DEPARTMENT OF VETERANS AFFAIRS
Washington, DC 20420

VA Handbook 6500.10
Transmittal Sheet
February 15, 2018

MOBILE DEVICE SECURITY POLICY

1. **REASON FOR ISSUE:** To provide the policy for Department of Veterans Affairs (VA) to centrally manage and secure VA GFE mobile devices (e.g., smartphones and tablets) used by VA employees and contractors to access the Department's information resources.

2. **SUMMARY OF CONTENTS/MAJOR CHANGES:** This Handbook provides policy and roles and responsibilities for VA's centralized management of VA GFE mobile devices. The Handbook is based on National Institute of Standards and Technology Special Publication 800-124, Guidelines for Managing the Security of Mobile Devices in the Enterprise.

3. **RESPONSIBLE OFFICE:** The Office of the Assistant Secretary for Information and Technology (005), Information Security (005R), Cyber Security (005R2), is responsible for the content of this Handbook.

4. **RELATED DIRECTIVE:** VA Directive 6500 rev.4, Managing Information Security Risk: VA Information Security Program and VA Handbook 6500 rev.4, Risk Management Framework for VA Information Systems – Tier 3: VA Information Security Program

5. **RESCISSIONS:** None

CERTIFIED BY:

/s/

Melissa S. Glynn, PhD
Assistant Secretary for
Office of Enterprise Integration

BY DIRECTION OF THE SECRETARY OF VETERANS AFFAIRS:

/s/

Scott R. Blackburn
Executive in Charge
for Information & Technology

Distribution: Electronic Only

This page is intentionally blank for the purpose of printing front and back copies.

MOBILE DEVICE SECURITY POLICY DRAFT

CONTENTS

PARAGRAPH **PAGE**

1. PURPOSE AND SCOPE 5

2. RESPONSIBILITIES 6

a. Assistant Secretary for Information and Technology 6
b. Deputy Assistant Secretary for Enterprise Program Management Office 6
c. Principal Deputy Assistant Secretary for Information and Technology 6
d. Information Owners 7
e. Deputy Assistant Secretary for IT Operations and Services and Information System Owners 7
f. Information Security Officers (ISO) 8
g. Privacy Officers (PO) 9
h. Local CIOs and System Administrators 9
i. Mobile Workgroup 9
j. Mobile Device Users 10
k. Office of Inspector General (OIG) 10

3. POLICY AND PROCEDURES 10

Appendix A. Terms and Definitions A-1
Appendix B. Acronyms and Abbreviations B-1
Appendix C. References C-1
Appendix D. Mobile Device Rules of Behavior D-1

This page is intentionally blank for the purpose of printing front and back copies

MOBILE DEVICE SECURITY

1. PURPOSE AND SCOPE

a. The purpose of the Department of Veterans Affairs (VA) Government Furnished Equipment (GFE) Mobile Device Security Handbook is to define the types of mobile devices that are permitted to access VA resources, the degree of access permitted, how provisioning and development should be handled, how VA will select, implement, and use centralized mobile device management technologies, and responsibilities related to mobile device security.

b. VA's Mobile Device Security Handbook is consistent with and complements VA's security policy as defined in VA Directive 6500 rev.4, *Managing Information Security Risk: VA Information Security Program* and VA Handbook 6500 rev.4, *Risk Management Framework for VA Information Systems – Tier 3: VA Information Security Program*, as well as other related VA Handbooks. Security policy for any Information Technology (IT) is provided in VA Directive and Handbook 6500 and is based upon National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*. This Handbook addresses specific security policy requirements for securing VA-issued mobile devices and incorporates the guidance of NIST SP 800-124, *Guidelines for Managing and Securing Mobile Devices in the Enterprise*.

c. This Handbook provides VA policy for securing particular types of mobile devices, including smartphones, tablets, and E-readers. Mobile devices within the scope of this Handbook have the following characteristics:

(1) Small form factor such that it can be easily carried by a single individual;

(2) Designed to operate without a physical connection (e.g., wirelessly transmit or receive information);

(3) Possesses local, non-removable or removable data storage;

(4) Includes a self-contained power source; and

(5) May include voice communication capabilities, on-board sensors that allow the devices to capture information, or built-in features for synchronizing local data with remote locations.

d. Laptops are specifically excluded from the scope of this Handbook because the security controls available for laptops are quite different from those available for smartphones, tablets, and other types of mobile devices. Additionally, mobile devices with minimal computing capability, such as basic cell phones, are out of scope of this Handbook due to the limited security options available and limited ability to access VA information resources.

2. RESPONSIBILITIES

The responsibilities listed below are specific responsibilities related to mobile device security. For overall information concerning security program responsibilities for these positions, see VA Directive and Handbook 6500 rev.4.

a. **Assistant Secretary for Information and Technology, as the VA Chief Information Officer (CIO),** is responsible for:

(1) Overseeing VA's mobile device security strategy and related policies, procedures, and standards, as needed, and to address changes in mobile device and mobile device management technologies; and

(2) Requiring security configuration of mobile devices consistent with VA's continued vigilance in safeguarding Veterans' personal information.

b. **Deputy Assistant Secretary for Enterprise Program Management Office is responsible for:**

(1) Developing a plan to implement mobile devices while ensuring Office of Information Security (OIS) is included in implementation planning;

(2) Maintaining awareness of changes in mobile device and mobile device management technologies to facilitate evaluation, approval, and baseline development for new solutions and devices;

(3) Approving any deviations from the approved devices, configurations, and baselines;

(4) Coordinating the approval of VA applications that will send, receive, or store any VA sensitive data (Personal Health Information (PHI)/Personally Identifiable Information (PII));

(5) Coordinating the approval of any applications for any operating system where the commercial application store does not perform validated malware tests;

(6) Adding approved applications (COTS/VA Developed) to the VA Application (App) Catalog once they are approved;

(7) Instituting the information security requirements necessary to protect the organization's mission; and

(8) Ensuring business functions are adequately addressed in all aspects of enterprise architecture, including reference models, segment solution architectures, and the resulting information systems supporting those mission and business processes.

c. **Principal Deputy Assistant Secretary for Information and Technology** is responsible for:

(1) Collaborating with IT Operations and Services (ITOPS) Solution Delivery (SD) in developing threat models for mobile devices and the resources accessed through the mobile devices;

(2) Collaborating with ITOPS SD in specifying security standards for mobile devices based on VA and Federal policy and reasonable security practices appropriate for the intended uses of the device;

(3) Collaborating with ITOPS SD to ensure baselines for mobile devices and mobile device management systems meet VA's security policies and applicable standards;

(4) Coordinating with ITOPS SD to identify content to be included in training on mobile device threats, recommended security practices, and users required to receive the training;

(5) Working with ITOPS SD to ensure mobile devices are compatible with the current VA security posture;

(6) Supporting ITOPS SD in developing a plan for mobile device implementation;

(7) Coordinating and performing the necessary activities required for the Assessment and Authorization (A&A) of mobile device solutions; and

(8) Collaborating with ITOPS SD in approving any deviations from the approved devices, configurations, and baselines.

d. **Information Owners** (e.g., Veterans Health Administration, Veterans Benefits Administration, and National Cemetery Administration) are responsible for:

(1) Identifying the levels of security controls and adhering to privacy and records management requirements for VA sensitive data created, collected, processed, disseminated, maintained and disposed of by mobile device systems;

(2) Determining the levels of access permitted from mobile devices to VA sensitive data; and

(3) Determining which mobile device services or features are enabled and/or accessible by their employees.

e. **Deputy Assistant Secretary for IT Operations and Services and Information System Owners** are responsible for**:**

(1) Ensuring the procurement, development, integration, modification, daily operations, maintenance, and disposal of VA mobile devices and mobile device management solutions;

(2) Ensuring compliance with Federal security regulations and VA security policies by VA's mobile device solutions;

(3) Ensuring the system is deployed and operated in accordance with the agreed-upon security controls;

(4) Ensuring compliance with the enterprise and security architecture throughout the system life cycle;

(5) Coordinating with OIS to define content included in training on mobile device threats, recommended security practices, and users required to receive the training;

(6) Ensuring the mobile device system implements appropriate security controls by scoping, tailoring, compensating, and supplementing the security control baseline as outlined in VA Handbook 6500, and documenting the system security controls in a System Security Plan (SSP);

(7) Ensuring mobile device solutions are assessed and authorized per the requirements of VA Handbook 6500.3, *Assessment, Authorization, and Continuous Monitoring of VA Information Systems*;

(8) Conducting information system security engineering activities for developing code for mobile devices and VA's mobile device management solutions;

(9) Employing best practices when implementing security controls within an information system, including software engineering methodologies, system/security engineering principles, secure design, secure architecture, and secure coding techniques;

(10) Ensuring VA contract and security language are agreed upon and followed with vendors and contractors prior to procurement and maintained throughout the life cycle of the mobile device and/or application. This includes, but is not limited to, Authorization and Assessments prior to procurement of the mobile device/application and continuous monitoring and re-assessments thereafter, vendor patch and change management, and meeting Federal Information Security Management Act (FISMA) security requirements, such as with NIST and Federal Information Processing Standard (FIPS) requirements;

(11) Reviewing and testing baseline configurations for approved mobile device solutions;

(12) Reviewing and evaluating mobile device solutions to ensure they are compatible with the current VA security posture and VA security tools;

(13) Ensuring mobile devices are capable of being managed by the mobile device management system and available VA resources;

(14) Testing encryption products to ensure compliance with VA and Federal requirements;

(15) Developing standards for device approvals, baseline configurations, and systems that manage mobile devices;

(16) Collaborating with OIS to ensure baselines for mobile devices and mobile device management systems meet VA's security policies and applicable standards; and

(17) Publishing information to the intranet regarding VA-approved devices, configurations, and baselines.

f. **Information Security Officers (ISO)** are responsible for:

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

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

(3) 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 (e.g., System Development Life Cycle (SDLC) management);

(4) Working with the System Owner and manager to ensure controls remain in place, operate correctly and produce the desired results; and

(5) Notifying the VA Network and Security Operations Center (NSOC) of any suspected incidents within one hour of discovering an incident and assisting in the investigation of incidents, if necessary.

g. **Privacy Officers (PO)** are responsible for**:**

(1) Working with System Managers and Information Owners to provide administrative, technical, and physical safe guards that protect the integrity, availability, and confidentiality of sensitive personal information within their administrations, staff offices, or facilities; and

(2) Coordinating with ISOs to respond to all privacy complaints and/or potential or actual privacy incidents that fall within their purview of responsibility within one hour of discovery; after normal business hours, and on weekends/holidays contact NSOC.

h. **Local CIOs and System Administrators** are responsible for:

(1) Administering the day-to-day operations of mobile devices as defined in the Scope of Work for this Handbook, including smartphones, tablets, and E-readers;

(2) Maintaining the asset management of mobile devices;

(3) Monitoring devices issued by the local facility, and enforcing compliance through working with Regional Administrators and receiving scheduled compliance reporting;

(4) Configuring mobile devices as required per VA security requirements and configuration baselines; and

(5) Ensuring compliance with Federal security requirements and VA policies.

i. **Mobile Workgroup** is commissioned by the VA CIO and is responsible for**:**

(1) Identifying any issues related to mobile devices which need to be addressed; and

(2) Resolving any issues arising from the implementation of baseline configurations and mobile device management solutions.

j. **Mobile Device Users** are responsible for:

(1) Complying with their responsibilities as stated in the VA National Rules of Behavior and Mobile Device Rules of Behavior, and completing annual information security awareness training and any required mobile device training;

(2) Permitting VA to examine any VA GFE mobile device promptly upon request;

(3) Reporting unauthorized access or disclosure of VA sensitive information, lost or stolen devices, or any other suspected or identified information security incidents immediately to their supervisor, ISO, and PO; and

(4) Accepting that use of mobile device is subject to monitoring of access and connection to VA's network.

k. **Office of Inspector General (OIG)**

Due to statutory independence, procures and manages its mobile devices. VA will provide mobile device management support including access to other resources on the VA internal network in accordance with 5 U.S.C. Appendix §6(d). OIG users will adhere to OIG's Rules of Behavior and OIG policies. OI&T will coordinate with officials designated by the OIG CIO to implement OIG CIO's authorized application whitelisting (e.g., law enforcement applications that process PII and that cannot be hosted in any VA application store), device configuration, or other requirements. OI&T will provide mobile device management policy and configuration support to ensure OIG CIO requirements only apply to OIG devices. Technical Reference Model (TRM) and other OI&T approvals do not apply to OIG devices. OI&T will log and monitor OIG devices on VA's device management solution and will report incidents to the OIG ISO and OIG CIO-designated staff.

3. POLICY AND PROCEDURES

a. Mobile Device Security Overview

(1) VA will centrally manage mobile devices accessing the VA network through a mobile device management system. Only VA GFE mobile devices may be connected to the VA network or may be used to store or transmit VA data. To be approved, VA mobile devices must be capable of being supported by the mobile device management system. Unapproved devices will be blocked from accessing the network.

(2) VA requires mobile devices to comply with applicable Federal laws, Executive Orders, policies, regulations, standards, and guidance. OIS will specify security standards for Government mobile devices based on VA and Federal requirements and reasonable security practices appropriate for the intended uses of the device.

(3) OIS will maintain the Mobile Device Rules of Behavior in Attachment D of this Handbook that identifies the mobile device users' responsibilities to comply with the requirements of this policy and to protect mobile devices from emerging threats. The Mobile Device Rules of Behavior will be published on the Talent Management System for users to review and document their acceptance prior to receiving a VA mobile device.

(4) VA mobile device solutions must receive an authorization to operate prior to their implementation. Requirements for completing A&A are found in VA Handbook 6500.3, *Assessment, Authorization, and Continuous Monitoring of VA Information Systems*. Subsequent to receiving an authorization to operate, mobile device solutions will be continuously monitored.

(5) VA-approved mobile device operating systems will be included in VA's TRM. For those that have not been approved in the TRM, ASD will coordinate a waiver. VA will ensure the organization's mobile device solutions and standards are updated as needed. VA will periodically reassess its mobile device solutions and standards, at which time VA may change the types of mobile devices that are permitted and the types of access granted.

(6) VA will secure each VA GFE mobile device by configuring mobile devices as required per VA security requirements and configuration baselines before allowing a user to access it. VA will implement minimally acceptable baseline security configuration requirements for VA GFE mobile devices in accordance with FISMA and VA Handbook 6500 rev.4. VA will configure mobile solutions based on existing/established standards. VA will leverage Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIG) when developing these threat models.

(7) VA will develop threat models for mobile devices and the resources that are accessed by such devices. VA will use threat modeling to identify security requirements and to design mobile device solutions that incorporate the controls needed to meet the security requirements. OIS, including the NSOC, and SD will collaborate to perform threat modeling. Mobile device threat models will address the following security concerns inherent in the use of mobile technology:

(a) Lack of physical controls: Devices may be used outside of VA facilities or transported from place to place within VA facilities and their mobility makes them more susceptible to loss or theft.

(b) Use of untrusted mobile devices: VA assumes that all mobile devices are susceptible to compromise (even after security controls have been applied) and will factor this susceptibility into decisions made about allowing such devices to access enterprise applications and data.

(c) Use of untrusted networks: VA has no control over non-organizational networks used for Internet access from mobile devices. VA assumes that the networks between the mobile device and the organization cannot be trusted.

(d) Use of applications created by unknown parties: VA assumes that unknown third-party mobile device applications downloadable by users should not be trusted; therefore, VA will block third-party App stores (e.g., Amazon). Applications that will send/receive/store VA PHI/PII/sensitive data must be downloaded from the VA Catalog only. The use of the approved OEM App store for applications that will not send/receive/store VA PHI/PII/sensitive data is permitted. Sideloading of applications is prohibited.

(e) Interaction with other systems: Mobile devices may have the potential to synchronize with other systems, putting VA's data at risk of being stored in an unsecured location outside of VA's control or at the risk of transmitting malware from device to device.

Users are prohibited from synchronizing mobile devices with non-VA systems. VA will use a blacklist to block cloud-based applications and applications with known vulnerabilities.

(f) Use of untrusted content: Mobile devices may use untrusted content that other types of devices generally do not encounter. VA will provide guidance to users on the risks inherent in untrusted content via the Mobile Device Rules of Behavior and discourage use.

(g) Use of location services: VA recognizes that mobile devices with location services enabled are at increased risk of targeted attacks. The information provided by these services may provide details about the user and the activities he or she performs, which may increase the risk of targeted attacks. VA may limit the use of location services.

(8) VA will make risk-based decisions about the levels of access that should be permitted from different types of mobile devices. In making these risk-based decisions, VA will consider:

(a) Sensitivity of the information or resources;

(b) Confidence in the security policy compliance of the device;

(c) Cost;

(d) Device location;

(e) Technical limitations; and

(f) Compliance with mandates and other policies.

(9) VA will periodically assess the mobile device program to confirm the organization’s mobile device policies, processes, and procedures are being followed properly.

(10) Incidents involving mobile devices should be handled as required by VA Handbook 6500 and VA Handbook 6500.2/1, *Management of Data Breaches Involving Sensitive Personal Information (SPI)*. When mobile devices are reported as lost or stolen, if the devices are connected to the network and enrolled in the mobile device management system, VA will use the centralized mobile device management system to remotely wipe all data from the device and lock the device to prevent access from anyone other than OI&T.

(11) OI&T may require users to promptly return devices to be scanned, inspected for tampering, or serviced at any time.

(12) Transmission of data to and from mobile devices over VA’s secure wireless networks is authorized and such networks should be used whenever possible.

b. Centralized Management of Mobile Devices

(1) VA will use enterprise-wide centralized mobile device management to provide consistent management, configuration, security, and continuous monitoring of VA GFE mobile devices and to ensure that mobile devices are compliant with VA’s security policies. A centralized mobile device management solution will allow VA to manage the configuration and security of mobile devices that connect to the VA network. Mobile devices must be managed

by the mobile device management system in order to access the VA network. VA's mobile device solution will provide centralized management capabilities and control over the client applications installed on each mobile device. If a mobile device is unable to be managed by the mobile device management system because the management system would interfere with the device or its applications' ability to operate as intended, the System Owner must request a risk-based decision from OIS for approval of the device to be connected to the network.

(2) VA's mobile device management system will provide the following services:

(a) General policy: The mobile device management system will enforce enterprise security policies on the device and will ensure devices are configured as described in the security baselines. The Information Owners will determine which mobile device services or features are enabled and/or accessible by their employees (e.g., location-based services, camera, Bluetooth, etc.).

1. VA must provide authorization before any VA mobile device is permitted to connect to another VA information system. The authorization must include documentation of the interface characteristics, security requirements, and the nature of information communicated. VA may perform security compliance checks on constituent components prior to the establishment of the internal connection.

2. VA prohibits the synchronization or connection of VA GFE mobile devices with non-VA owned equipment.

3. VA mobile device solutions will prohibit the remote activation of environmental scanning capabilities, such as cameras, microphones, global positioning systems, and accelerometers, unless remote activation of the features is approved in writing by the supervisor, ISO and System Owner, local CIO, or designee, and the capabilities are used only for authorized purposes. The device will be configured to provide an explicit indication when environmental scanning capabilities are in use and to provide the information collected only to authorized individuals or roles based on the mobile device management system and the specific mobile operating system.

4. VA may limit the use of location services.

5. VA will restrict use of peripherals (e.g., Bluetooth devices, USB devices, etc.) on mobile devices to limit exposure to untrusted content when possible, based on the mobile device management system and the specific mobile operating system. Users are prohibited from using peripherals unless the use is necessary to accomplish assigned tasks.

(b) Data Communication and Storage: If the devices are connected to the VA network and enrolled in the mobile device management system, VA will provide encrypted data communications between the mobile device and VA network and provide FIPS 140-2 validated encryption, or higher, of data stored on the device. VA may enforce either full-disk encryption on mobile devices, or mobile applications may provide encryption for data in storage and transmission based on the limits of the mobile operating system. The mobile device management system will be capable of remotely wiping devices storing VA information that are lost, stolen, fall into untrusted hands, or exceed the System Owner-defined number of incorrect authentication attempts, as documented in the SSP.

Removable storage must be encrypted by the device using FIPS 140-2 validated encryption or higher and be managed by the security policies of the mobile device management system.

(c) User and Device Authentication: The mobile device management system will require identification and authentication controls compliant with VA Handbook 6500 requirements. The system will implement automatic idle locks after a System Owner-defined number of minutes and will be capable of remotely locking the device if it is suspected that the device has been left in an unlocked state in an unsecured location, as documented in the SSP. The mobile device management system will enforce identification and authentication controls compliant with VA Handbook 6500 requirements.

(d) Applications: The mobile device management system will allow VA to centrally install, update, and remove applications, with acceptance dependent on the user. The mobile device management system will allow VA to remove applications managed by the mobile device management system without user input or acceptance when required. VA will use its mobile device manager to alert the user to applications that have been deemed unacceptable to VA. Once alerted, users should remove the application. If compliance is not met, the MDM can automate the removal of access features on the mobile device, severely limiting the user’s ability to leverage the device. Alerts can be customized to notify ISO staff as well for follow-up. VA has established a custom App Catalog, which is an internal App Store, to allow safe and manageable downloading of enterprise approved commercial off the shelf applications and VA-approved internal applications. The internal VA App Catalog will be the only source of VA business apps or apps that contain SPI.

(e) If a mobile device management agent is installed, the mobile device management system can be used to inventory mobile devices connected to VA’s network and identify the associated user; and use of the mobile device management system for inventory requires correct input of asset tag information when enrolling the device.

1. The network access controller (NAC) will inspect devices attempting to connect and devices that are not on the approved device list. Devices not in compliance with OI&T’s security policies or representing any threat to VA network or data will not be allowed to connect. Check-in is performed automatically between the mobile device and mobile device management system. Users are required to check-in with the mobile device management system every 48 hours to assure continued compliance and to prevent vulnerabilities.

2. Jailbroken or rooted devices are prohibited. VA’s centralized mobile device management solution will detect jailbroken and rooted mobile devices and will prohibit their use, either during enrollment or at the required check-in. If jailbroken or rooted devices are detected, VA will investigate and take action to mitigate the risk, which may include wiping the device.

c. Mobile Device Life Cycle

VA will follow a life cycle model for deploying its mobile device solutions. VA Handbook 6500.5, *Incorporating Security and Privacy in System Development Life Cycle,* identifies VA policy for incorporating security into the SDLC of VA IT systems.

(1) Initiation: VA will identify current and future mobile needs and specify requirements for performance, functionality, and security. Current and future mobile needs are identified through interactions between internal VA customers and VA's mobility teams, discussions with vendors, and tracking industry developments.

(2) Acquisition and Development: VA will determine which types of mobile device management technologies should be used and will design a solution to deploy the technologies. VA will determine requirements for architecture, device, and/or user authentication, cryptography, configuration, and application vetting and certification requirements. The security aspects of mobile device solution design should be documented in the SSP. VA should ensure the mobile device management solution and mobile devices provide OIG with the required decryption capabilities and with read-only access to all data (including logs) as required by VA Handbook 6500, Appendix F, §4p(3).

(3) Implementation and Assessment: VA will implement and test a prototype of the design before putting the solution into production. Testing should include evaluation of:

(a) Connectivity: Users are able to establish and maintain connections from the mobile device to VA and should be able to connect to all of the resources they are permitted to but should not be able to connect to any other VA resources.

(b) Protection: Information stored on the mobile device and communications between the mobile device and VA are protected in accordance with established requirements.

(c) Authentication: Authentication is required and cannot be readily compromised or circumvented. All device, user, and domain authentication policies are enforced.

(d) Applications: The applications to be supported by the mobile device solution function properly and restrictions on installing applications are enforced.

(e) Management: Administrators can configure and manage all components of the solution effectively and securely. Users are not able to alter settings.

(f) Logging: The solution logs security events in accordance with the requirements of VA Handbook 6500.

(g) Performance: All components of the solution provide adequate performance during normal and peak usage.

(h) Security of the implementation: The security of all components of the mobile device management solution will be maintained in accordance with the requirements of VA Handbook 6500.

(i) Default settings: Implementers should carefully review the default values for each mobile device setting and alter the settings as necessary to support security requirements, and should ensure that the mobile device solution does not revert to insecure default settings.

(4) Operations and Maintenance: VA will maintain mobile device security through the performance of the below actions and other actions as specified in the SSP.

(a) Managing updates and patches for mobile device solution operating systems and software components as required by VA Handbook 6500;

(b) Reconfiguring access control features as needed based on factors such as policy changes, technology changes, audit findings, and new security needs;

(c) Detecting and documenting anomalies with the mobile device infrastructure; and

(d) Providing training and awareness activities for mobile device users on threats and recommended security practices.

(5) Disposal: VA will follow the policy set forth in VA Handbook 6500.1, *Electronic Media Sanitization*, to remove VA information from a VA mobile device before the mobile device permanently leaves the organization.

This page is intentionally blank for the purpose of printing front and back copies.

Appendix A. **TERMS AND DEFINITIONS**

1. Authentication: Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system. SOURCE: NIST SP 800-53; NIST SP 800-53A; NIST SP 800-27A; FIPS 200

2. Encryption: The process of changing plain text into cipher text for the purpose of security or privacy. SOURCE: NIST SP 800-57

3. Incident: An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies. The term incident means security incident as defined in 38 U.S.C. § 5727. SOURCE: FIPS 200; NIST SP 800-53

4. Information Security Requirements: Information security requirements promulgated in accordance with law, or directed by the Secretary of Commerce, NIST, and Office of Management and Budget, and, as to national security systems, the President. SOURCE: 38 U.S.C. § 5727

5. Information System: A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information, whether automated or manual. SOURCE: 38 U.S.C. § 5727

6. Mobile Device: A portable computing device that: (i) has a small form factor such that it can easily be carried by a single individual; (ii) is designed to operate without a physical connection (e.g., wirelessly transmit or receive information); (iii) possesses local, non-removable or removable data storage; and (iv) includes a self-contained power source. Mobile devices may also include voice communication capabilities, on-board sensors that allow the devices to capture information, and/or built-in features for synchronizing local data with remote locations. Examples include smartphones, tablets, and E-readers. Mobile devices affected by this Handbook do not include laptops or cellular telephones (see 1. Purpose and Scope). SOURCE: NIST SP 800-53

7. Security Controls: The management, operational, and technical controls (e.g., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information. SOURCE: NIST SP NIST 800-53; NIST SP 800-37; NIST SP 800-53A; NIST SP 800-60; FIPS 200; FIPS 199; CNSSI-4009

8. Sensitive Personal Information (SPI): The term, with respect to an individual, means any information about the individual maintained by VA, including the following: (i) education, financial transactions, medical history, and criminal or employment history; (ii) information that can be used to distinguish or trace the individual’s identity, including name, social security number, date and place of birth, mother’s maiden name, or biometric records. SOURCE: 38 U.S.C. § 5727

9. **Sideloading:** Installing applications from a source other than the app store. SOURCE: VA-adapted

10. **System Development Life Cycle (SDLC):** The scope of activities associated with a system, encompassing the system's initiation, development and acquisition, implementation, operation and maintenance, and ultimately its disposal. SOURCE: CNSSI-4009

11. **System Security Plan (SSP):** Formal document that provides an overview of the security requirements for the information system and describes the security controls in place or planned for meeting those requirements. SOURCE: NIST SP 800-37; NIST SP 800-53; NIST SP 800-53A; NIST SP 800-18; FIPS 200

12. **Threat:** Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or Denial of Service (DOS). SOURCE: NIST SP 800-53; NIST SP 800-53A; NIST SP 800-27A; NIST SP 800-60; NIST SP 800-37; CNSSI-4009

13. **Threat Modeling:** Identifying resources of interest and the feasible threats, vulnerabilities, and security controls related to these resources, quantifying the likelihood of successful attacks and their impacts, and analyzing this information to determine where security controls need to be improved or added. SOURCE: NIST SP 800-124

14. **Unauthorized Access:** Gaining logical or physical access to VA information or information systems either without authorization or in excess of previously authorized access. SOURCE: NIST SP 800-61

15. **User:** Individual or (system) process acting on behalf of an individual authorized to access an information system. SOURCE: NIST SP 800-53; NIST SP 800-18; CNSSI-4009

16. **VA National Rules of Behavior:** A set of Department rules that describes the responsibilities and expected behavior of users of VA information systems or VA sensitive information. SOURCE: 38 U.S.C. § 5727

17. **VA Sensitive Information/Data:** All Department Information and/or data on any storage media or in any form, which 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 not only information that identifies an individual, but also includes other information whose improper use or disclosure could adversely affect the ability of an agency to accomplish its mission, proprietary information, and records about individuals requiring protection under applicable confidentiality provisions. SOURCE: 38. USC § 5727

This page is intentionally blank for the purpose of printing front and back copies

Appendix B. **ACRONYMS AND ABBREVIATIONS**

Acronym/ Abbreviation	Definition
A&A	Assessment and Authorization
CIO	Chief Information Officer
DISA	Defense Information Systems Agency
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Management Act
GFE	Government Furnished Equipment
ISO	Information Security Officer
IT	Information Technology
NIST	National Institute of Standards and Technology
NSOC	Network Security and Operations Center
OIS	Office of Information Security
OI&T	Office of Information and Technology
PHI	Personal Health Information
PII	Personally Identifiable Information
SD	Solution Delivery
SDLC	System Development Life Cycle
SP	Special Publication
SPI	Sensitive Personal Information
SSP	System Security Plan
STIG	Security Technical Implementation Guide
TRM	Technical Reference Model
U.S.C.	United States Code
VA	Department of Veterans Affairs

This page is intentionally blank for the purpose of printing front and back copies.

Appendix C. **REFERENCES**

1. Statutes and Regulations

a. 44 U.S.C. § 3541, Federal Information Security Management Act of 2002

b. 38 C.F.R. § 1.575-1.582, Safeguarding Personal Information in Department of Veterans Affairs Records

c. 38 U.S.C. §§ 5721-5728, Veterans' Benefits, Information Security

2. Federal Information Processing Standards (FIPS) Publications

a. FIPS Pub 199, Standards for Security Categorization of Federal Information and Information Systems

b. FIPS Pub 200, Minimum Security Requirements for Federal Information and Information Systems

3. National Institute of Standards and Technology (NIST) Special Publications (SP)

a. NIST SP 800-18, Guide for Developing Security Plans for Federal Information Systems

b. NIST SP 800-27A, Engineering Principles for Information Technology Security (A Baseline for Achieving Security)

c. NIST SP 800-37, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach

d. NIST SP 800-53, Security and Privacy Controls for Federal Information Systems and Organizations

e. NIST SP 800-53A, Guide for Assessing the Security Controls in Federal Information Systems and Organizations, Building Effective Security Assessment Plans

f. NIST SP 800-57, Recommendation for Key Management

g. NIST SP 800-60, Guide for Mapping Types of Information and Information Systems to Security Categories: (2 Volumes) - Volume 1: Guide Volume 2: Appendices

h. NIST SP 800-61, Computer Security Incident Handling Guide

i. NIST SP 800-66, An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule

j. NIST SP 800-124, Guidelines for Managing the Security of Mobile Devices in the Enterprise

k. NIST SP 800-164, Guidelines on Hardware-Rooted Security in Mobile Devices

4. VA Directives and Handbooks

a. VA Directive 6500, Managing Information Security Risk: VA Information Security Program

b. VA Directive 6550, Pre-Procurement Assessment for Medical Device/Systems

c. VA Handbook 6500, Risk Management Framework for VA Information Systems – Tier 3: VA Information Security Program

d. VA Handbook 6500.1, Electronic Media Sanitization

e. VA Handbook 6500.2/1, Management of Data Breaches Involving Sensitive Personal Information (SPI)

f. VA Handbook 6500.3, Assessment, Authorization, and Continuous Monitoring of VA Information Systems

g. VA Handbook 6500.5, Incorporating Security and Privacy into the System Development Life Cycle

5. Other References

a. CNSSI-4009, National Information Assurance Glossary

b. DISA Application Security and Development STIG, version 3, release 8

c. Health Insurance Portability and Accountability Act (HIPAA) Security Rule

Appendix D. **MOBILE DEVICE RULES OF BEHAVIOR**

1. **Background**

a. To use a Department of Veterans Affairs (VA)-owned mobile device, you must sign and follow the Mobile Device Rules of Behavior in addition to completing annual security awareness training and signing the VA National Rules of Behavior.

b. Mobile devices are information technology (IT) devices that:

(1) Are small and easy to carry;

(2) Designed to connect to the Internet over wireless networks;

(3) Can store data;

(4) Do not have a full desktop or laptop operating system;

(5) Have applications available through many methods;

(6) Can synchronize data from the device to another IT system; and/or

(7) Use a built-in power source to stay powered on for extended periods of time.

c. Laptops, desktops, and basic cell phones are not considered mobile devices. Examples of mobile devices are smartphones and tablets.

d. Contact your local IT staff to find out if a device is considered a mobile device.

e. Mobile devices need special protection because:

(1) They are used within and outside VA facilities. Since they are moved around, they are more likely to be lost or stolen.

(2) They are used on networks that VA has no control over and which may not be trustworthy.

(3) They use applications developed by unknown third parties who cannot be trusted.

(4) They can connect or synchronize with other systems. This puts VA data at risk of being stored on systems outside VA’s control. This also puts VA at risk of malware being sent from device to device.

2. Rules of Behavior

a. I understand, accept, and agree to the following rules for using a VA mobile device.

b. I will use only VA-approved devices, systems, software, services, and data which I am authorized to use. Also, I will follow any software licensing or copyright restrictions.

c. I will not store VA sensitive information on a VA mobile device unless I have approval from my supervisor. The local Chief Information Officer (CIO) and Information Security Officer (ISO) must also approve and document that the device meets VA security requirements. VA sensitive information stored on a VA mobile device must be encrypted.

d. I will not store the only copy of VA information on a VA mobile device.

e. I will always keep VA mobile devices safe and secure. I will use care when moving the devices around within a VA facility or taking them outside a VA facility. I must have approval from my supervisor, local CIO, and ISO to take a device outside a VA facility.

f. I will not connect personally-owned mobile devices to the VA network. I will also not use personally-owned mobile devices to store or send VA data.

g. I will not connect or synchronize a VA mobile device to other VA information systems unless I have been approved to do so.

h. I will not connect or synchronize a VA mobile device to non-VA owned information systems.

i. I understand VA will monitor my actions when I'm using the network or a VA mobile device. I have no expectation of privacy when using a VA mobile device. VA will also monitor the device to make sure that security controls stay in place.

j. I understand that VA will use a centralized system to control the security and setup of VA mobile devices. VA will secure mobile devices before allowing them to be used. VA will block access to the VA network by any mobile device that does not meet VA's security policies or is a threat to VA's network or data.

k. I understand that VA's centralized management system for mobile devices will inspect devices connecting to the VA network. VA will not allow devices to connect if they are not approved, do not meet the security policies, or are a threat to the network or data.

l. I will not try to change, avoid, or disable mobile device security controls or the setup of a mobile device. I will not try to change the operating system of the device, also known as jailbreaking or rooting a mobile device. VA's centralized management system for mobile devices will detect and prohibit jailbroken devices. VA will investigate and take action on jailbroken devices. Jailbroken devices may be wiped of all data. Wiping the device will remove all the data.

m. I will only use the mobile device features that I need to do my job. VA will disable features that I don't need to do my job. If enabled, features such as location or global positioning system (GPS) services, camera, or voice recording should be accessed only when needed to do my job. VA prohibits remote activation of such features unless approved by my supervisor, ISO, and local CIO for authorized uses.

n. I will use caution before accessing Quick Response (QR) codes with the mobile device camera. These codes cannot be trusted. I will only access such codes when needed for my job and I will only access the codes when I am aware of the source of the code and its purpose.

o. I understand VA will block access to unapproved external app stores. I will not attempt to access application stores that have been blocked by the VA.

p. I will not download or install applications from a source other than an approved app store (known as sideloading).

q. I will download applications that interact with VA systems to my mobile device only from VA's internal app store.

r. I will download applications that do not interact with VA systems from the commercial app store.

s. I will download an application only if it complies with VA security policy.

t. I will bring VA-owned mobile devices to Office of Information and Technology (OI&T) staff for maintenance, updates, incident response, scanning, or inspection promptly when asked.

u. I will tell my supervisor, ISO, and Privacy Officer immediately about unauthorized access or disclosure of VA sensitive information, lost or stolen devices, or any other suspected or identified information security incidents. When possible VA will use the centralized management system for mobile devices to lock and wipe lost or stolen mobile devices. If a device is locked, only OI&T staff will be able to access it.

v. I will tell my VA supervisor, local CIO, ISO or designee before I take a VA mobile device out of the U.S. Before I leave and when I return, VA may take actions to protect the device and VA information. I may be issued a special device with limited functions for international travel. When I return, OI&T may inspect the device or remove and reinstall of the software.

w. I will exercise a higher level of awareness in protecting mobile devices when traveling outside the U.S. I will take special care to make sure that I protect VA mobile devices. Laws and individual rights may vary by country and threats against Federal employee devices may be heightened.

x. I understand that VA prohibits access to VA's internal network from countries that pose a significant security risk. I will therefore not access VA's internal network from any foreign country designated as such unless approved by my VA supervisor, ISO, local CIO, and Information System Owner. This prohibition does not affect access to VA external web applications.

y. I will use VA's secure wireless networks for sending data. I will not send VA sensitive information over wireless technologies unless the connection or the application uses FIPS 140-2 (or its successor) validated encryption to protect the information.

z. I will log off or lock any VA mobile device or mobile application when I am no longer using it. The mobile device will lock automatically after a set number of minutes.

aa. I will take precautions, as directed by my ISO and local OI&T staff, to protect mobile devices from new threats.

bb. I will not allow other people, such as family members or friends, to use a VA mobile device issued to me.

cc. When I am using a mobile device in an uncontrolled area, like an airport, hotel, or public access work area, I must protect VA sensitive information from unauthorized disclosure. I will prevent people from seeing or hearing VA sensitive information. I will watch out for people looking over my shoulder or listening to my conversations.

dd. I will never swap or surrender VA mobile devices to anyone other than an authorized OI&T employee.

ee. I will sign for any mobile device given to me for my use and return the device when I no longer need it to do my job.

ff. I will check-in my mobile device with the centralized management system for mobile devices every 48 hours following the direction given by my local OI&T staff. This check will make sure the device stays secure.

gg. I understand that if I refuse to sign this Mobile Device Rules of Behavior then I cannot use a VA mobile device.

3. Mobile Device Rules Of Behavior Acknowledgement and Acceptance

1. I acknowledge that I have received a copy of these Mobile Device Rules of Behavior.

2. I understand, accept, and agree to follow all rules of these Mobile Device Rules of Behavior.

Print or type your full name   Signature   Date

Office Phone   Position Title