DEPARTMENT OF VETERANS AFFAIRS (VA)
INFORMATION SECURITY RULES OF BEHAVIOR (ROB)
FOR NON-ORGANIZATIONAL USERS

1. COVERAGE

a. *VA Information Security Rules of Behavior for Non-Organizational Users* identifies the specific responsibilities and expected behavior for non-organizational users of VA information and information systems as required by 38 U.S.C. § 5723(f)(5), Office of Management and Budget Circular A-130, Appendix I, paragraph 4(h) (6-7), VA Directive 6500, VA Cybersecurity Program and VA Handbook 6500, *Risk Management Framework for VA Information Systems – VA Information Security Program*.

b. *Non-organizational users* are users other than users explicitly categorized as organizational users. These include affiliates and individuals with a Veteran/claimant power of attorney. Change Management Agents at the local facility are responsible for onboarding power of attorney/private attorneys.

c. *Organizational users* are VA employees, contractors, researchers, students, trainees, volunteers, and representatives of Federal, state, local, or tribal agencies authorized to access VA information and information systems for the performance of official duties, but do not represent a Veteran or claimant. The ROB for organizational users is identified in VA's Information Security Rules of Behavior for Organizational Users.

d. VA information is the information under the control of the VA or stored on a VA information system. This includes both VA-sensitive and non-sensitive information. Information properly disclosed by the VA to a non-organizational user (for example, contents of a Veteran's claims file for purposes of representing a Veteran or claimant) is no longer VA information and its security and confidentiality are the recipient's responsibility.

e. This ROB for Non-Organizational Users does not supersede any policies of VA facilities or other agency components that provide higher levels of protection to VA's information or information systems. The ROB provides the minimum requirements with which individual users of VA information and information systems agree to comply and VA facilities and other agency components may issue requirements for protection that exceed this ROB.

2. COMPLIANCE

a. Non-Organizational Users are required to comply with this ROB. Non-compliance with this ROB may result in suspension or removal of access to VA information or information systems. Although such a suspension would not prevent the VA from making an authorized disclosure of records to a non-organizational user; a

Initial_____ Date_____

suspension of access may prevent disclosure through a particular method, for example, through a VA information system. Depending on the severity of the violation and management discretion, consequences may include access restriction or suspension of access privileges. Theft, conversion, or unauthorized disclosure or disposal of Federal property or disclosure of information may result in civil or criminal penalties.

b. Unauthorized access, upload, download, change, transmission, or deletion of information on VA systems without authorization; unauthorized modification of VA systems; denying or granting access to VA systems without authorization; unauthorized purpose on VA systems; or otherwise, misusing VA systems or resources is strictly prohibited and may result in civil or criminal penalties.

c. This ROB does not create any other right or benefit (substantive or procedural) enforceable by law by a party in litigation with the Government.

3. ACKNOWLEDGEMENT

a. Non-organizational users must sign this ROB before access is provided to VA information and information systems. This ROB must be signed annually by all non-organizational users of the VA information or information systems. This signature indicates agreement to comply with this ROB and refusal to sign this ROB will result in denied access to VA information or information systems.

b. This ROB may be signed in hard copy or electronically. If signed using the hard copy method, the user must initial and date each page and provide the information requested under Acknowledgement and Acceptance.

4. INFORMATION SECURITY RULES OF BEHAVIOR

Access and Use of VA Information and Information Systems

I Will:

- Comply with all Federal statutes, regulations, and policies applicable to VA information security, information privacy/disclosure, and records management policies.

- Follow established procedures for requesting access to VA information or an information system and notifying the VA when the access is no longer needed.

- Only use VA-approved solutions, software, or services for connecting non-VA-owned systems to the VA's network remotely or directly.

- Log off or lock any computer or console with access to or displaying VA information before I leave my workstation.

- Only use my access to VA information and information systems for officially authorized and assigned duties. The use of VA information and information systems must not violate any VA policy regarding jurisdiction, restrictions, limitations, or areas of responsibility.

I Will Not:

- Have any expectation of privacy in my activities while accessing or using VA information systems, as I understand that all activity is logged for security purposes.

- Attempt to probe computer systems to exploit system controls or to obtain unauthorized access to VA sensitive information.

- Use personally owned equipment on-site at a VA facility to directly connect to the VA network or remotely to the VA network unless approved before use.

- Copy in any manner or use any technology (such as a mobile device) to copy or otherwise create unauthorized copies of VA information to which I do not have lawful access.

- Connect information systems to the VA network or engage in sending VA sensitive data outside the VA network without ensuring the system has the authority to operate decisions provided by a VA Authorizing Official.

Protection of VA-Issued Devices

I Will:

- Protect Government-furnished equipment (GFE) from theft, loss, destruction, misuse, and threats.

- Follow VA policies and procedures for handling Federal Government IT equipment and sign for items provided to me and return them when no longer required for VA activities.

I Will Not:

- Have any expectation of privacy regarding my use of any GFE. I understand that VA may monitor, intercept, search, and/or seize GFE I have been provided without notice or consent.

Initial_____ Date_____

- Swap or surrender VA hard drives or other storage devices to anyone other than an authorized Office of Information and Technology (OIT) employee.

- Attempt to override, circumvent, alter, or disable operational, technical, or management security configuration controls unless expressly directed to do so by authorized VA staff.

Data Protection

I Will:

- If authorized to connect to a VA system, only use virus protection software, anti-spyware and firewall/intrusion detection software authorized by VA.

I Will Not:

- Download or install prohibited software from the internet or other publicly available sources, offered as free trials, shareware, or other unlicensed software to a VA-owned system.

- Disable or degrade software programs used by VA that install security software updates on computer equipment and all electronic devices used to connect to VA information systems or used to create, store, or use VA information.

- Transmit VA sensitive information via wireless technologies unless the connection uses Federal Information Processing Standards (FIPS) 140-2 (or its successor) validated encryption and is properly authorized to release the data.

- Use unauthorized or unapproved cloud-based software as a service (SaaS) or emerging technologies, including Artificial Intelligence (AI).

Remote Access

I Will:

- Keep VA information safe, secure, and separated from my personal property and information.

- Protect VA information from theft, loss, destruction, misuse, and emerging threats.

- Obtain approval before using remote access capabilities to connect non-GFE devices to VA's network.

- Provide authorized VA personnel access to inspect the remote location when approved remote access to VA information and information systems includes access to VA sensitive information.

- Protect information about remote access mechanisms from unauthorized use and disclosure.

I Will Not:

- Access non-public VA information systems from publicly available computers, such as remotely connecting to the internal VA network from computers in a public library.

- Access any internal VA information system from any foreign country unless all appropriate approvals have been obtained in writing.

- Access VA's internal network from any foreign country designated as a security risk unless all appropriate approvals have been obtained in writing. This prohibition does not affect access to VA external web applications.

User Accountability

I Will:

- Complete mandatory security and privacy awareness training within designated time frames.

- Complete any additional role-based security training required based on my roles and responsibilities.

- Understand that authorized VA personnel may review my conduct or actions concerning VA information and information systems and take appropriate action.

- If applicable, have my GFE scanned and serviced by VA-authorized personnel; this may require me to return it promptly to a VA facility upon request.

- Permit only those authorized by OIT to perform maintenance on GFE or VA IT components, including installation or removal of hardware or software.

- Sign specific VA Information Security ROBs required for access or use of specific VA or non-VA systems.

Initial_____ Date_____

Sensitive Information

I Will Not:

- Access information protected by federal privacy statutes or regulations unless I have a need for the information to accomplish the purpose for which access was granted. Further, I will not use or disclose such information without appropriate legal authority.

Identification and Authentication

I Will:

- Use passwords that meet the VA minimum requirements.

- Protect my passwords, verification codes, tokens, and credentials to prevent unauthorized use and disclosure.

- Turn in my VA credential or PIV card when it is expired or the reason for VA having issued it to me has ended.

I Will Not:

- Store my VA passwords or verify codes in any format 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.

- Hardcode credentials into scripts or programs.

- Divulge a personal username, password, access code, verify code, or other access credentials to anyone.

- Share my credential personal identification number with any other individual.

- Keep my VA credential or PIV card once it has expired or the purpose for VA having issued it to me has ended.

Incident Reporting

I Will:

- Report suspected or identified information security incidents, including loss or theft of GFE, unauthorized disclosures of VA information, or unauthorized access to a VA information system, as well as anti-virus, antispyware, firewall, or intrusion detection software errors or significant alert messages (security and

privacy) on VA information systems to the Enterprise Service Desk immediately or as soon as reasonably feasible.

Social Media and Networking for Officially Authorized VA Purposes

***I Will*:**

- Use the VA Intranet when using social media/networking sites for officially authorized VA purposes.
- Use web-based collaboration and social media tools in accordance with VA Directive 6515, Use of Web-Based Collaboration Technologies.
- Limit the personal use of social media/networking sites on GFE in accordance with VA Directive 6001, Limited Personal Use of Government Office Equipment Including Information Technology.
- Ensure that my use of social media for officially authorized VA purposes complies with VA Handbook 8502, Use of Social Media.
- Only post and use content in accordance with applicable ethics, intellectual property, records, and privacy laws, regulations, and policies.
- Use only instant messaging services approved by the VA when using VA-furnished equipment.

***I Will Not*:**

- Post VA information protected by the Privacy Act of 1974; 38 U.S.C. §§ 5701, 5705 or 7332; the Health Insurance Portability and Accountability Act (HIPAA) Rules; or VA policy on non-VA websites; without legal authority and prior approval by an authorized VA official.
- Indicate that I represent VA unless officially authorized to do so.
- Publish personal views in blogs, wikis, or any other form of user-generated media while conducting officially authorized VA business.

Identification of Persona and Branding

I Will:

- Use display names and branding that are professional, appropriate for the context and align with VA values and mission.

Initial_____ Date_____

- Be aware that display names and branding may be visible to external audiences and act accordingly to represent VA positively.

- Follow VA policies and guidelines regarding online identification and branding that may require alignment with specific branding or naming conventions.

- Be reminded that VA reserves the right to take disciplinary action if display names or branding are found inappropriate, misleading, or damaging to its reputation.

I Will Not:

- Use controversial or polarizing display names or branding that could negatively affect VA or create conflicts.

- Use display names and branding that contain offensive language, can be perceived as discriminatory content or, misrepresents one's identity.

- Use display names and branding that contain personal or sensitive information.

- Use graphical elements in place of names, such as logos, photographs, or custom illustrations that do not meet VA branding guidelines and that are not part of the va.gov design system.

5. ACKNOWLEDGEMENT AND ACCEPTANCE

a. I acknowledge that I have received a copy of the *VA Information Security ROB for Non-Organizational Users*.

b. I understand, accept, and agree to comply with all terms and conditions of the *VA Information Security ROB for Non-Organizational Users*.

c. I will provide a supervisor or appropriate designee a signed copy of this document promptly to ensure awareness and compliance.

d. These provisions are consistent with and do not supersede, conflict with, or otherwise alter any applicable obligations, rights, or liabilities created by existing statute or Executive order relating to (1) classified information; (2) communications to Congress; (3) the reporting to an Inspector General of a violation of any law, rule, or regulation or mismanagement, a gross waste of funds, an abuse of authority or a substantial and specific danger to public health or safety; or (4) any other whistleblower protection. The definitions, requirements, obligations, rights, sanctions, and liabilities created by applicable Executive Orders and statutory provisions are incorporated into this agreement and control.

Print or type your full name **Signature** **Date**

_____ _____ _____

Office Phone _____ **Position Title** _____

Initial_____ Date_____