DEPARTMENT OF VETERANS AFFAIRS (VA)
SALT LAKE CITY HEALTH CARE SYSTEM
Salt Lake City, Utah

MEMORANDUM 005R5.04 June 8th, 2018

FACILITY INFORMATION SECURITY POLICY – INFORMATION SECURITY OFFICE

1. PURPOSE: This document establishes policy and responsibilities for the security of VA's information and information systems contained in this organization. The security program of this VHA Salt Lake City VA Medical Center is designed to protect all Information Technology (IT), systems, information, and telecommunications resources from unauthorized access, disclosure, modification, destruction, or misuse.

2. POLICY:

a. This VHA SLC VAMC follows the security policy and procedures contained in VA Directive and Handbook 6500.

b. This VHA SLC VAMC has developed Standard Operating Procedures (SOPs) for the policies/controls that need to be defined at the local level. These SOPs have been distributed to the individuals required to perform the procedures and copies can also be obtained from the VHA SLC VAMC intranet site http://vaww.visn19.portal.va.gov/sites/slc/policies-memorandums/SitePages/Home.aspx) in the Publications/Policies & Memorandums section under 142I (Area Manager) and 005R5 (Facility ISSO).

3. SCOPE:

a. This policy applies to this VHA SLC VAMC and any related facilities (i.e., CBOCs) and to the security of all information that is collected, transmitted, used, stored, or disposed of, by or under the direction of this staff or its contractors.

b. All users of this VHA SLC VAMC's VA information systems or VA sensitive information are responsible for complying with the rules outlined in the VA National or Contractor Rules of Behavior (ROB), as well as procedures and practices developed in support of the VA National ROB. At VA, users are Department personnel, employees, contractors working under an approved contract, business associates working under approved business associate agreements, and any other individuals providing services or performing functions for, to, or on behalf of VA who have been authorized by VA to access VA information systems or VA sensitive information.

c. All users responsible for implementing the policy and procedures outlined in VA Directive and Handbook 6500, as well as the VA National or Contractor ROB will be provided copies of the documentation.

d. Violations of security policy or procedures will be brought to the attention of management for appropriate disciplinary action and reported in accordance with local and national IT Operatsions (ITOPS) Incident Reporting policies and standard operating procedures.

e. Security requirements also apply to 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.

f. 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.

g. Security applies to all information collected, transmitted, used, stored, or disposed of, by or on behalf of VA.

4. <u>INFORMATION SECURITY RESPONSIBILITIES:</u>

a. **Program Directors/Facility Directors**, through the ISSO, are responsible for:

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

(2) Ensuring a VA ISSO and a VHA Health Care Security Requirements Compliance, Advisory, and Security Engineering Security Engineer (for VHA projects) 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, and other procurement documents that require the ISSO's participation;

(3) Ensuring that respective staff, with defined FISMA security roles, provide the ISSO (in a timely manner) the information required to complete the quarterly FISMA reporting to ITOPS and OMB; and

(4) Ensuring all Plan of Action and Milestone (POA&M) corrective actions are taken by their respective staff.

b. **Information System Security Officers (ISSO)** are the agency officials assigned responsibility by ITOPS to ensure that the appropriate operational security posture is maintained for an information system or program. VA ISOs are responsible for:

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

(2) Reviewing proposed statements of work for VA contracts to ensure that the resulting contracts sufficiently define information security requirements, as appropriate;

(3) 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, or disposal activities (i.e., SDLC System Development Life Cycle management);

(4) Assisting in the determination of the appropriate security categorization of the IT system commensurate with the impact level;

(5) Coordinating, advising, and participating in the development and maintenance of information system security plans, system risk analysis, and contingency plans for systems within their area of responsibility;

(6) Verifying and validating, in conjunction with the System Owners and managers, that appropriate security measures are implemented and functioning as intended;

(7) Working with the System Owner and manager according to the information systems at the site, to ensure controls remain in place, operate correctly and produce 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;

(8) Participating in security self-assessments, external and internal audits of system safeguards and program elements, and assessment and authorization of the systems supporting the offices and facility within their area of responsibility;

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

(10) Notifying the VA-NSOC and/or the OIG of any suspected incidents within one hour of discovering an incident and assisting in the investigation of incidents, if necessary;

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

(12) Monitoring compliance with the VA Privacy and Information Security Awareness and Rules of Behavior training requirements for each employee/contractor;

(13) Coordinating, monitoring, and conducting periodic reviews to ensure compliance with the VA National or Contractor ROB requirement for users of VA information systems or VA sensitive information;

(14) Serving as the liaison to the VA Training Manager to ensure VA Privacy and Information Security Awareness and Rules of Behavior training is provided within their area of responsibility;

(15) Coordinating with the facility Privacy Officer for the assurance of reasonable safeguards as required by the Privacy Act, the HIPAA Privacy and Security Rules, and other Federal privacy statutes;

(16) Working with the facility Privacy Officer to ensure information security and privacy procedures complement and support each other;

(17) Coordinating with ITOPS staff to add, change, suspend, or revoke access privileges according to the Director's guidance and concurrence when a system user under their oversight no longer requires access privileges or fails to comply with this policy; and

(18) Reviewing human subject research protocols (VHA ISSOs) as outlined in VHA Directive 2007-040, *Appointment of Facility Information Security Officer and Privacy Officer to the Institutional Review Board (IRB) or the Research and Development (R&D) Committee*, and VHA Handbook 1200.05, *Requirements for the Protection of Human Subjects in Research*.

c. **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:

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

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

(3) 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 their official duties;

(4) Ensuring users under their oversight comply with this policy and pursue appropriate disciplinary action for noncompliance;

(5) Ensuring users of VA information systems or VA sensitive information under their oversight complete all security and privacy training requirements;

(6) Ensuring users of VA information systems or VA sensitive information under their supervision or oversight review and sign VA's National or Contractor ROB on an annual basis;

(7) Notifying system administrators and ISSOs of new users per locally approved procedures;

(8) Notifying system managers and ISSOs to revoke access privileges in a timely manner when a user under their supervision or oversight no longer requires access privileges or the user fails to comply with this policy;

(9) Participating in internal audits, as required, to ensure users have appropriate access;

(10) Authorizing remote access privileges for authorized users 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;

(11) Ensuring users report any suspected or potential incidents immediately upon discovery to management officials, ISSOs, and POs;

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

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

d. **Local Area Manager/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:

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

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

(3) Participating in risk assessments as outlined in the system security plan;

(4) Participating in self-assessments, external and internal audits of system safeguards and program elements, and in assessment and authorization of the system;

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

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

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

(8) Developing system administration and operational procedures and manuals as directed by the System Owner;

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

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

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

(12) Providing information on users and/or the system in support of any reports or documents necessary for oversight and authorization;

(13) Reading and understanding all applicable use policies or other ROB, including the VA National or Contractor ROB, regarding use or abuse of the Operating Unit's information system resources;

(14) 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;

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

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

e. **Contracting Officers (CO)/Contracting Officer's Representatives (COR)** are responsible for:

(1) Ensuring that security requirements and security specifications are explicitly included in VA contracts, as appropriate;

(2) Working with the ISSO and PO to ensure that contracts contain the required security clause and security language necessary for compliance with FISMA and 38 U.S.C. 5721-28 and to provide adequate security for information and information systems used by the contractor, including the requirement for signing VA Contractor ROB, when applicable;

(3) Ensuring contractors meet the appropriate background investigation requirements in accordance with VA Directive and Handbook 0710, *Personnel Security and Suitability Program*.

(4) Ensuring contractors complete VA's Privacy and Information Security Awareness and Rules of Behavior training and any additional role-based training, as outlined in the contract;

(5) Monitoring the contract to ensure that security requirements are being met, consulting the ISSO and/or PO as necessary; and

(6) Assisting other VA officials with significant IT responsibilities in the remediation and updating the POA&M identified during the assessment and authorization process of a contractor's system when required, including periodic compliance validation reviews and the FISMA annual assessment reporting to reduce or eliminate system vulnerabilities.

f. **Local HR Staff/Security and Law Enforcement Staff** are responsible for implementing specific security role based functions and are responsible for the following:

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

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

g. **Users of VA Information and Information Systems** are responsible for complying with the VA National ROB. VA contractors are responsible for complying with the VA Contractor ROB.

5. REFERENCES

a. The VHA SLC VAMC complies with:

(1) VA Directive 6500, *Managing Information Security Risk: VA Information Security Program;*

(2) VA Handbook 6500, *Risk Management Framework for VA Information Systems – Tier 3: VA Information Security Program*;

(3) Federal IT security laws and regulations, including the Computer Security Act of 1987 (PL 100-235);

(4) Office of Management and Budget (OMB) Circular A-130 and its appendices;

(5) Health Insurance Portability and Accountability Act (HIPAA);

(6) Federal Information Security Management Act of 2002 (FISMA); and

(7) National Institute of Standards and Technology (NIST) guidance.

6. RECISSION: New Local Policy

7. RECERTIFICATION DATE: This Policy is scheduled for recertification on or before the last work day of June 2021

8. FOLLOW-UP RESPONSIBILITY: Information Security Officer (005R5)

SHELLA STOVALL
Director

/S//