15 - **VA NATIONAL RULES OF BEHAVIOR**

Department of Veterans Affairs
VA NATIONAL RULES OF BEHAVIOR

Rules of Behavior, as required by OMB Circular A-130, Appendix A, are part of a comprehensive program to convey information security requirements. Rules of Behavior are established to delineate responsibilities and expected behavior of all individuals with access to automated information systems. These rules establish standards of behavior in recognition of the fact 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 data it contains is an essential part of their job.

General Terms and Conditions

These General Terms and Conditions 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 administration, and serves to provide notice of what is considered expected use of all VA systems and behavior of VA users.

By using a Government system, I understand that I have NO expectation of Privacy in accessing or using any VA or other Federal government information systems (IS).

By accessing any VA computer system, I consent to review and action by authorized VA staff. Authorized VA staff includes my supervisory chain for efficient operation of the workplace as well as VA systems administrators and Information Security Officers (ISOs) for protection of the VA infrastructure. This action may include monitoring, recording, copying, inspecting, restricting access, blocking, tracking, and disclosing to all authorized Office of Inspector General (OIG), VA, and law enforcement personnel.

I understand and accept that unauthorized attempts or acts to access, upload, download, change, circumvent, or delete information on VA systems; modify VA systems; deny access to VA systems; accrue resources for unauthorized use on VA systems; or otherwise misuse VA systems or resources are prohibited.

I understand that such unauthorized attempts or acts are subject to action that may result in criminal, civil, and/or administrative penalties. Applicable Federal Laws provide for criminal penalties for theft, conversion, or unauthorized disposal or destruction of Federal IT property and data assets.

I will report suspected or identified information security incidents to the VA Point-of-Contact (POC), or the VA ISO or authorities as appropriate or agreed upon.

Rules of Behavior

The following Rules of Behavior (ROB) apply to everyone (employees, volunteers, contractors, and business partners) who have access to VA Information System resource(s). Because written guidance cannot cover every contingency, personnel are asked to go beyond the stated rules, using "due diligence" and highest ethical standards to guide their actions. Personnel must understand that these rules are based on Federal laws, regulations, and VA Directives. As such, there are consequences for non-compliance with ROB. Depending on the severity of the violation, at the discretion of management and through due process of the law, consequences can include: suspension of access privileges, reprimand, suspension from work, demotion, removal, and criminal and civil penalties. Failure to sign this ROB will result in denial of access to VA information assets or resources.

The following rules apply to all VA users

As a user of the U.S. Department of Veterans Affairs (VA) information technology infrastructure I agree that I will abide by all of the following:

- To follow established procedures for requesting access to any VA computer system and for notification to the VA POC and/or ISO when the access is no longer needed,
- To follow established VA information security and privacy policies and procedures this includes the requirement to sign the ROB.
- To use only systems, software, and data which I am authorized to use, including any copyright restrictions.
- To only use my access for authorized and official duties, and to only access data that is needed in the fulfillment of my duties.
- To properly dispose of the information, either in hardcopy, softcopy or electronic format, in accordance with VA policy and procedures.
- Not attempting to override, circumvent or disable operational, technical, or management security controls unless expressly directed to do so by authorized VA staff in writing to prevent social engineering.
- Not attempting to, or alter the configuration on government equipment unless authorized; this includes operational, technical, or management security controls.
- Complying with the personal use of government equipment in accordance with Federal and local policies and procedures. This includes using VA resources only for appropriate and legal purposes. I understand that my actions are subject to monitoring.
- Protecting my verify codes and passwords from unauthorized use and disclosure and ensuring I utilize only passwords that meet the VA minimum requirements for the system authorized to use.
- Not storing any passwords/verify codes in any type of script file or cache on VA systems.

User's Initials: _____ **Date: _____**

NOTE: Individuals are responsible for initialing each page.

VA Handbook 6500, Appendix G (9/18/07)

- Ensuring that I log off or lock my assigned workstation before walking away.
- Not misrepresenting, obscuring, suppressing, or replacing a user's identity on the Internet or any VA electronic communication system.
- Refraining from copying, storing, or maintaining sensitive information on non-VA equipment or storage devices (i.e., thumb drives) without written authorization via Business Associate Agreement (BAA), Memorandum of Understanding (MOU), Interagency Security Agreement (ISA), Contract, or by the ISO or IT management.
- Ensuring that appropriate management officials have approved information for public dissemination, including e-mail communications outside of the VA as appropriate. I will not disclose any inappropriate information through the use of any means of communication including but not limited to e-mail, instant messaging, online chat, web bulletin board, logs or list servers.
- Not to host, set up, administer, or operate any type of Internet server on any VA network or attempt to connect any personal equipment to a VA network unless explicitly authorized in writing and in compliance with Federal and VA policies.
- No attempt will be made to probe computer systems in obtaining information on either TCP/UDP open or closed ports or activate computer commands that involve net stat, ping or trace route. Participation in Telnet and FTP sessions must be approved in writing by VA staff.
- Protecting Government property from theft, destruction, or misuse. I will follow VA policies and procedures for handling Federal Government IT equipment.
- Only use virus protection software, anti-spyware, and firewall/intrusion detection software authorized by the VA on VA equipment or on computer systems that are connecting to any VA network, and ensure software is maintained with current patches and updates.

Not disable or degrade tools used by the VA that install security software updates to computer equipment.

- Agreeing to have all equipment scanned by the appropriate VA IT Operations staff prior to connecting to the VA network if the equipment has not been connected to the VA network for a period of more than three weeks.
- Complete mandatory periodic security and privacy awareness training within designated timeframes, and complete any additional required training for the particular systems to which I require access.

Additional conditions for use of non-VA information technology resources

These conditions apply to my access to or use of non-VA information technology resources as a VA user. I agree that I may be restricted by the non-VA entity that controls the system or data I am attempting to use. I agree that I may have to sign the user agreement or rules of behavior of the non-VA entity, if required.

Additional conditions for remote access users, including access from home or other non-VA locations/networks

- Remote access is allowed from other Federal government computers and systems, subject to the terms of VA and the host Federal agency's policies.
- VA users will directly connect to the VA network whenever possible. If a direct connection to the VA network is not possible, then VA users will use VA-approved remote access software and services. VA users must use VA-provided IT equipment for remote access when possible. VA users may be permitted to use personally-owned IT equipment upon approval, but must follow all VA security policies and requirements.
- Users will not have both a VA network line and any kind of non-VA network line (including a modem or phone line or wireless network card, laser, infrared) physically connected to any computer at the same time unless the dual connection is explicitly authorized in writing.
- I will review and follow VA Directive 6504, Restrictions On Transmission, Transportation and Use of and Access to, VA Data Outside VA Facilities for protecting VA Information assets while using them in uncontrolled environments. I agree to conform to the requirements/direction provided to me by this Directive.
- I am responsible for ensuring that any VA sensitive information I may be accessing or storing remotely is secured and transmitted using VA approved encryption.

Additional conditions for installation or use of encryption

I will protect sensitive information from unauthorized disclosure, use, modification, or destruction, including using encryption products approved and provided by the VA to protect sensitive data. I will follow the instructions and terms for using any VA-provided encryption. I will only use encryption products as explicitly authorized by the VA. Sensitive data, including but not limited to identifiable patient information, will not be sent via Outlook mail unless VA-provided encryption is used.

Additional conditions for access to or use of specific VA systems

I agree that I may be required to acknowledge or sign the specific or unique rules of behavior that apply to specific VA systems. Those specific rules of behavior 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.

User's Initials: _____ Date: _____
NOTE: Individuals are responsible for initialing each page.

VA Handbook 6500, Appendix G (9/18/07)

Additional conditions for Contractors

Contractors are strictly limited to system or data access to fulfill the terms of the contract. Limited personal use must be explicitly authorized in the terms of the contract. Upon resignation, termination or completion of the contract, all contractor equipment used to store VA data will be sanitized to VA standards by the VA ISO or VA IT Operations staff.

Statement on Litigation

Rules of Behavior do not and should not be relied upon to create any other right or benefit, substantive or procedural, enforceable by law, by a party to litigation with the United States Government.

Acknowledgement and Acceptance

I acknowledge receipt of the Rules of Behavior (ROB). I understand and accept all terms and conditions of this document, and I will comply with the terms and conditions of this and any additional VA warning banners, system rules of behavior, policies, procedures, notices, or directives regarding access to or use of VA data, information systems or resources. This document is not meant to supersede any local directives that provide higher levels of protection to VA's information or assets. ROB provides for the minimal level of protections that individual users must employ. Access to VA information systems and resources will not be granted to individuals that do not acknowledge and agree to comply with ROB.

_____ _____
[Print or type your full name] Signature

_____
Date

_____ _____
Office Phone Position Title

_____ _____
(Company Name for Contractors)