

APPENDIX D. DEPARTMENT OF VETERANS AFFAIRS NATIONAL RULES OF BEHAVIOR**1. BACKGROUND.**

a. Section 5723(b)(12) of title 38, U.S.C., requires the Assistant Secretary for Information and Technology to establish “VA National Rules of Behavior for appropriate use and protection of the information which is used to support Department missions and functions.” OMB Circular A-130, Appendix III, paragraph 3a(2)(a) requires that all Federal agencies promulgate ROB that “clearly delineate responsibilities and expected behavior of all individuals with access” to the agencies’ information and information systems, as well as to state clearly the “consequences of behavior not consistent” with the ROB. **The Department of Veterans Affairs (VA) National ROB that begins on page D-4 is required to be used throughout VA.**

b. Congress and OMB require the promulgation of ROB for two reasons. First, Congress and OMB recognize that knowledgeable users are the foundation of a successful security program. Users must understand that taking personal responsibility for the security of their computer and the VA data that it contains, or that may be accessed through it, as well as the security and protection of VA information in any form (e.g., digital, paper), are essential aspects of their job. Second, individuals must be held accountable for their use of VA information and information systems.

c. VA must achieve the Gold Standard in data security which requires that VA information and information system users protect VA information and information systems, especially the personal data of Veterans, their family members, and employees. Users must maintain a heightened and constant awareness of their responsibilities regarding the protection of VA information. The Golden Rule with respect to this aspect of VA employees’ responsibilities is to treat the personal information of others the same as they would their own.

d. Since written guidance cannot cover every contingency, authorized users are asked to go beyond the stated rules, using “due diligence” and highest ethical standards to guide their actions. Users must understand that these rules are based on Federal laws, regulations, and VA directives.

2. COVERAGE

a. ROB must be signed annually by all users of VA information systems or VA information. All users of VA information systems or VA information, other than contractors/subcontractors, must sign the VA National Rules of Behavior. Contractors/subcontractors authorized to use VA information systems or access VA information, must sign the VA Contractor ROB, as addressed in VA Handbook 6500.6. The Contractor ROB can be found as an appendix to VA Handbook 6500.6. Contractors sign the VA Contractor ROB; they do not sign the VA National ROB. All users of VA information systems or VA information must sign the appropriate ROB to indicate that they have read, understood, and agree to abide by the ROB before access is provided to the VA information system or the VA information.

b. The VA National ROB and the Contractor ROB address notice and consent issues identified by the Department of Justice and other sources. It also serves to clarify the roles of management and system administrators, as well as to provide notice of what is considered acceptable use of all VA information and information systems, VA sensitive information, and behavior of VA users.

c. The VA National ROB uses the phrase “VA sensitive information.” This phrase is defined in VA Handbook 6500, Appendix F. This definition covers all information as defined in 38 U.S.C. 5727(19), in 38 U.S.C. § 7332, and in 38 U.S.C. 5727(23). The phrase “VA sensitive information” as used in the attached VA National ROB means:

All Department data, on any storage media or in any form or format, 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 information whose improper use or disclosure could adversely affect the ability of an agency to accomplish its mission; proprietary information; records about individuals requiring protection under various confidentiality provisions such as the Privacy Act of 1974 and the HIPAA Privacy Rule; and information that can be withheld under the Freedom of Information Act.

Examples of information that could be considered VA sensitive information, depending on the specific circumstances, include the following: individually identifiable medical, benefit, and personnel information; financial; budgetary; research; quality assurance; confidential commercial; critical infrastructure; investigatory and law enforcement information; information that is confidential and privileged in litigation such as information protected by the deliberative process privilege, attorney work-product privilege, and the attorney-client privilege; and other information which, if released, could result in violation of law or harm or unfairness to any individual or group, or could adversely affect the national interest or the conduct of Federal programs.

d. The phrase “VA sensitive information” includes information entrusted to the Department.

e. The VA National ROB and the Contractor ROB are included in VA’s Security and Privacy Awareness training module located in the VA Talent Management System (TMS). Users are advised to complete their ROB electronically within the TMS system, if possible.

f. The VA National ROB and the Contractor ROB can be signed in hard copy or electronically. If signed using the hard copy method, the user should initial and date each page and provide the information requested on the last page.

g. For Other Federal Government Agency users, documentation of a signed ROB will be provided by the VA requesting official to the TMS administrator for recording in TMS.

3. RULES OF BEHAVIOR

Immediately following this section is the VA-approved National ROB that all employees as outlined above, who are users of VA information systems or VA information, are required to sign in order to obtain access to VA information systems or VA information.

DEPARTMENT OF VETERANS AFFAIRS NATIONAL RULES OF BEHAVIOR

I understand, accept, and agree to the following terms and conditions that apply to my access to, and use of, information, including U.S. Department of Veterans Affairs (VA) information or information systems.

1. GENERAL RULES OF BEHAVIOR

a. I understand that an essential aspect of my job is to take personal responsibility for the secure use of VA systems and the VA data that they contain or that may be accessed through them, as well as the security and protection of VA information in any form (e.g., digital, paper, verbal).

b. I understand that when I use any government information system, I have NO expectation of privacy in any records that I create or in my activities while accessing or using such information system.

c. I understand that authorized VA personnel may review my conduct or actions concerning VA information and information systems, and take appropriate action. Authorized VA personnel include my supervisory chain of command as well as VA system administrators and Information Security Officers (ISOs). Appropriate action may include monitoring, recording, copying, inspecting, restricting access, blocking, tracking, and disclosing information to authorized Office of Inspector General (OIG), VA, and law enforcement personnel.

d. I understand that the following actions are prohibited: unauthorized access, unauthorized uploading, unauthorized downloading, unauthorized changing, unauthorized circumventing, or unauthorized deleting of information on VA systems, modifying VA systems, unauthorized denying or granting access to VA systems, using VA resources for unauthorized use on VA systems, or otherwise misusing VA systems or resources. I also understand that attempting to engage in any of these unauthorized actions is also prohibited.

e. I understand that such unauthorized attempts or acts may result in disciplinary or other adverse action, as well as criminal or civil penalties. Depending on the severity of the violation, disciplinary or adverse action consequences may include: suspension of access privileges, reprimand, and suspension from work, demotion, or removal. Theft, conversion, or unauthorized disposal or destruction of Federal property or information may also result in criminal sanctions.

f. I understand that I have a responsibility to report suspected or identified information security incidents (security and privacy) to my VA supervisor, ISO and Privacy Officer (PO), immediately upon suspicion.

g. I understand that I have a duty to report information about actual or possible criminal violations involving VA programs, operations, facilities, contracts or information systems to my VA supervisor; Information System Owner, local Chief Information Officer (CIO), or designee; and ISO, any management official or directly to the OIG, including reporting to the OIG Hotline.

I also understand that I have a duty to immediately report to the OIG any possible criminal matters involving felonies, including crimes involving information systems.

h. I understand that the VA National Rules of Behavior (ROB) do not and should not be relied upon to create any other right or benefit, substantive or procedural, enforceable by law, by a party in litigation with the U.S. Government.

i. I understand that the VA National ROB do not supersede any policies of VA facilities and other agency components that provide higher levels of protection to VA's information or information systems. The VA National ROB provides the minimal rules with which individual users must comply.

j. I understand that if I refuse to sign this VA National ROB as required by VA policy, I will be denied access to VA information systems or VA information. Any refusal to sign the VA National ROB may have an adverse impact on my employment with the Department.

2. SPECIFIC RULES OF BEHAVIOR

a. Basic

(1) I will follow established VA information security and privacy policies and procedures.

(2) I will comply with any directions from my supervisors, VA system administrators, POs, and ISOs concerning my access to, and use of, VA information and information systems or matters covered by these ROB.

(3) I understand that I may need to sign a non-VA entity's ROB to obtain access to their system in order to conduct VA business. While using their system, I must comply with their ROB. However, I must also comply with VA's National ROB whenever I am accessing VA information systems or VA information.

(4) I may be required to acknowledge or sign additional specific or unique ROB in order to access or use specific VA systems. I understand that those specific ROB may include, but are not limited to, restrictions or prohibitions on limited personal use, special requirements for access or use of the data in that system, special requirements for the devices used to access that specific system, or special restrictions on interconnections between that system and other IT resources or systems

(5) I understand VA's system of records may contain Confidential Medical Information that relates to the diagnosis or treatment of drug abuse, alcoholism or alcohol abuse, infection with the human immunodeficiency virus (HIV), or sickle cell anemia. I will not disclose information relating to the diagnosis or treatment of drug abuse, alcoholism or alcohol abuse, HIV, or sickle cell anemia without appropriate legal authority as outlined in applicable federal laws and regulations, including 38 U.S.C. § 7332. I understand my responsibilities as outlined in 38 U.S.C. § 7332, and I understand unauthorized disclosure of this information may have a serious adverse effect on agency operations, agency assets, or individuals.

b. Data Protection

(1) I will safeguard electronic VA sensitive information at work and remotely. I understand that all VA owned mobile devices and portable storage devices must be encrypted using Federal Information Processing Standards (FIPS) 140-2, *Security Requirements for Cryptographic Modules*, validated encryption (or its successor) unless encryption is not technically possible, as determined and approved by my local ISO, CIO and the Deputy Assistant Secretary for Information Security (DAS for OIS). This includes laptops, flash drives, and other removable storage devices and storage media (e.g., Compact Discs (CD), Digital Video Discs (DVD)).

(2) I understand that per VA Directive 6609, Mailing of Sensitive Personal Information (SPI), the following types of SPI are excluded from the encryption requirement when mailed according to the requirements outlined in the directive:

(a) Information containing the SPI of a single individual to:

1. That person (e.g., the Veteran's, beneficiary's, dependent's, or employee's own information) or to his or her personal representative (e.g., guardian, attorney-in-fact, attorney, or Veteran Service Organization contact person). Such information may be mailed to an entity, not otherwise the subject of an exception, with the express written consent of the individual. Such information may be mailed via U.S. Postal Service regular mail unless tracked delivery service is requested and paid for by the recipient;

2. A business partner such as a health plan or insurance company, after reviewing potential risk;

3. A court, adjudicative body, parties in litigation, or to persons or entities in the course of a judicial or administrative proceeding; and

4. Congress, law enforcement agencies, and other governmental entities.

(b) Information containing SPI of one or more individuals when sent to a person or entity that does not have the capability of decrypting the data, provided that the mailing is approved in advance and in writing by my supervisor or ISO.

(3) I understand that I must have approval from my supervisor to use, process, transport, transmit, download, or store electronic VA sensitive information remotely (outside of VA owned or managed facilities (e.g., medical centers, community based outpatient clinics (CBOC), or regional offices)).

(4) If approved to use, process, store, or transmit electronic VA sensitive information remotely, I must ensure any device I utilize is encrypted using FIPS 140-2 (or its successor) validated encryption. VA owned and approved storage devices/media must use VA's approved configuration and security control requirements. The Information System Owner, local CIO, or designee, and ISO and PO must review and authorize the mechanisms for using,

processing, transporting, transmitting, downloading, or storing VA sensitive data outside of VA owned or managed facilities.

(5) I will ensure that all printouts of VA sensitive information that I work with, as part of my official duties, are physically secured when not in use (e.g., locked cabinet, locked door).

(6) I acknowledge that particular care should be taken to protect SPI aggregated in lists, databases, or logbooks, and will include only the minimum necessary SPI to perform a legitimate business function.

(7) I recognize that access to certain databases, whether regional-level or national-level data, such as data warehouses or registries containing patient or benefit information, and data from other Federal agencies, such as the Centers for Medicare and Medicaid or the Social Security Administration, has the potential to cause great risk to VA, its customers and employees due to the number and/or sensitivity of the records being accessed. I will act accordingly to ensure the confidentiality and security of these data commensurate with this increased potential risk.

(8) If I have been approved by my supervisor to take printouts of VA sensitive information home or to another remote location outside of a VA facility, or if I have been provided the ability to print VA sensitive information from a remote location to a location outside of a VA facility, I must ensure that the printouts are destroyed to meet VA disposal requirements when they are no longer needed and in accordance with all relevant record retention requirements. Two secure options that can be used are to utilize a cross-cut shredder that meets VA and National Institute of Standards and Technology (NIST) requirements or return the printouts to a VA facility for appropriate destruction.

(9) When in an uncontrolled environment (e.g., public access work area, airport, or hotel), I will protect against disclosure of VA sensitive information which could occur by eavesdropping, overhearing, or overlooking (shoulder surfing) from unauthorized persons. I will also follow a clear desk policy that requires me to remove VA sensitive information from view when not in use (e.g., on desks, printers, fax machines, etc.). I will also secure mobile devices and portable storage devices (e.g., laptops, Universal Serial Bus (USB) flash drives, smartphones, tablets, personal digital assistants (PDA)).

(10) I will use VA-approved encryption to encrypt any email, including attachments to the email, which contains VA sensitive information before sending the email. I will not send any email that contains VA sensitive information in an unencrypted form. I will not encrypt email that does not include VA sensitive information or any email excluded from the encryption requirement under paragraph b(2).

(11) I will not auto-forward email messages to addresses outside the VA network.

(12) I will take reasonable steps to ensure fax transmissions are sent to the appropriate destination, including double checking the fax number, confirming delivery of the fax, using a fax cover sheet with the required notification message included and only transmitting individually identifiable information via fax when no other reasonable means exist and when

someone is at the machine to receive the transmission or the receiving machine is in a secure location.

(13) I will protect VA sensitive information from unauthorized disclosure, use, modification, or destruction, and will use encryption products approved and provided by VA to protect sensitive data. I will only provide access to sensitive information to those who have a need-to-know for their professional duties, including only posting sensitive information to web-based collaboration tools restricted to those who have a need-to-know and when proper safeguards are in place for sensitive information. For questions regarding need-to-know and safeguards, I will obtain guidance from my VA supervisor, ISO, and/or Information System Owner, local CIO, or designee before providing any access.

(14) When using wireless connections for VA business I will only use VA authorized wireless connections and will not transmit VA sensitive information via wireless technologies unless the connection uses FIPS 140-2 (or its successor) validated encryption.

(15) I will properly dispose of VA sensitive information, either in hardcopy, softcopy, or electronic format, in accordance with VA policy and procedures.

(16) I will never swap or surrender VA hard drives or other storage devices to anyone other than an authorized Office of Information and Technology (OI&T) employee.

c. Logical Access Controls

(1) I will follow established procedures for requesting access to any VA computer system and for notification to the VA supervisor, ISO, and/or Information System Owner, local CIO, or designee when the access is no longer needed.

(2) I will only use passwords that meet the VA minimum requirements defined in control IA-5: Authenticator Management in VA Handbook 6500, Appendix F, including using compliant passwords for authorized web-based collaboration tools that may not enforce such requirements.

(3) I will not share my password or verify codes. I will protect my verify codes and passwords from unauthorized use and disclosure. I will not divulge a personal username, password, access code, verify code, or other access requirement to anyone.

(4) I will not store my passwords or verify codes in any file on any IT system, unless that file has been encrypted using FIPS 140-2 (or its successor) validated encryption and I am the only person who can decrypt the file. I will not hardcode credentials into scripts or programs.

(5) I will use elevated privileges (e.g., Administrator accounts), if provided for the performance of my official duties, only when such privileges are needed to carry out specifically assigned tasks which require elevated access. When performing general user responsibilities, I will use my individual user account.

d. Remote Access/Teleworking

(1) I understand that remote access is allowed from other Federal Government computers and systems to VA information systems, subject to the terms of VA and the host Federal agency's policies.

(2) I agree that I will directly connect to the VA network whenever possible. If a direct connection to the VA network is not possible, then I will use VA-approved remote access software and services. I will use VA-provided IT equipment for remote access when possible.

(3) I agree that I will not have both a VA network connection and any non-VA network connection (including a modem or phone line or wireless network card, etc.) physically connected to any computer at the same time unless the dual connection is explicitly authorized by my VA supervisor, ISO, and/or Information System Owner, local CIO, or designee.

(4) I am responsible for the security of VA property and information, regardless of my work location. VA security policies are the same and will be enforced at the same rigorous level when I telework as when I am in the office. I will keep government furnished equipment (GFE) and VA information safe, secure, and separated from my personal property and information.

(5) I will ensure that VA sensitive information, in any format, and devices, systems and/or software that contain such information are adequately secured in remote locations (e.g., at home and during travel). I agree that if I work from a remote location, pursuant to an approved telework agreement with VA sensitive information, authorized OI&T personnel may periodically inspect the remote location for compliance with security requirements.

(6) I will protect information about remote access mechanisms from unauthorized use and disclosure.

(7) I will notify my VA supervisor, ISO, and/or Information System Owner, local CIO, or designee prior to any international travel with a mobile device (laptop, PDA) so that appropriate actions can be taken prior to my departure and upon my return, including potentially issuing a specifically configured device for international travel and/or inspecting the device or reimaging the hard drive upon return.

(8) I will exercise a higher level of awareness in protecting mobile devices when traveling internationally as laws and individual rights vary by country and threats against Federal employee devices may be heightened.

(9) 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.

e. Non-VA Owned Systems

(1) I agree that I will not allow VA sensitive information to reside on non-VA systems or devices unless specifically designated and authorized in advance by my VA supervisor, ISO, and Information System Owner, local CIO, or designee. I agree that I will not access, transmit, or store remotely any VA sensitive information that is not encrypted using VA-approved encryption.

(2) I will only use VA-approved solutions for connecting non-VA-owned systems to VA's network. I will follow VA Handbook 6500 requirements for connecting any non-VA equipment to VA's network.

(3) I will not use personally-owned information systems (capable of storing data) on-site at a VA facility to directly connect to VA's network. I will not use personally-owned information systems on-site to perform assigned official duties unless approved by the Information System Owner, local CIO, or designee. I will obtain my Information System Owner, local CIO, or designee's approval prior to using remote access capabilities to connect personally-owned equipment to VA's network while within the VA facility.

f. System Security Controls

(1) I will not attempt to override, circumvent, or disable operational, technical, or management security controls unless expressly directed to do so by authorized VA staff. I will not attempt to alter the security configuration of government equipment unless authorized.

(2) I will only use virus protection software, anti-spyware, and firewall/intrusion detection software authorized by VA on VA equipment.

(3) I will not disable or degrade software programs used by VA that install security software updates to VA computer equipment, to computer equipment used to connect to VA information systems, or to create, store or use VA information.

(4) I agree to have issued GFE scanned and serviced by VA authorized personnel. This may require me to return it promptly to a VA facility upon demand.

(5) I will permit only those authorized by OI&T to perform maintenance on IT components, including installation or removal of hardware or software.

g. System Access

(1) I will use only VA-approved devices, systems, software, services, and data which I am authorized to use, including complying with any software licensing or copyright restrictions.

(2) I will only use VA-approved collaboration technologies for conducting VA business.

(3) I will not download software from the Internet, or other public available sources, offered as free trials, shareware, or other unlicensed software to a VA-owned system.

(4) I will not host, set up, administer, or operate any type of Internet server or wireless access point on any VA network unless explicitly authorized by my Information System Owner,

local CIO, or designee and approved by my ISO. I will ensure that all such activity is in compliance with Federal and VA policies.

(5) I will not attempt to probe computer systems to exploit system controls or to obtain unauthorized access to VA sensitive data.

(6) I will only use my access to VA computer systems and/or records for officially authorized and assigned duties. The use must not violate any VA policy regarding jurisdiction, restrictions, limitations or areas of responsibility.

(7) I will use my access under VA Directive 6001, *Limited Personal Use of Government Office Equipment Including Information Technology*, understanding that this Directive does not pertain to accessing VA applications or records. I will not engage in any activity that is prohibited by the Directive.

(8) I will prevent unauthorized access by another user by ensuring that I log off or lock any VA computer or console before walking away or initiate a comparable application feature that will keep others from accessing the information and resources available in my computing session.

h. Miscellaneous

(1) I will complete mandatory periodic security and privacy awareness training within designated time frames, and complete any additional role-based security training required, based on my roles and responsibilities.

(2) I will take precautions as directed by communications from my ISO and local OI&T staff to protect my computer from emerging threats.

(3) I understand that while logged into authorized Web-based collaboration tools I am a representative of VA and I will abide by the ROB and all other policies and procedures related to these tools.

(4) I will protect government property from theft, loss, destruction, or misuse. I will follow VA policies and procedures for handling Federal Government IT equipment and will sign for items provided to me for my exclusive use and return them when no longer required for VA activities.

(5) If as an Other Federal Government Agency employee, I cause any level of data breach, I understand it may result in disciplinary or other adverse action, as well as criminal or civil penalties; and I recognize that I will be required to complete VA's security and privacy awareness training as part of incident remediation measures.

3. ACKNOWLEDGEMENT AND ACCEPTANCE

- a. I acknowledge that I have received a copy of these Rules of Behavior.
- b. I understand, accept and agree to comply with all terms and conditions of these Rules of Behavior.

Print or type your full name

Signature

Date

Office Phone

Position Title