

## AUTOMATED INFORMATION SYSTEMS (AIS) SECURITY

1. **REASON FOR ISSUE:** This Veterans Health Administration (VHA) Directive revises automated information systems (AIS) security policy.
2. **SUMMARY OF MAJOR CHANGES:** This directive sets forth policies and responsibilities for the establishment, maintenance and oversight of the automated information systems (AIS) security program within the VHA. It incorporates additional requirements mandated by the Office of Management & Budget (OMB) Circular A-130, Appendix III, and provides additional technical security policy and requirements.
3. **RELATED HANDBOOK:** VHA Handbook 6210.1 (to be published), Automated Information Systems Security, will contain the mandatory procedures for implementing appropriate AIS security.
4. **RESPONSIBLE OFFICE:** The Director, Medical Information Security Service (MISS) (193C) is responsible for the contents of this VHA Directive. Questions may be referred to Medical Information Security Service at (304) 262-7300.
5. **RESCISSIONS:** VHA Manual M-11, Chapter 16, is rescinded.
6. **RECERTIFICATION:** The document is scheduled for recertification on or before the last working day of March 2005.

S/ Frances Murphy, M.D. for  
Thomas L. Garthwaite, M.D.  
Deputy Under Secretary for Health

Distribution: **RPC: 0005**  
FD

Printing Date: 3/2000



## AUTOMATED INFORMATION SYSTEMS (AIS) SECURITY

**1. PURPOSE.** This Veterans Health Administration (VHA) Directive defines policies and responsibilities for the establishment, implementation, maintenance and oversight of the automated information systems (AIS) security program within VHA. *NOTE: This policy extends to any new VHA AIS resources acquired, developed, or used on behalf of VHA after the effective date of this Directive.*

### 2. BACKGROUND

a. The “Paperwork Reduction Act, as amended, Title 44 United States Code (U.S.C.) Chapter 35, the Computer Security Act of 1987, Public Law 100-237, and Office of Management and Budget (OMB) Circular A-130, Appendix III, require all Federal agencies to plan for the security of all sensitive AIS resources throughout their life cycle.

b. Department of Veterans Affairs (VA) Directive 6210 provides department-wide policy on complying with applicable legal requirements. AIS security policy development and adherence by VHA components will help ensure that:

- (1) AIS resources operate effectively and accurately;
- (2) There are appropriate technical, personnel, administrative, physical, environmental, and telecommunications safeguards for each system; and
- (3) The continuity of these systems is maintained and preserved.

*NOTE: Throughout this policy the term “facility” will be used to refer to all VHA operations that fall under VHA control, including, but not limited to, facilities, offices, clinics, etc.*

### 3. POLICY

a. Each VHA facility must establish, maintain, and enforce a comprehensive security program, as detailed in this policy, to assure an adequate level of security protection for all AIS, whether maintained in-house or by a non-VA entity.

b. Specifically, each facility must ensure:

- (1) AIS operates effectively and accurately, using appropriate technical, personnel, administrative, environmental, and telecommunications safeguards.
- (2) That a full-time position be established to manage this program effectively.

c. This policy is divided into three AIS security elements: (1) System Security Management (Management Controls); (2) Program Security Management (Operational Controls); and (3) Technical Security (Technical Controls).

**(1) System Security Management (Management Controls)**

(a) System Identification. All AIS resources are to be identified. **NOTE:** *OMB A-130, Appendix III and the National Institute for Standards and Technology (NIST's) Guide for Developing System Security Plans for Information Technology Systems provides guidance in this area.*

(b) Security Plan. A security plan must be prepared for each identified system. The purpose of the system security plan is to provide an overview of the controls and rules of behavior for securing the system, to delineate responsibilities, and to promote communication between managers of different systems. Medical Information Security Service's (MISS) "System Security Plan" Guidance Document provides the necessary instructions and the required format for completion of the System Security Plan document.

**(c) Risk Management**

1. Risk Analysis. All VHA facilities must establish and implement a risk analysis process for each identified AIS resource to ensure that the balance of risks, vulnerabilities, threats, and countermeasures achieve a residual level of risk that is acceptable based on the sensitivity or criticality of individual systems. A risk analysis must be conducted on each identified system to ensure that appropriate and cost effective safeguards are incorporated. A risk analysis is to be performed prior to the approval of design specifications for new systems, whenever a significant change occurs to a system, or at least every 3 years.

**2. Contingency Planning**

a. The VHA mission is dependent upon automated information systems for the support of essential healthcare delivery functions. All facilities are responsible for the development, maintenance, and annual testing of individual AIS contingency plans for these functions. The contingency planning process must address:

- (1) Backup and retention of data and software.
- (2) Selection of a backup or alternate operations strategy.
- (3) Emergency response actions to be taken to protect life and property and minimize the impact of the emergency.
- (4) Actions to be accomplished to initiate and effect backup or alternate site.
- (5) Resumption of normal operations in the most timely, efficient, and cost-effective manner.

b. Copies of the plan are to be communicated to all users, updated as needed, and a copy maintained off-site. **NOTE:** *VA Handbook 6210 outlines mandatory operational requirements for all VA contingency plans.*

(d) Certification. Certification of the system is based on the documented results of the design reviews, system tests, and the recommendations of the testing teams. Certification is a requirement for all systems.

1. New AIS resources, or those not fully operational, must complete all certification requirements and be accredited (approved for processing) prior to full implementation. Prior to accreditation, each AIS resource must undergo appropriate technical certification evaluations to ensure that:

a. It meets all Federal, VA, and VHA policies, regulations, and standards.

b. All installed security safeguards are adequate and appropriate for the protection requirements of the system.

2. Systems will be re-certified when substantial changes are made or at least every 3 years.

(e) Accreditation (Authorization for Processing). Accreditation is required for all systems. New AIS, or those not fully operational, must complete all requirements and be accredited prior to full implementation.

1. The designated management official reviews the accreditation support documentation (i.e., security plan, risk analysis, certification results, contingency plan, rules of behavior) and either concurs, thereby declaring that a satisfactory level of operational security is present; or does not concur, indicating that the level of risk either has not been adequately defined or reduced to an acceptable level for operational requirements.

2. The approving official signs a formal accreditation statement declaring that the system appears to be operating at an acceptable level of risk, or specifies any conditions or constraints that are required for appropriate system protection. Systems will be re-accredited when major changes occur to the system or every 3 years, whichever occurs first.

## (2) **Security Program Management (Operational Controls)**

(a) Personnel Security. Each VHA facility will establish personnel security policies that ensure:

1. All AIS related positions are evaluated and assigned a sensitivity level as defined in Title 5, Code of Federal Regulations (CFR) Section 731.202, Suitability Determinations, and Sections 736.201 and 732.201, Investigative Requirements. The appropriate investigation will be requested to ensure the screening of all individuals (including non-VHA individuals, (e.g., contractors, volunteers, work-study, Compensated Work Therapy (CWT)) before they are granted access to sensitive data or are allowed to participate in the design, operation or maintenance of sensitive systems. The level of screening required may vary from minimal checks to a full background investigation depending on the sensitivity of the information to be handled or the risk and magnitude of loss or harm that could be caused by the position. **NOTE:** *The Emergency Preparedness and Administration Security Office (07C) has issued a "Security and Risk Designation, Appendix A," that establishes guidelines with regard to position sensitivity designation, risk levels and corresponding security investigation requirements.*

2. All position descriptions are written or annotated to reflect specific AIS security responsibilities. Within this context, “specific security responsibilities” refer to employee obligations to protect sensitive data and the use of such data and information derived from it only in the execution of official duties. **NOTE:** *When an employee in a sensitive position transfers or is terminated from the facility, Human Resources Management must notify the appropriate staff at VA Central Office.*

3. Separation of duties for individuals in sensitive positions is assured. This precludes any one individual from gaining the opportunity of adversely affecting the system. Procedural checks and balances must be defined and enforced so that accountability is established and security violations are detectable.

4. A process is established for individual accountability for the proper use and security of the information systems being accessed. This process must ensure that all users are provided with periodic security awareness briefings, copies of system rules, and training to fulfill their AIS security responsibilities.

5. A process is established to grant access privileges based on a legitimate and demonstrated need to have system access. Individuals will be granted access only to that information which is necessary for the job assignment. All user access and privilege must be reviewed at least every 90 days for appropriate level of access or continued need.

6. VHA facility management, or designee(s), are assigned responsibility for approving access to VHA AIS functions upon receipt of a written and/or electronic request from an office or unit supervisor. At a minimum, this request must include the name, service, purpose for access, and the specific access requirements. All approved requests must be routed through the VHA facility ISO.

7. Requests for access to or from remote systems and networks not under the VHA facility management control (e.g., Austin Automation Center, VA-Wide Area Network ) are routed through the ISO prior to approval.

8. Procedures are established that require all users to sign an “Access Notice” before actual access is granted. The “Access Notice” must state at a minimum that the user has reviewed and will abide by the facility’s security policies and procedures. The signed access notices will be maintained centrally by the System Administrator, Chief, Information Resources Management (IRM) Service, or the ISO.

9. Guidance and policy for access to sensitive data is in place for all non-VHA employees (volunteer, work-study, contractors, etc.). In the absence of specific program guidance, each facility is to seek guidance from the Privacy Act Officer and the Regional Counsel prior to allowing access to this class of individuals. **NOTE:** *Access shall be no less stringent than for VHA employees.*

10. Programmer access to Veterans Information Systems Technology and Architecture (VISTA), is approved by VHA facility management, or their designee(s).

11. There is a process to revoke access privileges in a timely manner when the requirement for access ceases (e.g., transfer, resignation, retirement, change of job description, etc.).

12. There is a process to immediately revoke access privileges for individuals being separated for adverse reasons on or just prior to notifying them of the pending action.

(b) Incident Reporting. VHA facilities are to establish and implement a process to minimize the risk associated with violations of AIS security and ensure timely detection and reporting of actual or suspected incidents. An AIS security incident is any event, suspected event, or vulnerability that could pose a threat to the integrity, availability, or confidentiality of VHA information systems' applications or data. Incidents may result in the possession of unauthorized knowledge, the wrongful disclosure of information, denial of service, the unauthorized alteration or destruction of data or systems and violation of Federal or state laws. **NOTE:** *If such events are detected or suspected, the procedures outlined in VA Handbook 6210 must be followed.*

(c) Education, Training, and Awareness. VHA facilities are to establish AIS security awareness and training programs to ensure that all individuals involved in the management, operation, programming, maintenance, or use of the systems are aware of their security responsibilities and are adequately trained prior to being granted access to AIS resources. Any individuals given access to a Federal system, or a system being operated on behalf of the Federal government, must receive a security awareness briefing as part of their orientation training and must be provided with refresher awareness material or briefings at least annually. **NOTE:** *VA Handbook 6210 outlines approved computer security training procedures.*

(d) Software and Data Security. An application that processes sensitive data, or requires protection because of the risk and magnitude of loss or harm that could result from improper operation, manipulation, or disclosure must be provided protection appropriate to its sensitivity.

1. Software applications created by VHA developers are required to meet specific security criteria and be accredited by management prior to release. Security criteria and requirements for certification and accreditation of in-house developed application software, operating system software, and other general purpose software must be in accordance with current NIST and other applicable requirements (e.g., Health Insurance Portability and Accounting Act).

2. All executable software used on sensitive VHA AIS resources must be obtained through authorized procurement channels. The use of software acquired by any other means (e.g., public domain software, bulletin board services, personally owned software) is to be evaluated and approved by facility management (i.e., the officially designated individual or team) before it is downloaded or installed on any system.

3. Safeguards must be in place to detect and minimize inadvertent or malicious modification or destruction, or attempts to do so, of AIS application software, operating system software, and critical data files. These safeguards are to be documented in the facility AIS security plan.

4. Executable software authorized to run on VHA AIS resources must be identified in the AIS security plan.

5. At a minimum, essential data must be backed-up and stored in a location physically separate from the AIS. Appropriate physical and environmental controls must be in place to ensure viability of such back-ups. **NOTE:** *The actual location of backed-up data must be determined by analysis of local risk.*

6. Virus (malicious code software) prevention and control measures must be employed to protect the integrity of the software and data in VHA AIS. **NOTE:** *VA virus control procedures are outlined in VA Handbook 6210.*

7. VHA organizations are to ensure that all software used complies with copyright laws and license agreements. **NOTE:** *Copyright security procedures are outlined in VA Handbook 6210.*

8. In order to maintain software integrity, VHA facilities must use proper configuration management and controls to monitor installation and updates of software. This process is to provide a historical record of software and operating system changes, to ensure that software functions as expected and that only authorized software is permitted on VHA AIS resources.

9. Policies and procedures must be established to protect sensitive information from either accidental, unauthorized, or intentional modification, destruction, or disclosure during input, processing, or output operations.

(e) Hardware Security

1. VHA facilities must ensure that appropriate technical security requirements are included in specifications for the acquisition or operation of new information technology equipment intended to process sensitive information. These specifications are to be reviewed by the Information Security Officer (ISO) prior to the acquisition.

2. Facilities must develop local policy regarding the use of government-owned equipment based on current VA level policies.

3. Security measures must be taken to protect against theft and unauthorized use of AIS peripheral and communications devices, microcomputers, laptops, and related items such as printers, floppy disks, and software.

4. Remote off-site (e.g., dial-in) access to computer systems must be controlled and locally authorized. The removal of peripheral or communication devices from a facility for use off-site must be controlled. Property passes, or other Acquisition and Materiel Management (A&MM) Service approved procedures, are to be issued and a record maintained for all AIS equipment and software removed from the facility, including the individual responsible for the equipment and the date(s) the equipment was removed from, and returned to, the facility.

(f) Technical Support and Maintenance. Technical support and maintenance activities for VHA AIS resources must ensure that:

1. Hardware and software maintenance activities do not affect the integrity of AIS resources and data, particularly existing safeguards or permit the introduction of security exposure into an automated information system (e.g., computer viruses, Trojan horses, logic bombs, etc.).

2. Sensitive VHA AIS electronic storage and memory devices are not released from VHA control without proper clearing procedures to remove residual data. Software that effectively wipes all residue data from systems and hard drives must be used. **NOTE:** *Procedures for safeguarding sensitive information stored on AIS resources during disposal are outlined in VA Handbook, 6210.*

3. Automated (i.e., computer-connected) dial-up diagnostic maintenance of sensitive VHA systems via remote communications between vendors and VHA AIS resources is prohibited unless authorized by management in the system's accreditation (authorization for processing) document. The accreditation should reference an approved contract, Memorandum of Understanding (MOU), or other agreement when such a service is included.

4. AIS technical support and maintenance work performed at VHA facilities (on-site) must be supervised by or under the control of VHA personnel knowledgeable in appropriate AIS operations.

(g) Facility Security. Physical access to AIS resources must be based upon legitimate and demonstrated need. Individuals are only to be granted the access authority and/or system privileges necessary to accomplish their assigned duties.

1. Physical Security. Controlled and restricted areas are to be protected by physical security as appropriate for the sensitivity or criticality of the system. **NOTE:** *System sensitivity and criticality are determined by the results of a risk analysis and as defined in the System Security Plan for the system.*

a. At a minimum, access to controlled areas is to be limited to those individuals having an official need to be in the area.

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

c. All access to these areas are to be logged, and the logs reviewed monthly to determine if access is still required.

d. Media used to record and store sensitive software or data is to be externally identified, protected, controlled, and secured when not in actual use. **NOTE:** *There will be no signs informing the public that an information system is located in any particular building or area.*

2. Environmental Security. Adequate environmental safeguards are to be installed and implemented to protect AIS resources as deemed appropriate for the sensitivity or criticality of the system as determined by the results of a risk analysis and as defined in the System Security Plan for the system. At a minimum, the following environmental safeguards must be implemented in dedicated computer rooms:

a. Fire prevention, detection, and suppression;

- b. Water hazard prevention and detection;
- c. Electric power supply protection;
- d. Temperature control;
- e. Humidity control;
- f. Magnetism protection; and
- g. Good housekeeping procedures for protection against dust, dirt and fire hazards.

(h) Contractor and or Procurement Security

1. Security requirements and specifications for contractors involved in all aspects of the VHA information infrastructure (e.g., system development, system management, software development, system analysis, data input, hardware disposition, data storage, back-up) must be defined in the statement of work and contract. Procurement officials are to ensure negotiated contracts include a separate section dealing with security issues. This section must specify the level of trust required and the contractor's responsibility in complying with established requirements. These documents are approved by the responsible ISO and IRM management prior to signing of a contractual agreement.

2. VHA facilities that utilize contractor assistance in managing, deploying, or operating information systems which process sensitive data must establish all requirements in local policy.

3. Contractor personnel performing work under contract must satisfy all requirements for security eligibility. Contractor personnel who access VHA AIS resources or data shall have a background investigation. Contracts are to stipulate that the contractor will be held responsible for the cost of background investigations, if appropriate. Contractors must submit evidence of prior background investigations to the VA Security Office (07C) for review to ensure that the investigation is of an acceptable level.

(i) AIS Sharing Agreements

1. All non-VHA users having access to VHA AIS resources through a negotiated sharing agreement are to satisfy all requirements for security eligibility prior to the effective date of the agreement. The VHA entity that is party to the sharing agreement is to bear the responsibility for ensuring that security requirements are included in the written agreement and that they are met.

2. Procurement officials are to ensure that all AIS sharing agreements pertaining to AIS hardware and software are reviewed for security implications. They are responsible for the inclusion of a separate section in the contract dealing with AIS security issues, where appropriate.

3. All security requirements of OMB A-130, Appendix III, must be implemented.

(3) **Technical Security (Technical Controls)**

(a) **System Security.** The design of AIS resources that process, store, or transmit sensitive data must include, at a minimum, the automated security features discussed in this paragraph. Security safeguards must in place to ensure those persons having access to an AIS resource are individually accountable for their actions while on the system.

**1. User Identification.** User access will be controlled and limited based on positive user identification and authentication mechanisms that support the minimum requirements of access control, least privilege, and system integrity for all platforms.

**a.** To ensure accountability, individual access codes (passwords) are mandatory for all sensitive VHA information systems.

**b.** Controls must be implemented to require passwords that meet Departmental standards and complexity. *NOTE: These controls must be tested quarterly to ensure compliance.*

**c.** Passwords must be changed at least once every 90 days.

**d.** Passwords that are inactive for 90 days are to be disabled.

**e.** Operating systems are sometimes installed with a standard set of default user accounts and associated standard security passwords. This access route must be protected by either disabling the standard user account or by changing the passwords.

**2. Authentication.** The AIS resource must ensure that each user is authenticated prior to access.

**3. Access Control.** AIS resources must employ additional discretionary access control measures such as file passwords, access control lists, disk encryption, or other techniques, as identified and required by the approved system security plan. In addition, the following automated security processes are required:

**a. Warning Banner.** A warning banner must be displayed to users as part of the logon dialogue, followed by a pause requiring manual intervention to continue.

**b. Automatic Interactive-session Time-out (logoff).** The automatic interactive-session timeout must be implemented for all VHA AIS. This time-out period is to be determined by system and/or data criticality as defined in the risk analysis.

**4. Audit Records.** AIS transactions are subject to recording and are to be reviewed at least weekly for adverse activity. Audit trail records must be sufficient in detail to facilitate reconstruction of events if compromise or malfunction occurs, or is suspected. Audit trail records must be reviewed as specified in the facility system security plan. Audit trails should be maintained for a minimum of 6 months.

**5. Object Reuse.** Automated information systems must clear memory and/or data storage areas prior to reallocation of the area to a different user. *NOTE: This prevents one user from obtaining residual data of another user.*

(b) Network and Communication Security. Network and communication security deals specifically with the safeguarding of sensitive information from unauthorized access while it exists in its electronic form during transmission. Sensitive information must be protected while traveling across networks (e.g., Wide Area Networks (WANs), Internet). **NOTE:** *VA is currently seeking solutions to incorporate global encryption technology and standards for the WAN. If individual sites encrypt local area networks and databases, existing Federal and VA standards must be applied. Sensitive data must be secured when using mediums such as facsimile (FAX), Public Branch Exchange (PBX), and voice mail systems. Local area network (LAN) security procedures are located in VA Handbook 6210.*

### 1. Protection of Network Infrastructure

a. Routers, bridges, hubs, concentrators, gateways, digital termination equipment, communication controllers, communication servers, wiring closets, premise wiring, backbone network cabling and any other types of communication equipment are components of the network infrastructure. Physical and electronic access to network infrastructure components must be controlled with access limited to only those support personnel with a demonstrated need. Network infrastructure components must be stored in secured facilities or locked inside containers to prevent unauthorized access.

b. Facilities are to incorporate physical labeling of infrastructure components (e.g., servers, routers, and firewalls) to assist in proper identification. Facilities must inventory all components at regular intervals for asset management, physical protection, and proper functionality.

### 2. VHA Connections to External Networks

a. Security precautions need to be taken when connecting VHA networks with external “untrusted” networks such as the Internet, universities, and vendors. The primary objective is to provide legitimate users adequate access to sensitive data while preventing unauthorized individuals access to sensitive information or resources. Security (e.g., firewall, encryption, authentication) solutions must be put in place between external “untrusted” networks and internal, “trusted” networks.

b. Established interconnections are to be documented in the system security plan and accredited by the approving official at the facility.

c. Facilities establishing “independent gateways” to networks external to the VHA network must obtain official VHA approval. The gateways must meet VHA specified technical and security criteria and be accredited prior to operation.

d. Audit trail monitoring is to be activated on all gateways. All access attempts, both successful and unsuccessful, from the external networks to VHA systems are to be logged and reviewed regularly. Auditing will be activated 7 days a week, 24 hours a day.

e. Facilities planning to create interconnections with systems operated by state, commercial, or other government organizations shall review and resolve security and privacy implications prior to activating the connection.

f. VHA organizations that provide access to the general public via Internet web pages, etc. are to establish policies and procedures for doing so securely. *NOTE: Documentation of this process must be included as part of a system security plan.*

### 3. **Modem Communications**

a. Data communication connections via modems are to be limited and tightly controlled as they pose a serious risk that can circumvent security controls intended to protect VHA networks from external, "untrusted" networks.

b. Reliable and confidential hardware and software authentication systems are to be incorporated into the asynchronous communication servers. Positive authentication is to be established prior to granting access to network resources. Event logging functions are to be provided to enable a review of suspicious activities.

c. Controls are required for remote access to VHA systems. A log will be maintained and reviewed quarterly of individuals granted remote access to ensure accountability is maintained.

4. **Electronic Mail (E-Mail)**. Electronic mail and information messaging applications and systems are to be used as outlined in VA level and locally developed policy. They must contain only non-sensitive information unless the data, and accompanying passwords or other authentication mechanisms are appropriately secured. *NOTE: VA Directive 6301, Electronic Mail Records establishes the policies and responsibilities for managing the creation, maintenance, use, and disposition of Federal records created or received in electronic mail applications.*

## 4. ACTION

### a. **VHA Chief Information Officer (CIO)**

(1) The CIO has overall program responsibility for the VHA AIS Security Program and ensures that development and implementation of the AIS Security Program meets all Federal, Departmental, and VHA standards, policies and guidelines.

(2) The CIO, or designee, must authorize, in writing, that the security of information systems and major applications procured, developed, and deployed by the Information Office (IO) meet current security standards and include the explicit acceptance of any risks deemed uncontrollable.

b. **Associate Chief Information Officer (ACIO) for Customer Services**. The ACIO is responsible for:

(1) Ensuring that information security is incorporated into the overall VHA IRM plan.

(2) Selecting the Director, MISS, to manage the VHA AIS Security Program.

c. **Director, MISS.** The position of Director, MISS, serves as VHA ISO, and is responsible for the following functions:

(1) Developing and disseminating AIS security policy and guidelines to support the implementation of an effective national information security program in all VHA offices and facilities that use computing resources.

(2) Advising the VHA CIO on strategies for addressing information security deficiencies identified in VHA information systems

(3) Providing external reviews of VHA AIS resources at least every 3 years.

(4) Providing oversight of the VHA AIS security incident response program including incident reports as required.

(5) Providing technical security expertise and consultation to VHA facilities.

(6) Reviewing and disseminating information and implements procedures on:

(a) New laws, regulations, VA, and VHA policies concerning information security.

(b) New technology and techniques to improve information security measures.

(c) Investigation of potentially criminal information security breaches.

(d) Security awareness activities and training as set forth in the Office of Personnel Management (OPM) Computer Security Training guidance.

(e) Criteria for certifying and accrediting (authorization for processing) information systems that process sensitive information.

d. **VHA Developers, Information Technology (IT) Support Personnel and Procurement Staff.** These individuals are responsible for:

(1) Ensuring that all controls required to comply with applicable information security policies and standards are incorporated and operating in applications as specified.

(2) Ensuring system security plans, as required by applicable information security policies and standards, are incorporated into all development cycles and procurement documents.

(3) Ensuring an information system security review is performed on systems processing sensitive information before being placed into service.

(4) Ensuring all required information about systems developed, maintained, or procured is made available to persons responsible for authorizing the use of information systems that process sensitive information.

(5) Addressing information security deficiencies identified on the systems being developed, maintained, or procured, including deficiencies identified by either internal or external reviews.

e. **Veterans Integrated Service Network (VISN) Directors.** VISN Directors must provide management and resource support for security programs within their VISN. The VISN program must implement policies, standards, and procedures that are consistent with VHA, VA, and other Federal governing authorities (i.e., OMB, OPM, NIST).

f. **Medical Center Directors.** The Director of each medical facility is responsible for the implementation of the facility's information security program and the AIS resources within their facility. Each facility Director designates an ISO whose responsibility will be to develop, implement, and monitor station-specific information security policy and procedures.

(1) The ISO responsibility is to be assigned to an individual knowledgeable in information technology and security matters.

(2) The ISO position is a full-time position in larger and consolidated facilities and, at a minimum, the primary responsibility for ISOs in smaller facilities. *NOTE: From a security standpoint, key positions shall be separated so that the duties of any one person will not adversely affect the AIS resources due to conflict of interest or malicious intent.*

g. **ISO and the Alternate Information Security Officer (AISO).** The facility ISO is the principal officer at a VHA facility responsible for:

(1) Ensuring that policies and procedures related to the availability, confidentiality and integrity of all sensitive data in all information systems at the facility are adhered to and in place.

(2) Managing and coordinating an information security program that is in compliance with this directive and with other official documents that address the specific organizational structure, physical environment, and computing resources of the facility.

(3) Ensuring that the security of each VHA AIS under the facility's responsibility is documented with a System Security Plan and its related documentation (risk analysis, contingency plan, rules of behavior, certification, and accreditation).

(4) Ensuring that an information system security review is performed on all AIS at least every 3 years or when changes or modifications having security significance are made to the systems or environment.

(5) Providing required security training for facility staff.

h. **Facility Chief, IRM, CIO, or System Managers.** The Chief IRM, CIO, or System Manager is responsible for:

(1) Ensuring all applicable security controls are addressed in information systems that are managed by the Chief IRM, CIO, or System Manager.

(2) Ensuring all technical controls required to comply with applicable information security policies and standards are incorporated into those systems processing sensitive information under their control and that these systems are operating as designed.

(3) Ensuring that an information system security review is performed on all AIS resources under their control at least every 3 years, or when changes or modifications having security significance are made to the systems or environment.

(4) Ensuring all required information is made available to persons responsible for accrediting the AIS resources under their control.

(5) Documenting the security on all AIS resources under their control with a System Security Plan and its related documentation (risk analysis, contingency plan, rules of behavior, certification and accreditation).

(6) Ensuring that information security deficiencies identified on the systems under their control are addressed, including deficiencies identified through security review of systems performed by themselves, ISOs, AISOs, MISS, or other other applicable reviewing organizations (e.g., Inspector General (IG) and Joint Commission on Accreditation of Health Care Organizations (JCAHO)).

i. **Individual users.** Individual users are responsible for:

(1) Protecting AIS resources within their control or possession.

(2) Applying the security controls required by AIS security policies and standards.

(3) Attending AIS security training.

(4) Notifying supervisors of security violations.

(5) Accessing only the AIS applications and data necessary to perform their duties.

## 5. REFERENCES

a. Title 44 U.S.C. Chapter 35.

b. Public Law 100-237.

c. Title 5 CFR Section 731.202, 736.201 and 732.201.

d. OMB Circular A-130, Appendix III.

e. VA Directive 6210.

f. VA Handbook 6210.

g. VA Directive 6301.