provider, health plan, employer, or health care clearinghouse; and (2) Relates to the past, present, or future physical or mental condition of an individual; the provision of health care to the individual; or the past, present or future payment for the provision of health care; and (3) Identifies the individual or a reasonable basis exists to believe the information can be used to identify the individual. Also included in this category is individually-identifiable medical or health information maintained by VA on individuals who have applied for, been or have been treated for drug and alcohol abuse, infection with sickle cell anemia or testing and treatment for infection with HIV (38 U.S.C. § 7332). Individually identifiable health information encompasses protected health information.

(3) Protected health information (PHI) – Health information maintained in any form protected under the HIPAA Privacy and Security Rules, 45 Code of Federal Regulations, Parts 160 and 164. Also included in this category is health information in a limited data set.

(4) Privacy-protected information – All individually-identifiable personal information that is protected under Federal law. Privacy-protected information encompasses personally identifiable information, individually identifiable information, individually identifiable health information, and protected health information.

(b) Regulatory/Program specific information - Information that VA may not release or may release only in very limited, specified situations. This category of information, which normally would not be released to the public (5 U.S.C. Section 552 – the Freedom of Information Act), may include certain critical information about VA's programs, financial information, law enforcement or investigative information, procurement information, and business proprietary information. This means that additional procedures/review must be conducted prior to release of this category of information. The FOIA Officer can provide additional guidance on what particular documents would fall under each of these categories. Some examples are:

(1) Certain Medical Quality Assurance Records (38 U.S.C. § 5705).

(2) Limitations on access to financial records (38 U.S.C. § 5319)

(3) Security and law enforcement in Property Under the Jurisdiction of the Dept. of Veterans Affairs (38 U.S.C. , Chapter 9)

(4) Names and addresses of active duty members, veterans, and their dependents. (38 U.S.C. § 5701).

(5) Records of information compiled for law enforcement purposes; i.e., civil, criminal, or military law.

(6) Proposals submitted by a contractor in response to requirements of a solicitation for a competitive proposal (41, U.S.C. § 253b(m))

(7) Inter-agency or intra-agency memoranda or letters which would not be available by law to a party other than an agency in litigation with the agency

(8) VA information technology (IT) internal systems information revealing infrastructure used for servers, desktops, and networks; application name, version and release; switching, router, and gateway information; interconnections and access methods; mission or business use/need. Examples of information are systems inventories and enterprise architecture models.

(9) Information that could result in physical risk to personnel.

(2) **Administratively Confidential Information** – Information that is used in the daily operation of the VA. Any information that cannot be classified as Sensitive or Public is categorized as Administratively Confidential Information. Normally, Administratively Confidential Information is not labeled as such. Access to this information by individuals not conducting VA business is not authorized (except as required by law). This is information that is intended for use by employees when conducting VA business. The impact level is generally considered Low or Moderate, based on the CIA analysis formula. Some examples are:

a. Operational business information and reports

b. Non-VA information that is subject to a nondisclosure agreement with another company

c. VA phone book

(3) **Public Information** - Information is categorized as Public if the information has been made available or could be made public pursuant to a FOIA request for public distribution through authorized VA channels. Public information is not sensitive in context or content, and requires no special security. Some examples are:

a. VA Annual Reports

b. VA information disclosed pursuant an appropriately executed FOIA request or VA information available in the VA FOIA Reading Room.

c. Information specifically generated for public consumption, such as public service bulletins, marketing/informational brochures, and advertisements. Generally, information that is readily available from the public media or is a matter of public record is classified as Public. Information in this classification should be limited to that required by law or regulation and that which is specifically intended for public consumption. To allow other information to be viewed by the public would serve only to provide a potential advantage to competitors and provide the

media with the opportunity to shed an unfavorable shadow on the VA's reputation. Normally, Public information is not labeled as such and is normally considered Low impact.

(4) The process used by information owners to determine their category and impact level of specific program/mission information is as follows:

a. The potential impact is low if the loss of CIA of the information could be expected to have a limited adverse effect on VA operations, assets, or individuals.

b. The potential impact is moderate if the loss of CIA of the information could be expected to have a serious adverse effect on VA operations, assets, or veterans.

c. The potential impact is high if the loss of CIA of the information could be expected to have a severe adverse effect on VA operations, assets, or veterans.

(5) The security category and impact level of an information type is applicable to information in either electronic or non-electronic form.

(6) Establishing an appropriate security category of an information type requires determining the potential impact for each security objective associated with the particular information type.

(7) The generalized format for expressing the security category of an information type is:

Security Category, information type = {(**confidentiality**, impact), (**integrity**, impact), (**availability**, impact)}

Where the acceptable values for potential impact are Low, Moderate, or High

(8) The overall impact value assigned to the information is the highest value assigned to any one security component. For example:

Security Category, health records = {**(confidentiality**, high), (**integrity**, high), (**availability**, moderate)] = High

(3) System Security Categorization

(a) **Policy:** All VA information systems must have a security categorization in accordance with FIPS 199 and must document the results of this categorization in the system security plan. Designated VA OCS staff review and approve the security categorizations as part of the C&A process in accordance with *NIST Special Publication 800-37, Guide for the Security Certification and Accreditation of Federal Information Systems*.

(b) Security categorization standards for information systems provide a common framework and understanding for expressing security that, for the Federal government, promotes effective management and oversight of information security programs.

(c) **Procedure:** The determination of an information systems security categorization will be made in accordance with *FIPS 199* so that the appropriate controls can be implemented throughout the system development life cycle (SDLC). For nationally deployed information systems, the FIPS 199 categorization will be made by OI&T system development and will be

approved during the C&A process of the system prior to deployment to the field. The designation will be included in the security plan. For any locally developed information systems, the Operating Unit will utilize *NIST 800-60, Guide for Mapping Types of Information and Information Systems to Security Categories* to determine the sensitivity for the information system during the development of the system.

(4) System Security Plan (SSP)

(a) **Policy:** Every information system must be included/covered by a system security plan (SSP). The plan will contain all the elements outlined in *NIST Special Publication 800-18, Rev 1, Guide for Developing Security Plans for Information Technology Systems"* as well as the appropriate security controls as outlined in *NIST Special Publication 800-53, "Recommended Security Controls for Federal Information Systems.*"

(b) **Procedure:** The SSP provides an overview of system security requirements and the controls that are in place or planned to meet those requirements. SSPs are used to document system characterization, management controls, operational controls, and technical controls mapped back to the NIST 800-53 controls matrix. The SSPs are living documents, developed during the design phase and updated throughout the entire lifecycle. The SSPs are a major component in the certification and accreditation process for the system and will be reviewed and approved by the Certification Agent (CA) and the Authorizing Official Designated Representative (AODR) within OCS. The system managers and information system management, in close coordination with the ISO, are responsible for ensuring that SSPs are developed, reviewed annually, and maintained for each system within their area of responsibility. Significant changes are identified in the configuration management process as discussed in the IT System Hardware and Software Maintenance section of this document. A summary of the security plans for each facility's systems will be included in the overall facility OI&T strategic plan. The ISO plays an active role in reviewing SSPs as well as providing guidance on the security impact of changes to the system. Sites will utilize the templates provided by VA in developing their system security plans.

(5) Rules of Behavior

(a) **Policy**: Rules of Behavior (ROB) are required by FISMA, *OMB Circular A-130, Appendix III* and by the security controls contained in *NIST SP 800-53.* All individuals who use or gain access to VA information systems must read, understand and agree by signature to adhere to the VA National Rules of Behavior, before they can be authorized access to VA information systems.

(b) **Procedure**: VA has established a set of rules that describe the responsibilities and expected behavior with regard to information system usage. These rules clearly delineate security responsibilities and expected behavior of all system owners, users, operators, contractors and administrators. The rules include the consequences of inconsistent behavior or non-compliance. The rules include all significant aspects of information system use. The entire workforce will have access to a copy of these rules of behavior for review. A signed (manually or electronically) acknowledgement of these rules is a condition of access to any VA information system. The ISO is responsible for ensuring that a copy of a signed ROB for each member of the workforce, who has access to an information system, is readily available to management, if required.

(6) System and Services Acquisition

(a) **Policy:** The Operating Unit determines, documents, and allocates as part of its capital planning and investment control process the resources required to adequately protect the information systems.

(1) Outsourced Information System Services – Operating Units ensure that third-party providers of information system services employ adequate security controls in accordance with VA policy. Each facility monitors security control compliance. In contracts/agreements for hardware, software, computer-related services, or access to VA information systems, appropriate security requirements, specifications, and training must be included in statements of work and security requirements and specifications should be properly implemented before the system goes into operation and through the life cycle of the system. The security requirements and/or security specifications that are explicitly identified in information system acquisition contracts are based on an assessment of risk.

(2) All VA acquisitions of IT technology and services must be approved through the VA Acquisition Approval System as directed by the VA CIO.

(b) **Procedure:** The solicitation documents for information systems and services will include OI&T/Acquisition & Logistics approved standard security language. The ISO shall review all acquisition requests for OI&T products and services requested by their facility/program office. Their review is to ensure security is addressed throughout a system's life cycle, from mission and business planning through disposal. The ISO will participate on the local OI&T equipment committees to ensure security is addressed at the beginning of the life cycle of the system.

(1) Third party providers are subject to the same information security policies and procedures as the facility, and must conform to the same security control and documentation requirements as would apply to the facility's internal systems.

(2) The outsourced information system services documentation includes government, service provider, end user security roles and responsibilities and any service level agreements.

(3) The service level agreements define the expectations of performance for each required security control, describe measurable outcomes, and identify remedies and response requirements for any identified instance of non-compliance.

(7) System/New Technology Development Life Cycle

(a) **Policy:** Security must be implemented for all new system development and prior to new technology implementation within VA.

1. VA manages the information systems using a system development life cycle methodology that includes information security considerations. VA designs and implements their information systems and new technology (i.e., wireless, IPv6) utilizing security engineering principles. New technology must include control tests and evaluations, address any specific configuration requirements, additional monitoring, and any specialized training required.

2. All new VA systems will include the capability for recovery/decryption of any encrypted/protected information. Successful demonstration that the recovery/decryption process works is required prior to being granted any authority to operate.

3. Systems that cannot provide such recovery/decryption capabilities must be reviewed by the OIG, then subsequently agreed to by the VA CIO prior to system development and also prior to receiving authority to operate.

4. All new VA systems must include read-only capability for OIG and other authorized oversight and law enforcement entities. This requirement must be functional prior to being granted any authority to operate. Systems that cannot provide this capability must be agreed to by the VA CIO prior to system development and also prior to receiving authority to operate.

(b) **Procedure:** The system development life cycle is a proven series of steps and tasks (see Figure 1) used to build and maintain quality systems faster, at lower costs, and with less risk. Each information system operates in one of the below stages of system development. Any locally developed system will follow the life cycle steps and be certified and accredited prior to implementation. During the development of any system, security requirements will be defined. The information system developer creates and implements a configuration management plan that controls changes to the system during development, tracks security flaws, requires authorization of changes, and provides documentation of the plan and its implementation. The information system project manager/developer also creates a security test and evaluation plan, implements the plan, and documents the results. Developmental security test results may be used in support of the security certification and accreditation process for the delivered information system. In addition, a PIA must be performed and a System of Records Notice (SORN) need must be determined in the initial stage. These are the security steps of the system development lifestyle:

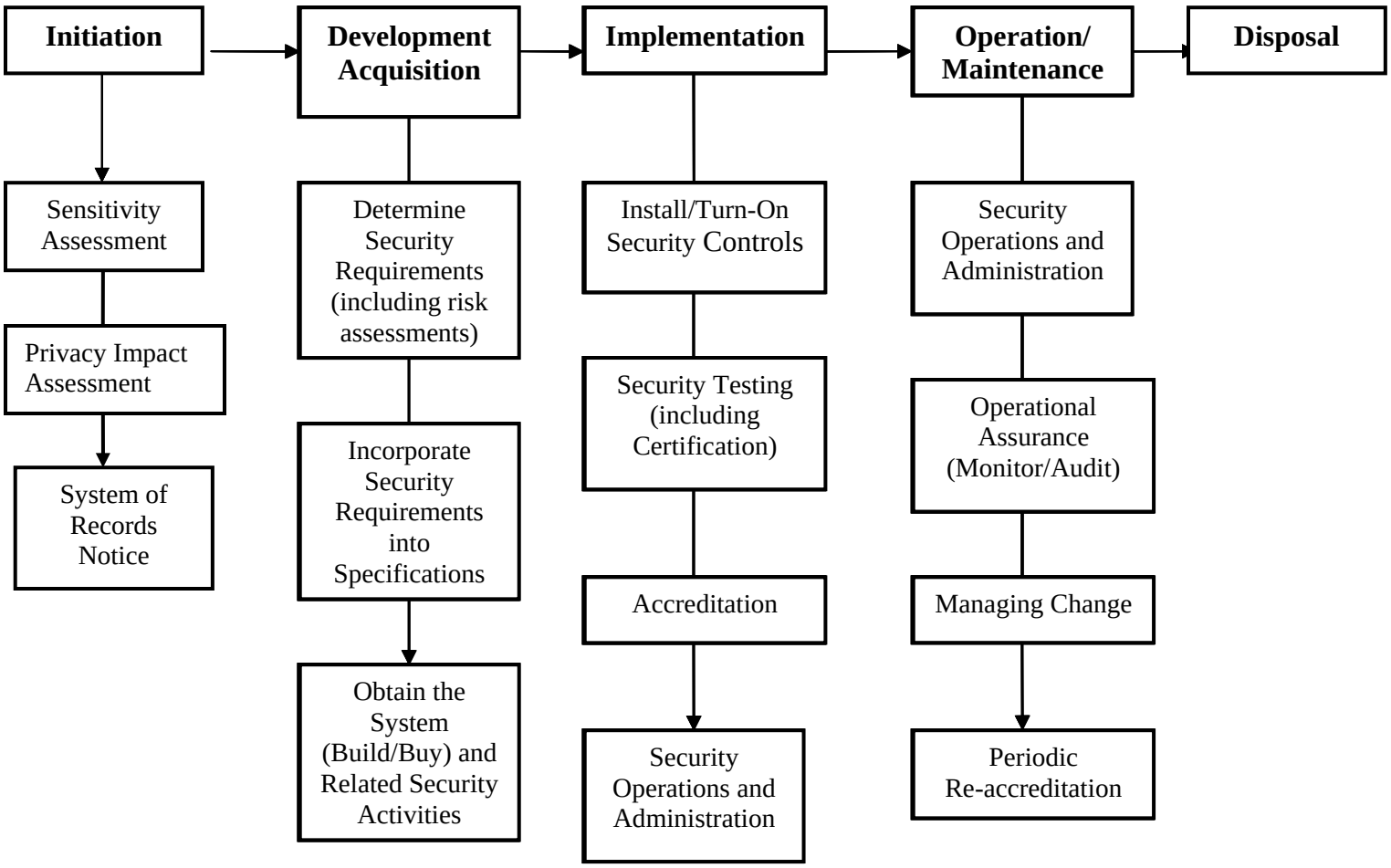
Initiation
Development Acquisition
Implementation
Operation/ Maintenance
Disposal
Sensitivity Assessment
Privacy Impact Assessment
System of Records Notice
Determine Security Requirements (including risk assessments)
Incorporate Security Requirements into Specifications
Obtain the System (Build/Buy) and Related Security Activities
Install/Turn-On Security Controls
Security Testing (including Certification)
Accreditation
Security Operations and Administration
Security Operations and Administration
Operational Assurance (Monitor/Audit)
Managing Change
Periodic Re-accreditation
Computer Security Plan

Figure 1

(8) Security Documentation

(a) **Policy:** Adequate documentation for VA information systems and its constituent components is maintained, protected when required, and distributed to authorized personnel. OI&T system managers and OI&T Chief/CIO in conjunction with the ISO must ensure that sufficient documentation is developed and maintained to formalize security and operational procedures for the Operating Unit's information systems.

(b) **Procedure:** In addition to the certification and accreditation documentation (security plan, risk analysis, contingency plan, and testing documentation) the following documentation will be maintained for each system, if applicable:

1. User manuals for software;

2. In-house application documentation (application requirements/program documentation, specifications/change control recommendations);

3. Any vendor-supplied documentation;

4. Standard operating procedures;

5. Network diagrams and documentation on setups of routers and switches;

6. Software and hardware testing procedures and results;

7. System interconnection agreements;

8. Hardware replacement agreements;

9. Vendor maintenance agreements and maintenance records; and

(c) The ISO will conduct annual reviews of security documentation with system owners, system managers, and other OI&T personnel.

(9) Business Associate Agreements

(a) **Policy:** The Contracting Officer, the Privacy Officer and the ISO will work together to identify entities that are Business Associates under the HIPAA Security Rule and ensure that Business Associate Agreements (BAAs) are enacted for all Business Associates in accordance with HIPAA BAA policies and procedures.

(b) **Procedure:** All contracts, agreements, purchase orders, and relationships must be assessed to determine if a business associate relationship exists. A business associate relationship exists if a VHA health care facility is required to release protected health information to a contractor or business partner in order for them to provide services on the facility's behalf. If a business associate relationship is determined to exist, a BAA must be enacted utilizing VHA Privacy Program approved BAA language. If a business associate is determined to serve more than one VA medical center, a national BAA may be enacted through the VHA Privacy Office. BAAs must be kept updated and documentation of agreements must be maintained as long as the agreement is in force. The VHA Privacy Office

maintains a web portal with all the nationally approved BAAs listed as well as the BAA approved language.

(10) Certification and Accreditation

(a) **Policy:** VA authorizes all systems for processing before operation and updates the authorization every three years, or whenever a significant change to the system environment occurs. All VA systems must be certified and accredited in accordance with *NIST Special Publication 800-37, Guide for the Security Certification and Accreditation of Federal Information Systems*. Security certification and accreditation are important activities that support a risk management process and are an integral part of an operating unit's information security program. VA officials sign and approve the security accreditation.

(b) **Procedure:** The initiation phase consists of three tasks:

1. Preparation;

2. Notification and resource identification; and

3. System security plan analysis, update, and acceptance. This phase requires that the appropriate security controls based on *NIST SP 800-53* are instituted and documented in the system security plan.

a. Each facility conducts an assessment of the security controls in their information systems to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the systems. The security certification phase consists of three tasks:

(1) Security control assessment (SCA);

(2) Security certification documentation; and

(3) Plan of action and milestones (POA&M).

(b) Testing is required to certify that the system meets the determined security requirements and testing must be accomplished prior to receiving full accreditation. Testing validates system compliance with the security policy and requirements stated in the system's documentation. Testing consists of but is not limited to a technical system test and evaluation, a penetration test, communications security evaluation, system management analysis, site evaluation, contingency plan evaluation, and risk analysis evaluation.

(c) Testing must be accomplished by a team from outside of the facility responsible for the system. Using the results of the testing, each facility then develops and updates periodically, a POA&M for the information system. A POA&M documents the planned, implemented, and corrected remedial actions taken to correct any deficiencies noted during the security controls assessment, risk assessment and any audits or reviews conducted on the system.

b. Each facility submits the required documentation to the appropriate VA official (determined by OCS) for authorization for processing (accreditation). The security accreditation Phase consists of two tasks:

(1) Security accreditation decision;

(2) Security accreditation documentation.

(a) The purpose of this phase is to determine if the remaining known vulnerabilities and risks are of an acceptable level of risk to the facility. A security plan, risk analysis, and a contingency plan are required to help make the appropriate decision.

(b) Upon successful completion of this phase, the system will have either an authorization to operate; an interim authorization to operate under specific terms and conditions; or denial of authorization to operate.

c. The continuous monitoring phase consists of three tasks:

(1) Configuration management and control;

(2) Security control monitoring and auditing;

(3) Status reporting and documentation

(a) Systems must be re-accredited by the system owner every three years or whenever a major change has been made to the system that may affect its security.

(b) Major changes include: an increase in the sensitivity/criticality of a system; an increase in threat level; policy change, a change in operating system (base platform); a change to security relevant software; a change to hardware that could affect the security architecture; an increase in interconnection with other systems outside the accreditation boundary; or significant changes in the security requirements that apply to the system.

(11) System Analysis/Identification

(a) **Policy:** All automated information resources that collect, process, transmit, store, or disseminate VA information must be identified, regardless of ownership.

(b) **Procedure:** The Operating Unit will include all automated information resources operated by the Operating Unit or facility or by contractors in support of VA work. The system owners and system managers working with the ISO will identify and analyze the system's boundaries and organizational responsibilities by utilizing the following four NIST criteria:

1. Be under the same direct management control. Direct management control does not necessarily imply that there is no intervening management. It is also possible for an information system to contain multiple subsystems. (For definition of subsystem see *NIST SP 800- 18, Revision 1, page 9)*;

2. Have the same function or mission objective;

3. Have essentially the same operating characteristics and security needs;
4. Reside in the same general operating environment.

(12) Federal Information Security Management Act

(a) **Policy:** The Operating Unit will conduct, as mandated by FISMA, an annual assessment for all applicable systems and the overall security program within the Operating Unit's control. Deficiencies identified during this assessment will be entered into the agency's approved database and the POA&M.

(b) **Procedure:** FISMA Annual Assessment survey is a review of the VA's overall information security program and includes the review of IT system security controls, the system boundary, and its interconnected systems. To meet this requirement, systems must be identified and entered into the VA approved database. Systems can be combined into groups based on system identification. Systems can be added or deleted from the VA approved database periodically based on their system life cycle designation. ISOs, system owners, system managers, and OI&T management and other offices with significant security responsibilities will complete the FISMA questionnaire. The questionnaire documents the security controls in place, their effectiveness, the POA&M to remediate any deficiencies noted, the anticipated completion date, and the actual completion date. OCS reviews and maintains the database, prepares the FISMA report for OMB, and monitors the department's POA&Ms.

(13) System Interconnections

(a) **Policy:** The Operating Unit authorizes connections (physical and wireless) from the information systems to other information systems outside of the accreditation boundary and monitors/controls the system interconnections on an ongoing basis. Local OI&T management and the ISO approve information system interconnection agreements. A System Interconnection Agreement (SIA) is not needed with internal agency systems if an agency manages and enforces a rigid system development life cycle, which requires approvals and sign-offs ensuring compliance with security requirements. If a system interconnection exists where VA controls information from other entities (e.g., Social Security Administration, DOD, FAA) VA must protect the information at the same level as similar VA information. If additional requirements are required, they should be outlined in the Memorandum of Understanding (MOU) and/or the System Interconnection Agreement (SIA).

(b) **Procedure:** The Operating Unit must prepare a MOU, stating the terms and conditions for sharing information and information resources, and a SIA, specifying the technical and security requirements for the connection, for each system interconnection. The MOU and SIA will be obtained prior to connection with other systems and/or sharing of sensitive data/information. It should detail the rules of behavior that must be maintained by the interconnecting systems.

b. Operational Controls

(1) Personnel Security

(a) **Policy**: Per VA Directive 0710, Personnel Suitability and Security Program, VA requires that a risk designation is assigned to all Federal and contractor positions and that screening criteria are established for filling those positions. These risk designations must be reviewed at least every three years and revised, if required.

1. VA requires that all personnel be subject to an appropriate background screening prior to permitting access to VA information and information systems. This includes VA applicants,

appointees, employees, contractors, and other individuals who require physical and/or logical access to VA information or information systems to perform their jobs. For medical equipment maintenance contracts, the contracts shall include the requirement that the vendor is responsible for conducting background screening.

2. When employment is terminated, VA requires termination of the user's information system access, exit interviews, and the return of all organizational information and information system related property (e.g., keys, identification cards, building passes) in a timely manner; and that appropriate personnel have access to official records created by the terminated employee that are stored on VA information systems before the systems are recycled or disposed.

3. VA requires that all information systems/facilities access authorizations are reviewed when individuals are reassigned or transferred to other positions within the organization and appropriate actions (e.g., reissuing keys, identification cards, building passes, closing old accounts and establishing new accounts, and changing system access authorizations) are completed.

(b) **Procedure:**

1. Screening, as defined by VA Directive and Handbook 0710, of federal employees and contract personnel who participate in the design, development, operation, or maintenance of sensitive applications and sensitive systems, as well as those individuals having access to VA sensitive information or information is required. The COTR will ensure screening is conducted for all contract personnel and Human Resources personnel will ensure that screening is conducted for federal employees and all other appointed workforce members.

2. Position Descriptions: Supervisors will ensure position descriptions are written to reflect specific security responsibilities. Within this context, "significant security responsibilities", refer to employee obligations to protect VA sensitive information and to use such information, and the information derived from it, only in the execution of official duties. In conjunction with supervisors, Human Resources will use the completed VAF 2280 to annotate position descriptions with the risk/sensitivity level designations. These designations will be used to determine the appropriate background investigation level. OI&T requires that an assessment of all designations shall be done every three years in order to identify any changes in the information available or the duties and responsibilities of the position that would cause the position to be placed in a higher or lower category.

3. Background Investigations: The level of screening required will vary from minimal checks to full background investigations, depending upon the sensitivity of the information to be handled and the risk and magnitude of loss or harm that could be caused by the individual. Procedures for completing background investigations are contained in *VA Directive 0710 and its Handbook, "Personnel Suitability and Security Program.*"

4. Contractors: All non-VA users having access to VA information resources through a contract, agreement, or arrangement shall meet the security levels defined by the contract, agreement, or arrangement. Such users will read and sign the Rules of Behavior and complete security awareness and privacy training prior to receiving access to the information systems. Clauses must be included in the procurement document(s) to prevent the contractor from inappropriately using or disclosing the information during the course of the contract, agreement, or arrangement and after it has terminated. Contractors must adhere to Business

Associate Agreement requirements, as applicable. The COTR for contracts must monitor contractor compliance to ensure adequate security.

5. Transfers/Termination of Employees: When an employee transfers, both the losing and gaining services will adjust system menu access as necessary to ensure appropriate minimum-necessary access is granted. When an employee resigns from their position, their supervisor will ensure that all access is removed. In both instances, the following must be ensured:

a. Employee no longer has possession of unneeded VA sensitive information media;

b. Employee has returned all unneeded keys and access devices as applicable;

c. Employee security codes, electronic signatures, system menu options, and security keys for both local and remote systems have been reviewed for either alteration or termination;

d. Employee is debriefed on their responsibility to protect VA sensitive information used on the job from unauthorized disclosure;

e. Appropriate personnel have access to official records created by the employee who has transferred or resigned that are stored on facility systems.

(1) When an employee is removed or discharged from his or her position, the following procedures should be implemented:

(a) Termination of system access at the same time (or just before) the employee is notified of their dismissal or upon receipt of resignation;

(b) If applicable, during the "notice of removal/discharge" period the user may be assigned to a restricted area and function. This may be particularly true for employees capable of changing programs or modifying the system or applications;

(c) In some cases, physical removal of the employee from the facility may be necessary.

6. Without Compensation (WOC): Any individual that is not covered under a paid program, but works as a VA employee should have a WOC status. Access granted to these individuals shall be limited to non-sensitive, read-only information, whenever possible. These individuals must be supervised if granted access to information systems or VA information. All access requests for Volunteers, WOC and Work Study Students shall be routed through the ISO for review and concurrence.

7. Responsibility Coverage/Cross-training: Employees will be cross-trained in other facility roles to ensure responsibilities are covered in order to continue facility operations during other employees' scheduled time off. Mandated vacations, as well as cross training, are encouraged to provide additional security controls.

(2) Corrective Actions (Sanctions)

(a) **Policy:** The Operating Unit will apply appropriate corrective actions against workforce members who fail to comply with the security policies and procedures, and Rules of Behavior. The corrective actions process is included in VA's Human Resources' policies and procedures.

(b) **Procedures:** The ISO will determine and provide evidence of a security violation. The employee's supervisor will determine appropriate action and may, in conjunction with human resources, take the necessary steps and apply appropriate corrective actions for employees who are non-compliant with the security policies and procedures. Actions may include, but are not limited to, progressive discipline or other resolutions. Appropriate legal authorities outside of VHA may levy civil or criminal sanctions as a result of a HIPAA security complaint.

(3) Separation of Duties

(a) **Policy:** Separation of duties methodology is enforced for each information system. Separation of duties refers to dividing roles and responsibilities so that a single individual cannot subvert a critical process.

(b) **Procedure:** Supervisors must analyze the duties performed by their employees to ensure separation of duties and verify that users only have the system privileges that are needed to perform their assigned duties (least privilege). The ISO will help ensure that separation of duties issues are identified and appropriate actions taken to correct any conflicts. This type of control must ensure that a single individual cannot subvert a critical process. Supervisors should ensure that a single individual does not perform combinations of functions including, but not limited to:

1. Data entry and verification of data;

2. Data entry and its reconciliation to output;

3. Input of transactions that may result in a conflict of interest, fraud, or abuse (e.g., input of vendor invoices and purchasing and receiving information);

4. Data entry and approval functions.

5. Some examples of this principle include: The same individual should not enter and authorize a purchase order; the same individual should not request a user account and also create the account in the system; the system administrator should not be the one to conduct the audits/reviews of the system he/she is administering; and the ISO should not be a system administrator.

(4) Physical Security Controls

(a) **Policy:** VA will implement physical and environmental security controls to protect systems, buildings, and related supporting infrastructures from individual and environmental threats. Specific physical security requirements and options are found in VA Directive and Handbook 0730, "Security and Law Enforcement Appendix B".

(b) **Procedure:**

1. Physical Access Control Systems (PACS) – IT spaces, including but not limited to those identified in paragraph 2.a. through f. shall be protected with PACS equipment. In VHA facilities, the PACS system owner is the VA Chief of Police. In VBA or NCA facilities, the system owner is the facility director or designee. The PACS owner will grant access based on

a request from the OI&T Chief/CIO. The OI&T Chief/CIO will maintain internal access approval lists as described in subparagraph 2.

2. Access to locations that contain equipment or information critical to the information infrastructure shall be limited to authorized personnel. The OI&T Chief/CIO approves, maintains, and reviews a list of personnel based on system impact levels time frame as defined in Appendices D and E, with authorized access to these areas. These locked locations include, but are not limited to:

a. The computer room;

b. Telephone switch rooms (PBX);

c. The main telecommunications demarcation point if not located in computer room or PBX room;

d. Data/Telecommunication Closets;

e. IT storage areas; and

f. IT technician work areas

3. Direct physical access to these locations will be limited to authorized staff designated by OI&T Chief/CIO. All other entry into these areas will be prohibited unless authorized and accompanied by authorized IT staff. OI&T staff will coordinate and authorize access to areas that have co-located equipment, which is managed or supervised by a department other than OI&T.

4. Physical access is controlled to information systems by authenticating visitors before authorizing access to facilities or areas other than areas designated as publicly accessible. All visitors, contractors, maintenance, and housekeeping personnel are required to establish pre-planned appointments with OI&T prior to receiving access to sensitive areas. Visitors to restricted OI&T areas will be monitored and escorted. Each facility maintains a visitor access log that minimally includes:

a. Name and organization of the person visiting;

b. Signature of the visitor;

c. Form of identification;

d. Date of access;

e. Time of entry and departure;

f. Purpose of visit; and

g. Name and organization of person visited.

5. The ISO will review access logs, based on system impact levels as defined in Appendices D and E, and will provide the findings to the CIO.

6. Entrance doors to sensitive areas shall remain locked, unless necessary to open for deliveries or maintenance of equipment. All entrances to sensitive areas will have a sign-in/sign-out log for tracking individuals entering these areas. A list of individuals who are assigned a security code or key to access these sensitive areas will be maintained by OI&T Chief/CIO and the facility Police, if applicable. These logs will be reviewed periodically by the ISO and OI&T Chief/CIO for discrepancies and follow-up actions. Each facility/program office shall monitor real-time intrusion alarms and employ automated mechanisms to ensure potential intrusions are recognized and appropriate response actions initiated.

7. Physical access to storage media containing sensitive information shall be secured by locks and other access controls based on the highest *FIPS 199* security category of the information recorded on the media. Removal or movement of the media within the facility/program office is authorized by the Operating Unit and logged as applicable.

8. Each facility secures keys, combinations, and other physical access devices and inventories those devices annually. Changes to combinations and keys occur periodically, when keys are lost, combinations are compromised, or individuals are transferred or terminated. After an emergency-related event, re-entry is restricted to authorized individuals only.

9. Emergency access to sensitive areas will be coordinated by facility police and require police escorted entry, as appropriate. Facility police will maintain a log of emergency access and submit a follow-up report to OI&T Chief/CIO. OI&T Chief/CIO will provide the facility's Chief of Police and Security Services and the disaster emergency coordinator a list of names of OI&T individuals who would need access to the facility, in support of restoration of lost information under the disaster recovery plan and emergency mode operations plan in the event of an emergency.

10. Facility access by veterans, visitors and the general public is addressed in statute and regulation. See Title 38 United States Code Chapter 9, "Security and Law Enforcement", Title 38 Code of Federal Regulations §1.218; and VA Directive and Handbook 0730, Security and Law Enforcement, for further information.

11. All members of the workforce must wear ID badges.

12. Physical security reviews will be conducted and documented by the ISO on an annual basis as part of the annual review of the System Security Plans. These reviews will help analyze any new or existing physical security vulnerabilities. Corrective measures will be taken, when appropriate. Physical security reviews conducted by Police and Security Service will be made available to the ISO.

13. Maintenance records will be kept to document repairs and modifications to the physical components of a facility which are related to security (for example, hardware, walls, doors, and locks).

14. Work Area/Remote Access Security; Hardware, Software, and Information Concerns:

a. All employees, contractors, volunteers, students, and others are responsible for protecting the information equipment located within their work areas and any equipment used when working remotely.

b. Authorized equipment is for authorized use only;

c. Employees, contractors, volunteers, students, and others are required to implement physical safeguards for all equipment that accesses VA sensitive information. Equipment must be housed and protected to reduce the risks from environmental threats and hazards, and the opportunities for unauthorized access, use, or removal.

d. Portable computers that have sensitive information on their storage device(s) or have software that provides access to VA private networks must be secured under lock and key when not in the immediate vicinity of the responsible employee. This includes external hard drives and other storage devices. If such devices are maintained in a hotel room or residence, they must be stored out of sight and the door(s) to the room or residence must be locked when the employee is not physically present.

e. Employees must use physical locks to secure portable computers when the computers must be left in a meeting room, or other semi-public area to which individuals other than the authorized employee have access.

f. When in an uncontrolled environment, employees must follow “clear desk” practices for media to reduce the risk of unauthorized access to, loss of, and damage to VA sensitive information. Clear desk practices include removing any VA sensitive information, in any form, from desks, work areas, hotel room desks, printers, etc.

g. When in an uncontrolled environment (for example, when traveling on an airplane or in an airport), employees must guard against disclosure of VA sensitive information through eavesdropping, overhearing or overlooking (shoulder surfing) by unauthorized persons. When traveling, employees must keep portable computers or storage devices in their possession and may not check them as baggage.

h. Information and system backups that include VA sensitive information have the same confidentiality category as the originals. Therefore, these materials must be protected with the same or equally effective physical security as that provided to the source computer, its media, and information contained therein.

i. Backups must be stored where they are physically secured yet accessible within a reasonable time frame when they are needed.

j. Employees, contractors, volunteers, students, and others will log-off of information systems when leaving work areas and/or invoke a password protected screen saver;

k. Employees, contractors, volunteers, students, and others will protect information contained on printouts and other media by keeping VA sensitive information in locked files or cabinets when not in use, and dispose of VA sensitive information through shredding or other approved disposal methods;

l. To the extent possible, computer monitors will be positioned to eliminate viewing by unauthorized personnel. When computer monitors cannot be positioned to eliminate viewing by unauthorized personnel, the deployment of a privacy screen, which allows viewing only from straight on, will be used;

m. Users will not use function keys or scripts to store passwords or other VA sensitive information;

n. Supervisors are responsible for keeping their employees informed of proper procedures for fire safety, removal of equipment from VA premises, protection of equipment and information, and reporting theft of VA assets;

o. Supervisors are responsible for ensuring appropriate measures are taken to protect workstations and other peripheral equipment located within their areas of responsibility from misuse, theft, or unauthorized use; and

p. Classes of workstations that have specific functions (i.e., VHA's CareVue, Pyxis, PACS) should have their own set of user security controls and requirements.

15. Physical and logical configurations and changes:

a. Physical and logical modifications shall be strictly controlled and must be performed under the supervision and authority of OI&T personnel.

b. Users should be certain that the technician(s) performing maintenance is authorized by OI&T. Additionally, circuit boards or components should not be removed without the express approval of OI&T. Users are expected to challenge anyone not complying with this procedure.

c. VA policy prohibits the use of personally owned information systems for official U.S. Government business involving the processing, storage, or transmission of federal information unless a waiver is obtained.

d. Information technology systems or devices not specifically purchased or authorized by OI&T's Chief/CIO are prohibited from being connected to the VA local and wide area network or any other OI&T resource. This includes, but is not limited to, software applications, zip drives, thumb drives, CD burners and printers. OI&T will not support any system or application not approved through the national IT Tracking System and the local OI&T Chief/CIO. OI&T is authorized to remove from the network or OI&T resources, any system or application that does not meet national and/or local purchasing or security requirements.

e. For medical devices the procedures outlined in VA Directive 6550 must be followed. As a minimum, the local OI&T CIO, ISO and Chief of Biomedical Engineering must concur in the procurement of these devices since they will be connected to the OI&T controlled network and generally have the potential to store sensitive information. As part of the approval process, there must be assurance that a disciplined methodology exists to ensure sensitive information is not retained on the device in large amounts or for extended periods of time. Picture Archiving and Communications Systems (PACS) are excluded from this provision provided these devices are in a protected area as approved by the local OI&T CIO and ISO.

f. Only OI&T management will authorize the movement of computer equipment from one physical location to another.

g. When appropriate, all VA sensitive information will be backed-up and secured prior to moving equipment such as servers and mainframes.

h. Each Operating Unit controls information system-related items (i.e., hardware, firmware, software) entering and exiting the facility and maintains appropriate records of those items. Supervisors and managers, following local Acquisition and Logistics Service property rules and regulations, shall control the removal, loan, and inventory of OI&T equipment from the facility for use off-site.

i. Rooms where hardware or master console and control capabilities are located will be secured, or lockdown systems installed to secure the equipment to a table or desk.

16. Information Concerns:

a. All VA employees, contractors, business partners, and any person who has access to and stores VA information must ensure that all VA information is protected from risk of inadvertent or deliberate misuse, fraudulent use, improper disclosure, or destruction.

b. Securing Sensitive Documents: Forms, and other types of printed output produced by any computer system, will be evaluated by the responsible staff member for information sensitivity. Printed output containing VA sensitive information should be labeled as such, stored in locked cabinets or desks, and disposed of properly by shredding or placement in specially marked containers for shredding or recycling. All employees are responsible for retrieving all printed outputs they request from printers or facsimile machines in a timely manner. Information that is in public view or to be sent outside a secure location will be labeled appropriately.

c. Each Operating Unit controls information system media (paper and electronic) based on VA categorization and restricts the pickup, transfer, and delivery of such media to authorized personnel as required by VA policy.

d. When no longer needed, VA sensitive information must be destroyed by a method rendering it unreadable, undecipherable, and irretrievable as outlined in VA's current electronic sanitization procedures.

e. If computer-readable data extracts from databases are created that contain VA sensitive information, they must be logged and destroyed within 90 days unless they are still required. Once they are no longer required, they must be destroyed.

f. Storage of boxes, paper, etc. containing VA sensitive information is prohibited within VA Data Centers.

17. Software Concerns:

a. Software Licensing: All software, Shareware, and Public Domain software installed on workstations shall be installed by and registered with IT operations within the facility/program office. Approval must be granted from OI&T and VA Contracting Officers (or their designees) before an individual can use personally-owned software on any VA information system. Use of pirated or illegally obtained software on any VA information system is strictly prohibited. To ensure compliance with software copyright and licensing agreements, not less than annually, OI&T appointed staff shall conduct computer audits. OI&T has the authority to remove or disable any unapproved or pirated software found. The OI&T Chief/CIO, the ISO and VA NSOC shall be notified in accordance with the VA Incident Reporting policy.

b. All devices, except medical devices, that connect to any VA information systems, either on site or from a remote location, must be updated with the latest security patches as they are distributed. Medical devices under FDA control must have patches tested and approved prior to implementation. Due to this security risk, all medical devices must be placed on a Virtual Local Area Network (VLAN).

18. Environmental Controls:

a. Fire Safety: The ISO works with the responsible facility services to ensure that appropriate fire safety mechanisms and preventive measures are in place to adequately protect information and OI&T assets. Mechanisms include fire detection systems, a portable fire extinguisher placed at each end of the room, smoke detectors, automatic sprinkler systems, fire fighting equipment, regular maintenance of fire extinguishing equipment, and training of personnel in fire safety procedures and use of fire extinguishers. Fire suppression and detection devices/systems activate automatically in the event of a fire and provide automatic notification of any activation to the facility and emergency responders.

b. Electrical Outages: Engineering, or its equivalent, ensures that appropriate steps are taken to assure that the quality and reliability of electric power is satisfactory for the facility. All electrical maintenance work is coordinated with OI&T management to avoid inadvertent shut-off of computer room, environmental systems, or communications power. All electrical power distribution equipment is adequately protected physically against accidental damage or sabotage, and access to electrical equipment rooms or closets is controlled. The facility provides a short-term uninterruptible power supply to facilitate an orderly shutdown of the information system in the event of a primary power source loss and a long term alternate power supply that is capable of maintaining minimally required operational capability in the event of an extended loss of the primary power source.

c. Emergency Shutoff: The facility has provided the capability in the OI&T area of shutting off power to any information system that may be malfunctioning (e.g., due to an electrical fire) or threatened (e.g., due to a water leak) without endangering personnel by requiring them to approach the equipment.

d. Emergency Lighting: The facility maintains automatic lighting systems that activate in the event of a power outage or disruption and that cover emergency exits and evacuation routes.

e. Environmental Monitoring: To control the temperature and humidity, and detect the presence of water in the computer room, appropriate recording equipment is installed and monitored. The OI&T Chief/CIO is responsible for providing temperature and humidity ranges that are compatible with computer equipment specifications. Water sensors are utilized to ensure detection and immediate notification to appropriate staff. Master shutoff valves are accessible, working properly, and their location known to key personnel.

(5) Contingency Planning

(a) **Policy:** VA requires that Operating Units develop and implement a contingency plan for their information systems addressing contingency roles, responsibilities, assigned individuals with contact information, and activities associated with restoring the system after a disruption or failure.

(1) Designated officials within the organization will review and approve the contingency plan and distribute copies of the plan to key contingency personnel.

(2) Operating Units will train personnel in their contingency roles and provide refresher training annually.

(3) Operating Units will review and test their contingency plans annually.

(4) Operating Units will identify their alternate storage and processing sites.

(5) Operating Units must identify primary and alternate telecommunications services.

(6) Operating Units must conduct backups of user-level and system-level information.

(7) Operating Units must employ mechanisms to recover and reconstitute systems to their original state after a disruption or failure.

(b) **Procedure:** VA has developed the following levels of contingency planning to restore normal operations in the event of a service disruption to the facility or system.

(1) Disaster Recovery Plan:

(a) This plan is the overall facility contingency plan and is coordinated with the site's emergency management staff and approved by the facility director or program manager. This plan defines the overall contingency objectives and establishes the framework, roles, and responsibilities. The plan will address the scope (to include remote sites), resource requirements, processing priorities, training, testing, plan maintenance, and backup requirements. Activities involved in this function include conducting an impact analysis, identifying preventive measures, developing a recovery strategy, documenting the disaster plan, distributing the plan to appropriate individuals, training the staff, and testing the plan.

(b) The Operating Unit must have an alternate processing site policy that defines the site's policy and procedures. The alternate processing site is geographically separated from the primary processing site so as not to be susceptible to the same hazards. The alternate processing site is fully configured to support a minimum required operational capability and is ready to be used as the operational site. The Operating Unit has identified potential accessibility problems to the alternate processing site in the event of an area-wide disruption or disaster and has addressed these issues in the disaster recovery plan. This arrangement is documented, reviewed, and approved annually by the Operating Unit to ensure the plan is still appropriate and that the required resources are available.

(c) The contingency plan must identify the activities that are necessary to execute temporary information system processing capabilities, repair damage to the original system, and restore operational capabilities at the original or new facility. The recovery strategies must include the sequence of activities as well as detailed procedures for the technical recovery of operations until the system can be reconstituted. The information system contingency plan also documents the following resources required for supporting critical functions: computer hardware and software; computer supplies; system documentation; telecommunications; office facilities and supplies; and human resources.

(2) Emergency Mode Operation Plans

(a) Service Contingency Plans: Written contingency plans must be maintained for each service and should include a means by which routine business operations may continue when computer system capabilities have been eliminated or diminished. Contingency plans should also include procedures for information recovery when the computer systems come back on line. Contingency plans will be consolidated for each facility to respond to contingencies as necessary for their information systems. These plans will be part of the overall facility Disaster Plan. OI&T staff is responsible for the preparation and accuracy of contingency plans. OI&T management is responsible for prioritizing the critical functions and documenting plans for contingency/recovery of information systems in the event of scheduled or unscheduled downtime. Managers are responsible for the development of their specific components of the contingency plan and ensuring that employees under their management receive annual training on their specific roles and responsibilities. When applicable, simulated events and automated mechanisms are used to train individuals regarding their specific roles and responsibilities.

(b) Any changes to the plan must be fully documented and members of the contingency planning teams notified of the relevant changes. Each update of the contingency plan will require concurrence of the facility director/program manager or designee, and distribution to the appropriate individuals. Distribution of the plan will be limited to authorized individuals, and a complete copy of the plan will be stored at an off-site location.

(c) System Specific Contingency Plans: These plans will outline procedures specific to each system within the facility [to include hardware, operating system, third party utilities, and related software, databases, application software, LAN at the data center, Wide Area Network (WAN), and remote LAN] and will also include information such as procedures for shutting down and restoring a system during an emergency, contacts and vendors, and responsibilities during an emergency. The system administrator is responsible for preparing the contingency plan for the system. Distribution of the plan will be limited to authorized individuals and a copy of the plan will be stored with OI&T Chief/CIO and at an off-site location. Contingency plans are re-evaluated prior to a significant change in the system, but are reviewed at least annually. The plan should be revised to address system/organizational changes or problems encountered during plan implementation, execution or testing. Systems which may pose a high risk and potential magnitude of harm will be re-evaluated more often. Each plan will be documented as part of the certification and accreditation of the system.

(3) Electronic Media Backups:

(a) Information Back-up and Storage: OI&T Chief/CIO is responsible for establishing, maintaining, and executing written procedures for backup and restoration of production systems. Critical information files and operations will be identified and the frequency (daily, weekly, and monthly) and scope (full backup, incremental, and differential) of file backup are documented. All system security configurations will be documented and backed-up. The backups shall be completed on a prescribed basis and rotated off-site often enough to avoid disruption if current files are damaged. The location of the stored backups is documented. Backups shall also be verified periodically to ensure that they are complete and contain valid information by using system specific restore functions. Each site selectively uses backup information in the restoration system functions as part of contingency plan testing. Backups should be encrypted whenever possible.

(b) Off-Site Storage: Each site will identify and initiate a MOU for storage of the site's backup information when using another site within VA. For commercial entities, a contract is required. Backups are to be stored in a secured location away from the facility in order to avoid loss in the event of an accident or malicious incident. The information will be labeled, packed and transported to the off-site storage facility securely. A local risk assessment shall be completed to determine if the selected site is sufficiently distant from the facility to reduce the risk of the storage location being affected by the same disaster. The priority with which the facility can obtain its back-ups in the event of a catastrophic emergency will be considered. The storage facility will have controlled access, proper environmental controls, and reinforced concrete or steel beam construction that has been earthquake proofed. Access control to the VA information stored at this location will be stringently controlled and periodically tested. Locks and personnel will be used to control the off-site storage to prevent unauthorized access. System and application documentation and an up-to-date hard copy of the contingency plans are also stored securely at this off-site location.

(4) Contingency Plan Testing:

(a) To ensure the accuracy and reliability of contingency plans, IT managers and supervisors will conduct tests on the components of the plan for which they are responsible, and will update the components based on evaluation of the results. Tests will have a specific objective such as: determining the availability of needed back-up files, the validity/functionality of the back-up files, implementation of fire and evacuation procedures, and implementation of manual procedures. The tests will also provide an opportunity for training of key personnel in the proper procedures to be followed in the event of an emergency. Contingency plan testing will be documented and test results reported to the ISO. When applicable, the Operating Unit employs automated mechanisms to thoroughly and effectively test the contingency plan. When feasible, a full recovery and reconstitution of the information systems is used as part of the contingency plan testing.

(b) Alternate Processing Site: The alternate processing site will be geographically separated from the primary processing site so as not to be susceptible to the same hazards. The alternate processing site will be fully configured to support a minimum required operational capability and is ready to be used as the operational site. The Operating Unit will identify potential accessibility problems to the alternate processing site in the event of an area-wide disruption or disaster and will address these issues in the disaster recovery plan. This arrangement is documented, reviewed, and approved annually to ensure the plan is still appropriate and that the required resources are available. The agreement (MOU or contract) with the alternate site shall contain priority-of-service provisions. Security requirements for the alternate site should be the same as the production site.

(c) Telecommunications Services: The Operating Unit will identify primary and alternate telecommunications services to support the information system and will initiate necessary agreements to permit the resumption of system operations as soon as possible. The primary and alternate telecommunications service agreements shall contain priority-of-service provisions. The alternate telecommunications services will not share a single point of failure with the primary telecommunications services and the providers will be sufficiently separated from the primary service providers so as not to be susceptible to the same hazards. Both the primary and alternate telecommunications service providers must have adequate contingency plans.

(6) IT System Hardware and Software Maintenance

(a) **Policy:** VA requires that Operating Units develop, document, and maintain a current baseline physical and logical configurations of their information systems and an inventory of the system's constituent components. The security settings should be configured to the most restrictive mode consistent with operational requirements, documented, and enforced.

1. VA requires that Operating Units document and control changes to their systems. These changes shall be monitored and security impact analyses be completed to determine the effects of the changes. Access restrictions associated with changes must be enforced.

2. Operating Units shall schedule, perform, and document routine preventative and regular maintenance on the components of their information systems in accordance with manufacturer or vendor specifications.

3. Operating Units shall approve, control, and monitor remotely executed maintenance and diagnostic activities.

4. Operating Units shall maintain a list of VA personnel and vendors authorized to perform maintenance on their information systems.

(b) **Procedure:**

1. Configuration Management:

(a) Each Operating Unit utilizes the VA established guides and policies for the proper configuration, setup, and operation of servers, applications, and desktops. The security settings established by the configurations should be as restrictive as possible. Each site reviews their information systems periodically to identify and eliminate unnecessary functions, ports, protocols, and/or services. This process is defined and monitored via a configuration management plan. Vendor-supplied default security parameters must be changed to conform to the VA standards. The ISO will coordinate with system owners and system managers to identify and implement approved VA policies and guidelines necessary to ensure the compliance of approved configurations for the systems within the facility. System configurations (including links to other systems) will be documented and updated accordingly with any major changes in the system's security plan. The production configuration must be backed-up on a schedule specified by OI&T.

(b) Each site maintains an inventory of the systems' constituent components. The inventory of the information system components includes manufacturer, type, serial number, version number, and location (i.e., physical location and logical position within the information system architecture). Each Operating Unit updates the baseline configuration as an integral part of information system component installations and employs automated mechanism to maintain an up-to-date, complete, accurate, and readily available baseline configuration items.

2. Change Controls:

(a) OI&T Chief/CIO, the ISO, and other specified individuals as needed, comprise the Change Control Board. The Board ensures that changes are documented and tested. The Board monitors changes to the information system and ensures security impact analyses are completed to determine the effects of the changes. If the facility environment necessitates a

different configuration for a particular system than the configuration approved by VA, the change request must be documented and evaluated by the Change Control Board. If the proposed change affects the security of the system, the system must be re-certified and accredited by OCS.

(b) All changes to the configuration of a system will be documented in the system's security plan and Continuity of Operations plan, if applicable. The system owners, system managers, and the ISO will review all VA-NSOC security alerts and take appropriate remedial actions in a timely manner. The Board ensures that access restrictions associated with changes to the system are implemented and monitored. Emergency change procedures are documented and approved by management either prior to the change or immediately after the fact. Each Operating Unit audits activities associated with configuration changes to the information systems.

3. Hardware Maintenance:

(a) OI&T schedules, performs, and documents routine preventative and regular maintenance on the components of their information systems in accordance with manufacturer or vendor specifications.

(b) OI&T Chief/CIO approves the removal of the information systems or information system components from the facility when repairs are necessary. If off-site repair is required, the facility removes all information from associated media using approved procedures. After maintenance is performed on the information system, the facility checks the security features to ensure that they are still functioning properly.

(c) OI&T maintains a maintenance log for their information systems that includes the date and time of maintenance; name of the individual performing the maintenance; name of escort, if necessary; a description of the maintenance performed; and a list of equipment removed or replaced (including identification numbers, if applicable).

(d) Each Operating Unit employs automated mechanisms to ensure that periodic maintenance is scheduled and conducted as required, and that a log of maintenance actions, both needed and completed, is up to date, accurate, complete, and available.

(e) OI&T Chief/CIO approves, controls, and monitors the use of information system maintenance tools and maintains the tools on an ongoing basis. OI&T inspects all maintenance tools (e.g., diagnostic and test equipment) carried into a facility by maintenance personnel for obvious improper modifications. OI&T also checks all media containing diagnostic test programs (e.g., software or firmware used for system maintenance or diagnostics) for malicious code before the media are used in the information system.

(f) OI&T checks all maintenance equipment with the capability of retaining information to ensure that no VA information is written on the equipment or the equipment is appropriately sanitized before release; if the equipment cannot be sanitized, the equipment remains within the facility or is destroyed, unless an appropriate VA official explicitly authorizes an exception.

(g) OI&T Chief/CIO approves, controls, monitors remotely executed maintenance and diagnostic activities and assures that the use of remote diagnostic tools is described in the security plans for the systems. OI&T maintains maintenance logs for all remote maintenance,

diagnostic, and service activities and periodically reviews these logs. In addition, for systems categorized as high, the following controls are also required:

(1) OI&T audits all remote maintenance sessions and reviews the audit logs of the remote sessions.

(2) OI&T addresses the installation and use of remote diagnostic links in the security plan for the information system.

(3) Remote diagnostic or maintenance services are acceptable if performed by a service or organization that implements for its own information system the same level of security as that implemented on the information system being serviced.

b Biomedical Engineering, for medical equipment, and OI&T staff for other IT equipment maintain a list of personnel or the vendor (maintenance company) authorized to perform maintenance on their systems. Only authorized personnel perform maintenance on the information systems. Maintenance personnel have appropriate access authorizations to the information systems when maintenance activities allow access to sensitive information. When maintenance personnel do not have needed access authorizations, local staff must supervise maintenance personnel during the performance of maintenance activities on the information systems.

c Each site obtains maintenance support and spare parts based on service level agreements or contracts.

4. [VHA VistA] Processing Environments:

a. Production: This is the environment for the processing of official information utilized in the provision of health services to the veteran in support of the facility-wide mission. The system manager is responsible for production system maintenance and the implementation of mechanisms that address the protection of VA sensitive information and the processing system, ensuring access controls defined in this policy are in place. The ISO will perform routine monitoring of the production system ensuring adherence to set procedures.

b. Development and Verification: This is the environment for development, testing and verification of program code for the maintenance, modification or enhancement of existing applications, or the development of new applications. The development account is maintained by OI&T. User access to this account will be granted upon approval by OI&T. Minimum necessary access controls will be applied in granting these accounts. The distribution and implementation of new or revised software is documented and reviewed. Version control is utilized and all software programs are labeled and inventoried.

c. Test system: This may be an environment used for testing new software applications and revisions. OI&T is responsible for maintaining the test system. This includes the installation of software packages and necessary patches as they are released and mandated. OI&T is also responsible for managing test system user accounts. Existing users may receive access to the test system OI&T staff sponsoring the user. OI&T will ensure that test account access is appropriate for the user and that it does not allow them access that can compromise the integrity of the test system or compromise the 'mirroring' capability as the mirror of the production system.

(7) Information Integrity

(a) **Policy:** VA must identify, report, and correct information system flaws. VA sensitive information must be protected from improper alteration or destruction.

1. Local modification of the [VistA Kernel] software security features is strictly prohibited. Additionally, Health Information Management (VHA only) plays a role in maintaining the content, accuracy, and completeness of VA sensitive information and tracking historical changes to the health record.

2. VA requires that malicious code protection is utilized and automatically updated on its systems, when applicable. If applicable to the system, spam and spy ware protection is required.

3. VA requires the implementation of tools and techniques to monitor events, detect attacks, and provide identification of unauthorized use of the systems.

4. VA requires that Operating Units receive and take appropriate action on information system security alerts/advisories.

5. Information input shall be restricted to authorized personnel only.

(b) **Procedure:** The OI&T Chief/CIO is responsible for maintaining overall integrity for all IT systems within their facility. A record of modifications to existing commercial or locally-developed software will be maintained. The OI&T Chief/CIO reviews each system installation of facility-developed new or modified software and restricts and controls access to all program libraries.

1. Each site enforces access restrictions associated with changes to the information system. Willful and intentional modification of VA software processing fiduciary information (e.g., IFCAP, PAID) for illegal or disruptive purposes or for purposes of personal gain is a felony. There shall be no local modifications of fiduciary programs without the approval of the issuing CIO field office. The OI&T Chief/CIO or designee(s) shall ensure that programs processing fiduciary information have not been modified both prior to receipt and at least annually after they have been placed into production.

2. Any local modifications to VA software must be reviewed, tested, approved, and documented by OI&T Chief/CIO and the ISO. The site will be required to re-certify and accredit the software prior to going into production, if any local modifications to the VA software have the potential to affect the security of the software.

3. Each site protects the integrity of information and information systems through antivirus programs and intrusion detection software. The anti-virus solution is managed both locally and centrally and systems automatically update. Users will not take any action that invites or allows a computer virus to be introduced into any VA computer system. To reduce the risk of viruses, the following procedures will be followed:

4. Authorized and current anti-virus software will be used and enabled at all times. OI&T is authorized to disconnect, either physically or logically, any device that is not protected with current anti-virus software.

5. All new software shall be tested on an isolated computer to avoid damage if a virus is present.

6. Downloaded software from the Internet will be scanned for viruses.

7. Executables must not be launched without first having the origin validated by the sender and verified to be free of viruses.

8. All MOUs, contracts, statements of work, and data use agreements will define the party responsible for the expense of antivirus software for non-VA equipment.

9. Users will be given training which covers the risks that viruses pose to OI&T assets, common ways that viruses are introduced, how to prevent viruses, and how to detect them, warning signs of the most common viruses, and what to do if a virus is detected or suspected (who to call, when to call).

10. Malicious code infection handling includes:

a. Stop using any computer or software suspected of malicious infection or malfunction;

b. Remove the computer from VA's network;

c. Do not reboot (restart) the system, as many viruses are triggered to propagate upon system reboot which can cause further damage;

d. If it appears that a negative activity is occurring (such as deletion of files) then the system must be shut off and left off until clean anti-virus boot media is used to clean the system;

e. VA employees, contractors, subcontractors, and volunteers not authorized to attempt recovery and restoration must not remove the suspected software themselves, but must contact a qualified OI&T staff via their respective help desks to request recovery;

f. Never surrender or swap hard drives or other storage devices to anyone other than an OI&T employee if storing VA sensitive information on the drive at the time of system problem.

11. Each site employs tools and techniques to monitor events on the information systems, detect attacks, and provide identification of unauthorized use of the system. Intrusion detection tools are used to identify unauthorized attempts to probe a system, especially attempts to gain unauthorized access. The OI&T staff and the ISO will work with the VA NSOC to monitor VA's network.

12. The OI&T Chief/CIO is responsible for ensuring that adequate software security measures are implemented to verify the access authority of individuals and to protect files from unauthorized or accidental modification, destruction, or disclosure. Local managers or designees are responsible for monitoring compliance with, and ensuring that all employees are following, IT security policies.

13. Each site receives information system security alerts/advisories on a regular basis and takes appropriate actions.

(8) Penetration Testing and Vulnerability Scanning

(a) **Policy:** Penetration testing and vulnerability scanning will be used to assess the strength of security controls of the systems. Vulnerabilities discovered from scans and penetration testing will be reviewed and corrective actions taken by the system owners, system managers, and OI&T personnel. Each Operating Unit performs vulnerability scans at least monthly or when significant new vulnerabilities affecting the system are identified and reported.

(b) **Procedure:** OI&T and the ISO should be trained in the use and maintenance of vulnerability scanning tools and techniques. The information obtained from the vulnerability scanning process is freely shared with appropriate personnel throughout the facility to help eliminate similar vulnerabilities in other information systems. However, vulnerability scans are considered to be VA sensitive information and should be distributed, maintained and disposed of appropriately.

1. Vulnerability scanning tools include the capability to readily update the list of vulnerabilities scanned. Each facility will update the list of information system vulnerabilities as required or when significant new vulnerabilities are identified and reported. This process may be conducted independently or as a coordinated effort with the VA NSOC.

2. System owners, system managers, and other OI&T personnel will periodically review their systems to identify and, when possible, eliminate unnecessary services (e.g., FTP, HTTP, IIS).

(9) Information System Hardware and Electronic Media Sanitization and Disposal

(a) **Policy:** VA's electronic media sanitization procedures for electronic media are to be followed. These procedures ensure that electronic media are appropriately sanitized or destroyed; the action has been documented; and all VA sensitive information is protected to prevent subsequent disclosure when OI&T equipment containing VA sensitive information is surplused, donated, or otherwise removed from VA control.

(b) **Procedure:** The facility will ensure that sanitization of VA sensitive information from equipment is accomplished before the equipment is released from custody for disposal. This sanitization process must cause the removal of all VA sensitive information from information systems storage devices and render the information from these systems unreadable. The OI&T Chief/CIO will be responsible for identifying and training OI&T staff on VA media sanitization policy and procedures. The ISO will coordinate and audit this process and document the audit on an annual basis to ensure compliance with national media sanitization policy.

(10) Incident Response Capability

(a) **Policy:** The Operating Unit complies with the VA OI&T incident reporting procedures for all incidents. All incidents related to information security shall be reported immediately to the ISO.

1. Security and privacy incidents will be tracked and documented by the ISO and the Privacy Officer (PO) using the VA approved tools.

2. Personnel will be provided training by OI&T in their incident response roles and will receive refresher training annually.

3. The incident response capability will be tested at least annually using tests and exercises to determine the incident response effectiveness. The testing will be documented.

(b) **Procedure:** Users will immediately report any incident of theft, loss, or compromise of VA sensitive information or information systems to the ISO and/or PO and supervisor. Note: If any VA staff member witnesses a case of egregious waste of government resources or outright fraud, they must comply with 38 C.F.R. §1.201 and §1.204 and directly contact the OIG Hotline.

1. The ISO and PO will work with management and, if a compromise occurred, members of the appointed investigative team will examine the details surrounding the incident ensuring information and systems are not compromised. The ISO and or PO will contact, either automatically via electronic mail and/or via phone, the VA-NSOC within an hour to coordinate a response to the incident and to limit the damage. If the incident is believed to involve criminal activity, the ISO and/or PO will contact the local VA Police and the OIG. The VA-NSOC staff will file a report with the VA OIG Hotline. The VA-NSOC offers advice and assistance regarding handling and reporting of security incidents. This support resource is an integral part of the VA's incident response capability.

2. VA-NSOC may also alert the Operating Unit of suspicious or malicious activity when such activity has been detected. The ISO will resolve the matter according to VA's OI&T's policy and local procedures, as appropriate.

3. The VA NSOC will provide the technical guidance, advise vendors to address product/software related issues, and provide liaisons to legal and criminal investigative groups as needed. The VA NSOC will also ensure that, if appropriate, the related information will be shared with owners of interconnected systems, US CERT, and other local law enforcement.

4. Each Operating Unit will also:

a Train personnel in their incident response roles and responsibilities in respect to information security and provide annual refresher training. The training incorporates simulated events to facilitate effective response by personnel in crisis situations, and employs automated mechanisms, when applicable, to provide a more thorough and realistic training environment.

b Test the incident response capability for their information systems annually, using facility defined tests and exercises to determine the incident response effectiveness. All tests are documented and automated mechanisms are used when appropriate. The ISO and PO tracks and documents information system security and privacy incidents on an ongoing basis.

(11) Security Training, Education, and Awareness

(a) **Policy:** VA Directive 6500 requires mandatory periodic training in computer security awareness and accepted computer security practices for all VA employees, contractors, and all other users of VA sensitive information and VA information systems. All members of the workforce are required to complete computer security training annually and must complete computer security awareness training before they can be authorized to access any VA computer system. Each site identifies personnel with significant information system security

roles and responsibilities (i.e., management, system managers, system administrators, contracting staff, HR staff), documents those roles and responsibilities, and provides appropriate additional information system security training. Security training records will be monitored and maintained.

(b) **Procedure:** Orientation training will be conducted for all new employees in accordance with the New Employee Orientation program. For those individuals who cannot immediately attend new employee orientation, the service will provide basic security awareness training. At minimum, the following computer security awareness basics will be addressed prior to system access and during the orientation training:

1. Knowing the ISO;

2. Creating strong passwords and protecting them;

3. Maintaining confidentiality of information;

4. Complying with the Privacy Act;

5. Backing up information;

6. Using e-mail properly and securely;

7. Using “reply to all” in a manner that will not create a denial of service;

8. Identifying and reporting computer security related incidents;

9. Recognizing VA Cyber Security as part of the nation’s infrastructure protection;

10. Recognizing social engineering and defending against it;

11. Understanding authorized, limited personal use of government equipment and computer resources;

12. Understanding the HIPAA Privacy and Security Rules and the penalties for non-compliance;

13. Understanding proper disposal techniques for information on computers and portable media; and

14. Understanding proper workstation use and security.

(c) The workforce will receive security awareness training annually as part of the Mandatory Training Program.

(d) All computer security awareness training shall be documented in the training package. The ISO will monitor both the basic security awareness training and the role based system security training at their facility and will have access to the training information.

c. Technical Controls

(1) Identification and Authentication

(a) **Policy:** VA system controls must uniquely identify users (or processes acting on behalf of users) to the system. Each user ID will be associated with a unique password to authenticate the individual/entity.

(b) **Procedure:** User access will be controlled and limited based on positive user identification. Authentication mechanisms support the minimum requirements of access control, least privilege, and system integrity for all platforms.

1. The following are the VA's information system account and password management procedures:

a. Access Codes and User IDs:

b. The assignment of access codes and user IDs will follow VA naming conventions per *Appendix F* of VA Directive 6500 Handbook.

3. Electronic Signature Codes: Electronic signature codes shall be treated as VA sensitive information requiring the same level of protection as individual access and verify codes.

4. Multiple Sign-on Restriction: High impact systems should limit the number of concurrent sessions for general users to one session, and three sessions for privileged users. Requests for multiple sign-on, are handled on a case by case basis, and should include justification and concurrence by designated ISO and the CIO with the exception of users that require multiple sign-on to use the GUI and other software packages simultaneously. Exceptions should be documented in the system security plan.

5. Timed Read: The maximum time allowed shall be set to 900 seconds for users to prevent unauthorized access to unattended workstations with the exception of some clinical staff. Providers may receive timed read up to 1200 seconds for ease of use in clinical settings based on Clinical Application Coordinator (CAC) recommendations. Requests for increased timed read should be handled on a case-by-case basis, require justification, approved by the OI&T Chief/CIO and should be submitted to the designated ISO for concurrence.

6. Remote authentication: Remote access requires two-factor authentication where one of the factors is provided by a device separate from the computer gaining access.

7. Screen savers: Password protected screen savers are enabled for use as appropriate. The password protected screen savers are configured to activate after fifteen minutes or less of inactivity. Only VA-approved screen savers will be used.

8. Session Lock: Information systems prevent further access to systems by initiating a session lock that remains in effect until the user reestablishes access using appropriate identification and authentication procedures. Users can directly initiate session lock mechanisms. A session lock is not a substitute for logging out of the information system.

9. Programmer Mode Logs: For users that have been granted the Programmer Mode option and the associated security keys, a programmer access code (PAC) shall be assigned

for additional security. The Kernel (VHA) will prompt for the PAC just before allowing the user to enter programmer mode. Programmer mode access will be approved by the OI&T Chief/CIO and audited by the ISO.

10. File Access Security: OI&T is responsible for granting file access. The supervisor and/or application coordinator will determine the needs of each user and the appropriate degree of access authority to be assigned.

11. Access scripts with embedded passwords are prohibited.

12. Vendor supplied passwords are replaced immediately.

13. The OI&T Chief/CIO and the ISO must approve specific user actions that can be performed on the information systems without appropriate identification and authentication (i.e., service accounts, site-to-site VPN accounts, training accounts in test system).

14. When possible, the information system provides feedback to a user during an attempted authentication and that feedback does not compromise the authentication mechanism.

15. As appropriate and indicated, the information system identifies and authenticates specific devices before establishing a connection (i.e., site-to-site VPNs, wireless)

16. As appropriate, the information system employs authentication methods that meet the requirements of FIPS 140-2.

(2) Logical Access Controls

(a) **Policy:** Logical access controls are employed to permit only authorized access to VA computer systems and restrict users to authorized transactions, functions, and information. These automated controls ensure that only authorized individuals gain access to information system resources, that these individuals are assigned an appropriate level of privilege, and that they are individually accountable for their actions. These controls support the separation of duties principle. Every user account is reviewed by management and security staff based on system impact levels as defined in Appendices D and E, and provide the findings to the CIO to ensure appropriate separation of duties and to ensure that the most restrictive set of rights/privileges or access needed by users is in place. Refer to Section 5.0 Audits and Reviews for Access Control Audits conducted.

(b) Procedure:

1. Access Permissions:

a. OI&T Chief/CIO will maintain a current list of approved and authorized users and their access.

b. The OI&T Chief/CIO or designee will process all requests for access in accordance with the operating unit's access procedures.

c. System users will be prompted by the system to enter a new verify code and password every 90 days.

d. Accounts are automatically disabled if inactive for 30 days.

e. Application menus shall be created to permit the user to perform all duties required of his/her position and permit access to information for which the user has a need to know. The supervisor and application coordinator responsible for the user will determine the appropriate menus. Responsibility and authorization for the creation or modification of application menus will be under the control of the OI&T Chief/CIO or designee.

f. To ensure accountability, use of individual access codes and passwords are mandatory for all VA information systems. Only the individual to whom the codes were assigned will use their assigned codes. Guest accounts are not allowed on VA information systems, as this type of account exposes information systems to risk by allowing access through the use of a generic logon ID that requires no password or uses a widely known password. The use of shared and generic accounts on VA information systems is prohibited. In the event of lost or compromised password, the individual will notify the ISO or IT Chief/CIO or designee, who will take appropriate measures.

g. Attaching codes to equipment or furniture in work areas to avoid memorizing them is strictly prohibited. All codes allowing access to information systems are considered sensitive information and must be treated as such.

h. Access to system security files, system management/configuration files, and creation of shared drives or other protected files is limited to OI&T staff that requires this access in order to perform their duties. Users with programmer access, system manager or network administrator capabilities, which allow unrestricted access, shall not misuse access capabilities to view or modify anyone else’s files and/or mail messages.

i. Staffs who administer access control functions should not administer audit functions.

j. The OI&T Chief/CIO or designee shall generate security codes for newly authorized facility users and when appropriate, existing authorized users, and provide the codes in a secure manner to the user. If an existing user has difficulty accessing the system, OI&T will reset and allow the user to issue their own verify code or password after the user has been positively identified. Identification is required at the time a user receives password information.

k. The ISO will review all requests for all VA systems access by users. The request shall state the individual's name, last four digits of SSN, telephone number, facility, and purpose for access, and shall have the concurrence of a higher level official within the requestor's facility or Operating Unit. Distribution of security codes for authorized non-facility users will be handled in the same manner as with local users.

l. Requests for access to remote systems must be approved by the user's supervisor and submitted to the ISO for processing.

m. In the event of an emergency, emergency access to VA sensitive information will be granted in accordance with contingency procedures. These accounts will be terminated immediately upon conclusion of the emergency situation.

n. In the event that temporary access is required (i.e. OIG/JCAHO) access will be provided and an automatic termination date established to ensure the account is terminated appropriately.

o. System managers and others with special system level access privileges are expressly prohibited from reviewing or accessing individual accounts or personal computers unless specifically authorized in writing or email by appropriate senior management officials and the ISO.

p. In the event of non-routine circumstances in which the employee possesses VA sensitive information and is not available, management officials may review an account or personal computer as part of their supervisory responsibilities. The following procedures have been established for obtaining such access:

(1) Submit a request for access to a user's account or personal computer to the ISO and include, at a minimum, the following information: first and last name of user; username (account name); justification for access; location of files; location to save the files to (i.e. supervisor's drive or CD); duration of review.

(2) Upon approval from the designated supervisor/manager, the ISO will coordinate requested access with the OI&T Chief/CIO. The ISO will not be the recipient of user's individual files from a facility storage device.

(3) Audit logging for all activities related to this emergency access request is required and must be protected and saved.

(4) Emergency access must specify the person authorized to access the account. Under no circumstance will the unavailable individual's logon ID or password be used or compromised during emergency access.

(5) The system administrator will rewrite the access rules to give the manager or designee access to the information (files).

(6) Upon completion of the emergency access, all access to the information will be returned to the original state.

(7) It is the responsibility of the user's supervisor/manager or designee to notify the unavailable individual of the emergency access as soon as he or she becomes available.

(3) Remote Access

(a) **Policy:** VA sensitive information may not be transmitted via Internet or VA's internal network (Intranet) without proper security mechanisms that meet NIST FIPS 140-2 criteria. VA has chosen Public Key Infrastructure (PKI) as the current solution for transmission of sensitive information for Outlook Exchange. ISOs are responsible for ensuring that users who have a need for VA PKI receive appropriate training and support. ISOs coordinate requests for VA PKI certificates with the Local Registration Authority (LRA). ISOs may be required to perform Identity Proofing Procedures to securely and confidentially distribute VA PKI enrollment information to participants.

(b) Each operating unit must document, monitor, and control remote access to the information systems, including remote access for privileged functions.

(c) VA employees, contractors, subcontractors and volunteers may transport, transmit, access, and use VA sensitive information outside of VA facilities only when their VA supervisor authorizes such action in writing.

(d) Use of or access to VA sensitive information may be revoked, modified, or limited at any time by that person's VA supervisor or a superior of that supervisor.

(e) All memoranda of understanding, contracts, statements of work, and data use agreements will include assertions that all parties will conform to these remote use policies and procedures.

(f) Users will not simultaneously connect to VA and one or more non-VA networks.

(g) Only VA personnel may access VA-owned equipment used to process VA information or access VA processing services. Users may not share with non-VA employees or unauthorized personnel instruction or information regarding how to establish connections with VA private networks and computers. Users may not share remote access logon IDs, passwords, and other authentication means used specifically to protect VA information or access techniques to VA private networks.

(h) Remote Access is allowed and controlled through the National One VA VPN. The National One VA VPN controls all remote accesses through a managed access control point. All requests for One VA VPN accounts must be approved by the immediate supervisor, the IT Chief/CIO and the ISO. The National One VA VPN uses a "time-out" function that requires re-authentication after 30 minutes inactivity.

(i) In recognition of its responsibility to secure and safeguard information from misuse or improper disclosure, all remote access service computer users must provide proper justification of the need for access, and sign Rules of Behavior prior to remote access being granted. Approved remote access users can access VA systems from their residence or while they are on travel status using approved government furnished equipment (GFE). If non-VA owned equipment must be used in certain circumstances, a waiver must be in place. All of the security controls required for GFE must be utilized in approved non-VA owned equipment and must be funded by the owner of the equipment. Approved remote access users are governed under the same local policies, federal laws and regulations that apply to all local users of VA computer systems and the security and privacy of the information contained therein.

(j) Responsibility for access to, or training on, systems not covered by this policy lies solely with the individual or service/section requiring this access. Remote access to VA computer systems does not constitute approval for overtime pay or compensatory time.

(k) OI&T staff is responsible for ensuring that the requestor receives instructions on how to setup the PC or laptop for the required access and for providing any needed assistance. If the remote access user needs assistance with configuring this access or to determine hardware compatibility, they should follow their local Helpdesk procedures.

(l) Remote (Off-site) Users: Requests for access by remote users will be submitted in writing to the ISO including the user's name, service, phone number, mail code, the last four

digits of the social security number, and purpose for access, and will have the concurrence of a higher level official within the user's facility. The appropriate documentation will be coordinated with the remote facility ISO and forwarded to the ISO. Codes for authorized remote users will be delivered either electronically using PKI or in a sealed envelope to the remote facility's ISO. The outside of the envelope will be annotated with the user's name and the statement, 'TO BE OPENED BY ADDRESSEE ONLY". Users should contact their ISO if the envelope is not sealed when delivered.

(m) If a remote access account request is disapproved, the requester and his/her service chief will be notified and an explanation for disapproval will be provided. The request may be resubmitted if the requester's requirement for remote access changes.

(n) New users (those who do not have a current VA Network account) who request remote access must complete privacy and information security awareness training, and complete the authorization for information system access before any access can be granted.

(o) Contractors: Requests for access by contractors will be submitted in writing to the ISO and the CO or the COTR to include the user's name, service, phone number, mail code, the last four digits of the social security number, and purpose for access. All contractors are required to follow the same policy and procedures and will have the concurrence of a higher level official within the facility. The appropriate documentation will be coordinated with the contractor by the CO / COTR and ISO. Codes for authorized remote users will be delivered either electronically by PKI or in a sealed envelope to the ISO or to the CO or COTR for distribution to the contractor. Vendors may have a Site-to-Site VPN connection to VA's network. Requirements for access for a Site-to-Site VPN connection can be found on the VA Information Assurance Portal.

(p) Transferring, Retiring, Resigning, Removed or Discharged Employee: Supervisors will contact the ISO to ensure that remote access privileges are terminated as soon as they are no longer needed, when the account owner transfers out of the supervisor's office or leaves the VA, or when an authorized official determines that remote access privileges should be revoked. Upon termination of required access privileges, supervisors will confirm and notify the ISO and the individual responsible for the equipment inventory listing that the employee has returned all GFE related to remote access.

(q) ISOs ensure that remote access privileges are terminated promptly when they are no longer required. If a remote access account is not used for a period of ninety (90) days, the ISO will disable the account. If a remote access account remains unused after six months, the ISO will remove the account. ISOs will terminate the VPN accounts by using the VA NSOC approved VPN Administrative Software.

(r) ISOs are responsible for auditing remote access authorizations and ensuring remote access users know how to use the remote access connection securely.

(s) Modems may not be installed on workstations and systems connected to the VA network. If a dial-in connection is considered essential to a program mission, the facility must complete and have on file a waiver request form and obtain approval from OI&T. If approved, security controls and procedures will be documented in the security documentation for the affected system and maintained for future information security audits and inspections. Stand-alone systems not connected to the VA network must develop and document a procedure for remote diagnostics and maintenance of equipment that is tightly controlled. Event logging

functions are to be provided to enable the review of suspicious activity. Only remote control software configured and approved by OI&T and the OI&TChief/CIO may be used to control VA systems via the LAN, WAN, or remote access.

(4) Mobile/Portable/Wireless and Removable Storage Media and Device Security

(a) **Policy:** All VA employees, contractors, business partners, and any person who has access to and stores VA sensitive information must have permission from a supervisor and ISO to use removable storage media/devices to store sensitive information.

(b) In order to ensure the protection of sensitive information, all removable storage devices that connect to VA's resources via USB ports (i.e. thumb drives, MP3 Players – iPods, Zunes, and external hard drives) must be encrypted with FIPS 140-2 certified encryption. Similarly storage media such as CDs/DVDs that contain VA sensitive information must be adequately protected with FIPS 140-2 certified encryption.

(c) All Department staff, contractors, business partners, or any person who has access to and stores VA sensitive information must have written approval from their respective VA supervisor and ISO before sensitive information can be removed from VA facilities/operating units.

(d) VA sensitive information, to include all sensitive information entrusted to VA, must be in a VA protected environment at all times, or it must be encrypted. OI&T must approve the protective conditions being employed.

(e) Utilization of personally-owned USB thumb drives within the Department is prohibited. FIPS 140-2 certified USB thumb drives will be procured with VA funding for VA employee utilization, if the need to utilize a thumb drive as an external storage device exists. This must be approved by the individual's supervisor and the thumb drive must be provided by the local OI&T senior representative.

(f) The procurement of thumb drives will be accomplished under the direction and control of OI&T.

(g) VA employees are not authorized to access or store any VA information using a thumb drive that has not been procured and issued by OI&T and they must have written permission to receive and use a VA issued thumb drive.

(h) Non-VA personnel (contractors, business partners, etc.) supporting VA must furnish their own FIPS 140-2 certified USB thumb drives that conform to the published listing of VA approved USB thumb drives. Further, permission must be obtained from a designated VA supervisor before they can be utilized.

(i) The listing of VA approved USB thumb drives is derived from NIST FIPS 140-2, Validation Lists for Cryptographic Modules. This listing can be found on the Information Assurance Web Portal. The link to this portal can be found on the VA Intranet, Office of Information and Technology home page.

(j) VA sensitive information may not reside on other non-VA owned Other Equipment (OE) unless specifically designated and approved in advance by the appropriate VA official (supervisor), and a waiver has been issued by the VA's CIO.

(k) The non-VA systems or devices must conform to, or exceed, applicable VA security policies or are specifically authorized by official VA policy. Users of remote systems must follow all policies and procedures outlined in this policy.

(l) The local OI&T Chief /CIO and supervisors will authorize the use of portable, mobile and wireless devices within their operating unit.

(m) Two-factor authentication, (where one of the factors is provided by a device separate from the computer gaining access) is required for remote access to VA systems.

(n) All remote systems (VAGFE and OE) must be equipped with, and use, a VA-approved antivirus (AV) software and a personal (host-based or enclave based) firewall that is configured with a VA-approved configuration. Software must be kept current, including all critical updates and patches. The local facility OI&T office will provide and maintain the software for VAGFE. Users of waivered OE are responsible for providing and maintaining the anti-viral software and the firewall on the non-VA owned OE.

(o) All devices used to transmit and store VA information outside of VA's protected environment must use FIPS 140-2 approved encryption. This includes laptops and thumb drives and other removable storage devices.

(p) Mobile and portable systems will be stored securely when not in use. Supervisors must ensure users understand their responsibility to securely store all portable systems such as laptop computers, notebook computers, PDA's, handheld devices, wireless telephones and removable storage media devices when they are not in use and whenever they are in an unsecured environment.

(q) A mobile storage device must not contain the only copy of sensitive information. A back-up of the device must be created at regular intervals and stored securely.

(r) VA employees, contractors, subcontractors, and volunteers must immediately report to his or her VA supervisor and the local ISO any incident of theft, loss, or compromise of any VA sensitive information, VA equipment or device, or any non-VA equipment or device used to transport, access, or store VA information. The ISO will promptly report the incident (within one hour) to the VA-NSOC in accordance with the OI&T Incident Management procedures.

(s) Portable and mobile devices (e.g., notebook computers, workstations, personal digital assistants) are not allowed access to any VA network without first meeting the VA's and the facility's security policies, procedures, and configuration standards. These include scanning the devices for malicious code, updating virus protection software, scanning for critical software updates and patches, conducting primary operating system (and possibly other resident software) integrity checks, and disabling unnecessary hardware (e.g., wireless).

(t) Mobile, portable and wireless devices will follow VA policy regarding system hardware and electronic media sanitization and disposal.

(u) Wireless devices can pose a significant security risk to the VA due in part to unique vulnerabilities of the wireless extensions to the network located outside of the physical confines of the controlled area. To minimize the risk, the following measures shall be implemented.

1. FIPS 140-2 Encryption of information transmitted to and from a wireless device is required or an appropriate waiver has been approved by the CIO.

2. Wireless devices must meet and be kept up-to-date on the latest anti-viral and software/security patch remediation, as applicable.

3. Authentication is required to protect wireless access to the information system.

(5) Internet Gateways - The Operating Unit will use the VA approved national gateways to access the Internet. These gateways are configured to restrict information flow based on an approved rule set. Users will use the Internet in a secure manner. All users must adhere to the national and local Internet access and usage policy when accessing the Internet and understand that Internet activity is monitored.

(6) External Business Partner Connections - Data communication pathways from VA facilities to non-VA business partners that cannot pass through the One-VA Internet gateways must be fully documented and must have OI&T Chief/CIO and ISO approvals. These connections must be managed and coordinated with and by the VA NSOC. Additional procedures will be issued in a separate document.

(7) Electronic Mail:

(a) Electronic mail shall be used for authorized government purposes and shall contain only non-sensitive information unless the information is appropriately encrypted. Electronic mail users must exercise common sense, good judgment, and propriety in the use of this government resource. Electronic mail is not inherently confidential and users should have no expectation of privacy when using government mail systems. A technical or administrative problem sometimes causes a situation where a system manager or management official may need to review electronic mail messages. Such reviews will be handled in accordance with the Operating Unit's "Electronic Mail Review" standard operating procedure. The ISO will provide concurrence for requests for removal of electronic mail messages when warranted.

(b) Auto-forwarding of email messages to addresses outside the VA network is strictly prohibited.

(8) Facsimile (Fax) Machines:

(a) Care should be taken to assure confidentiality when faxing sensitive information. Following are the precautions that should be taken to protect the security of fax transmissions:

(b) Place the following statement on all fax cover sheets: "This fax is intended only for the use of the person or office to which it is addressed and may contain information that is privileged, confidential, or protected by law. All others are hereby notified that the receipt of this fax does not waive any applicable privilege or exemption for disclosure and that any dissemination, distribution, or copying of this communication is prohibited. If you have received this fax in error, please notify this office immediately at the telephone number listed above."

(c) The HIPAA Security Rule does not apply to faxing because the information is not in electronic format prior to sending. The HIPAA Privacy Rule requirements do, however, apply when faxing protected health information. In the event that a fax is sent via automated systems, or fax back from a computer, then the HIPAA Security Rule does apply because the information was already in electronic format before it was transmitted.

(d) Staff is trained to double check the recipient's fax number before transmittal and to confirm delivery by telephone or review of the appropriate confirmation of fax transmittal.

(e) Fax machines will be placed in controlled areas within VA office space sufficient to physically limit access to the machine by authorized VA staff only. Use of fax machines will be limited to authorized office personnel, and as necessary, or as equipment features allow, security codes used to prevent unauthorized use to transmit, or receive faxed documents.

(f) Staff periodically reminds regular fax recipients to provide notification in the event that their fax number changes.

(g) Fax transmittal summaries and confirmation sheets are saved and reviewed periodically for unauthorized access or use.

(h) Staff have pre-programmed and tested destination numbers in order to minimize the potential for human error.

(9) PBX Voice/Data Telephone Systems:

(a) PBX security includes maintaining an audit trail to capture the date, time, user(s), and activities performed on the PBX system and implementing adequate investigations and audit methods to ensure appropriate and authorized access to the PBX system.

(b) To reduce exposure to security risks, the following actions should be taken, if possible:

(1) Assign authorization codes randomly on a need-to-have basis

(2) Safeguard authorization codes and change them frequently

(3) Limit remote access trunks to domestic calling

(4) Implement the time-of-day PBX option

(5) Implement a system-wide barrier code

(6) Do not use or allow the use of trivial passwords such as "1111" or "2222".

(7) Do not include programmable function keys or speed dialing keys in the password.

(8) Monitor telephone bills regularly, looking for increased activity. If increased activity is suspected, contact the telephone vendor to request an audit of the PBX system to determine if fraud has occurred. Use of the PBX system to monitor telephone calls must be authorized by the facility director/program manager.

(9) All unused telephone jacks should be disabled as soon as possible to prevent unauthorized usage.

(10) Log-on Warning Banners

(a) **Policy:** Public Law 99-474 requires that any system that uses external communication mediums (e.g. dial-up, Internet, etc.) must have a warning banner that appears before the log-on sequence. If technically capable, the information systems within the Operating Unit will display the following VA approved banner:

"This system is intended to be used by [authorized VA network users] for viewing and retrieving information only except as otherwise explicitly authorized. VA information resides on and transmits through computer systems and networks funded by VA; all use is considered to be understanding and acceptance that there is no reasonable expectation of privacy for any data or transmissions on Government Intranet or Extranet (non-public) networks or systems. All transactions that occur on this system and all data transmitted through this system are subject to review and action including (but not limited to) monitoring, recording, retrieving, copying, auditing, inspecting, investigating, restricting access, blocking, tracking, disclosing to authorized personnel, or any other authorized actions by all authorized VA and law enforcement personnel. All use of this system constitutes understanding and unconditional acceptance of these terms.

Unauthorized attempts or acts to either (1) access, upload, change, or delete information on this system, (2) modify this system, (3) deny access to this system, or (4) accrue resources for unauthorized use on this system are strictly prohibited. Such attempts or acts are subject to action that may result in criminal, civil, or administrative penalties."

(b) The system use notification message provides appropriate privacy and security notices and remains on the screen until the user takes explicit actions to log on to the information system.

(c) All VA websites must use the banners approved in VA Directive 6102 Handbook, Internet/Intranet Services.

(d) **Procedure:** The OI&T Chief/CIO will coordinate with the system owners, system managers, and other OI&T personnel to ensure that VA approved logon warning banners are deployed on all VA computer systems, including servers, workstations, routers, switches, and other devices that can accommodate the VA approved banner within their area of responsibility. The ISO will perform regular audits to ensure all capable equipment displays the warning banner.

(11) Audits and Reviews

(a) **Policy**: Each Operating Unit regularly reviews/analyzes audit records for indications of inappropriate or unusual activity, investigates suspicious activity or suspected violations, reports findings to appropriate officials, and takes necessary actions. The Operating Unit employs automated mechanisms, when applicable, to integrate audit monitoring, analysis, and reporting into an overall process for investigation and response to suspicious activities. Each Operating Unit also periodically reviews changes to access authorizations. Each site

undergoes periodic technical and non-technical OI&T security reviews, both internal and external. The results of all reviews/audits are securely maintained.

(b) **Procedure:**

1. External Reviews: The following groups perform external security reviews that focus on both FISMA and HIPAA security requirements:

a. OIG

b. OI&T – *(*performs on-site security reviews)

c. The Joint Commission – (performs periodic reviews)

d. VA NSOC - (conducts penetrations studies when requested)

e. The facility may request or fund additional security reviews as required.

2. Internal Reviews: Activity involving access to and modification of sensitive or critical files is logged, monitored, and possible security violations investigated. At a minimum, the following internal reviews are conducted:

a. System Auditing: System audit logs must record sufficient information to establish what events occurred, the sources, and outcomes of the events. Additional details such as type, location, and subject are also required for moderate and high risk systems. Audit logs will be maintained as follows:

(1) Must be sufficient in detail to facilitate reconstruction of events if a compromise or malfunction is suspected or has occurred.

(2) Must be treated as restricted information and protected from unauthorized access, modification, or destruction and reviewed periodically for action. Access to logs must be granted based upon need to know and least privilege.

(3) Audit logs must be backed up and stored off-site.

(4) The system administrator allocates sufficient audit record storage capacity and configures auditing to prevent such capacity being exceeded.

(5) In the event of an audit failure or audit storage capacity being reached, the information system alerts appropriate OI&T staff and either overwrites the oldest audit records, shuts down the system, or stops generating audit records. A written risk based decision will be made for individual systems as to what happens when capacity is reached.

(6) Audit logs must be retained for one year. Audit logs which describe a security breach must be maintained for 6 years (HIPAA requirement).

(7) Audit logs must be reviewed periodically for potential security incidents and security breaches. Audit logs may be reviewed to evaluate the damage caused by a security breach and also may support the recovery of information lost or modified.

(8) Log-in monitoring: When a lockout occurs, the OI&T system manager will investigate to determine whether the action was that of an authorized user or an attempt to intrude. If it appears to be an intrusion attempt, the OI&T system manager will notify the ISO and the VA NSOC.

(9) Although they work in conjunction, there is a separation of duties between the ISO who reviews the audit trails and the system manager who administers the system.

b. Sensitive Record Audit (VHA specific): Certain health records within VHA are deemed and flagged "sensitive" and access to such records is monitored. The sensitive record access log will be reviewed by the ISO at least weekly (during the business work days). Supervisors/managers or designee in coordination with the ISO, will exercise reasonable controls to ensure that employees cannot obtain access to other employee health records except when they need to have access to the records in order to perform their official duties. If an employee obtains access to another employee's health record without having the requisite need for access to perform his or her duties, the employee could be subject to disciplinary action and/or criminal penalties. Employees that need to review their own record or require copies of their record must present a written request to the Employee Health Nurse or Release of Information section to obtain this information. Veteran employees must contact their local Release of Information section to review or receive copies of their record.

c. Incident-triggered Audits: Investigation of an incident may necessitate a focus review audit. The OI&T Chief/CIO and ISO will collaborate in the audit.

d. Information Access Controls/Security Keys (VHA specific): The ISO reviews the access logs and security key allocations in VistA on a regular basis, at least quarterly, so that each individual's access is restricted to only those functions necessary to perform their duties.

e. Using appropriate tools, such as NetIQ, account policies and restrictions are monitored in Windows 2000 Active Directory in order to determine how password and logon policies are enforced for the entire domain. The status of each user account can be checked in the User Manager. Appropriate security logs for Windows 2000 Active Directory must be enabled and reviewed routinely by system administrators to ensure that security controls are in effect.

f. Menu Reviews: Employee menus (access) are reviewed at least quarterly to ensure that employees are restricted to the menus necessary to perform their duties. Menu adjustments will be made accordingly by the service and audited quarterly by the service and the ISO.

g. User Reviews:

(1) VistA (VHA): Account status is reviewed by the supervisors/managers and the ISO on a quarterly basis to assure the need for account continuation. All accounts unused for more than 90 days are placed in disuser status and thereby made inoperable. Disuser accounts are terminated within one year unless the user's supervisor/manager certifies, in writing, the need for continuation of access. Disuser and terminated accounts are inactive. All user accounts of separated employees, contractors, volunteers, or any other user no longer requiring access will be terminated immediately.

(2) Network: Account status is reviewed by OI&T and reported to the supervisors/managers and the ISO on a quarterly basis to assure the need for account continuation. All accounts unused for more than 90 days are placed in disabled status and

thereby made inoperable. Disabled accounts are terminated within one year unless the user's supervisor/manager certifies, in writing, the need for continuation of access. All user accounts of separated employees, contractors, volunteers, or any other user no longer requiring access will be terminated immediately.

3. FISMA: Management, operational and technical security controls are reviewed each year by completing the FISMA Annual Assessment and regularly updating SMART. New security questions/issues are added to this survey and database as required. This questionnaire helps to identify security deficiencies within the systems. The ISO will ensure the completion of the FISMA Annual Assessment and will oversee the addressing noted deficiencies via the Plans of Action and Milestones (POA&M).

4. HIPAA: VHA has provided the field a HIPAA Self-Assessment Tool that a facility can utilize to ensure HIPAA compliance.

5. Security Documentation Review: The ISO will conduct an annual review with the system owner, system manager, and other OI&T personnel of security documentation for each system within the Operating Unit. Documentation will be updated accordingly.