Appendix A: Organizational Rules of Behavior

DEPARTMENT OF VETERANS AFFAIRS (VA) INFORMATION SECURITY RULES OF BEHAVIOR (ROB) FOR ORGANIZATIONAL USERS (FY) 2025

1. COVERAGE

A. This *Department of Veterans Affairs (VA)) Information Security Rules of Behavior (ROB) for Organizational Users* document identifies the specific responsibilities and expected behavior for 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 4h (6-7), VA Directive 6500, *VA Cybersecurity Program* and VA Handbook 6500, *Risk Management Framework for VA Information Systems – VA Information Security Program*.

B. *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.

C. *Non-organizational users* are personnel not explicitly categorized as organizational users. The ROB for non-organizational users are identified in VA's *Information Security ROB for Non-Organizational Users* document. These include affiliates and individuals with a Veteran/claimant power of attorney.

D. The ROB provides the minimum requirements that organizational users of VA information and information systems must comply with and 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. Organizational users may exceed these minimum requirements to protect VA information and information systems when appropriate by exercising due diligence and ethical standards.

2. COMPLIANCE

A. Organizational users are required to comply with the ROB. Non-compliance with the ROB may be cause for restricting access to VA information or information systems, suspension of access privileges, and disciplinary or adverse actions up to removal. Theft, conversion or unauthorized disclosure or disposal of Federal property or information may result in civil or criminal penalties.

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

C. The ROB does not create any other rights or benefit (substantive or procedural) enforceable by law by a party in litigation with the Government.

3. ACKNOWLEDGEMENT

A. Organizational users must sign the *ROB for Organizational Users* before access is provided to VA information and information systems. This *ROB for Organizational Users* must be signed annually by all VA information and information systems users. This signature acknowledges agreement to comply with the ROB and refusal to sign this ROB will result in denied access to VA information and information systems. Any refusal to sign the *ROB for Organizational Users* may result in disciplinary or adverse action.

B. The *ROB for Organizational Users* may 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 under the Acknowledgement and Acceptance section found at the end of this document. For other Federal, state, local and tribal agency users, documentation of a signed VA Information Security ROB will be provided to the VA requesting official.

_____
Initials

4. INFORMATION SECURITY ROB

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.
- Use only VA-approved devices, systems, software, services, and data that I am authorized to use, including complying with any software licensing or copyright restrictions.
- Follow established procedures for requesting access to any VA computer system and notifying my VA supervisor or designee when the access is no longer needed.
- Only use my access to VA information and information systems for officially authorized purposes to which I have legal authority and VA approval. The use of VA information and information systems must not violate any VA policy regarding jurisdiction, restrictions, limitations, or areas of responsibility.
- Log out of all information systems and lock any VA computer or console before leaving my workstation and at the end of each workday whether at a VA location or alternate worksite.
- Only use other Federal Government information systems as expressly authorized by the terms of those systems; personal use is limited by VA standards.
- Only use VA-approved solutions for connecting non-VA-owned systems to the VA's network.

_____
Initials

I Will Not:

- Have any expectation of privacy in any information I access, create, receive, or maintain, or in my activities while accessing or using VA information systems, as I understand that all activity is logged for security purposes.
- 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.
- Attempt to probe computer systems to exploit system controls or to obtain unauthorized access to VA systems or information.
- Engage in any activity prohibited by VA Directive 6001, *Limited Personal Use of Government Office Equipment Including Information Technology*.
- Connect information systems to the VA network or engage in sending VA sensitive data outside the VA network without ensuring the system has an Authority to Operate (ATO) approved by a VA Authorizing Official.
- Have a VA network connection and a non-VA network connection, such as a modem or phone line or wireless network card, physically connected to any device at the same time unless the dual connection is explicitly authorized by my Information System Owner and local Area Manager (AM) or designee.
- Host, set up, administer, or operate any internet server or wireless access point on any VA network unless explicitly authorized by my Information System Owner and AM or designee.

Protection of VA-Issued Devices

I Will:

- Secure VA-issued devices (e.g., laptops, tablets, smartphones) and portable storage devices (e.g., compact discs, digital video discs, universal serial bus (USB) flash drives).
- Protect VA-issued devices from theft, loss, destruction, misuse, and threats.

I Will Not:

- Swap or surrender VA hard drives or other storage devices to anyone other than an authorized Office of Information and Technology (OIT) employee or when instructed by a VA law enforcement official.
- Attempt to override, circumvent, alter, or disable security configuration controls unless expressly directed to do so by authorized VA staff.

Data Protection

I Will:

- Only use virus protection software, anti-spyware and firewall/intrusion detection software authorized by VA.
- Safeguard VA mobile devices and portable storage devices containing VA information, at work, remotely, and while in transit.
- Only use VA-owned or approved storage devices encrypted with Federal Information Processing Standards (FIPS) 140-2 (or its successor) validated encryption, consistent with VA's approved configuration and security control requirements to perform VA work.
- Use VA email in the performance of my duties when issued a VA email account.
- Only disseminate VA information to the public when authorized to do so and in the performance of my duties.

I Will Not:

- Transmit VA sensitive information via wireless technologies unless the connection uses FIPS 140-2 (or its successor) validated encryption and is properly authorized to release the data.
- Auto-forward email messages or forward phone calls outside the VA network.
- Download 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 used to connect to VA information systems or used to create, store, or use VA information.
- Use unauthorized or unapproved cloud-based software as a service (SaaS) or emerging technologies, including Artificial Intelligence (AI).

Teleworking and Remote Access

I Will:

- Keep Government-furnished equipment (GFE) and VA information safe, secure, and separated from my personal property and information, regardless of work location.
- Obtain approval prior to using remote access capabilities to connect non-GFE devices to VA's network.
- Secure all appropriate approvals prior to any international telework with a VA mobile device so that appropriate actions can be taken prior to my departure and upon my return, including potentially issuing a specifically configured device for international telework and/or inspecting the device or reimaging the hard drive upon return.
- Comply with any security measures, including using a specifically configured device issued for international travel and surrendering the device for inspection or reimaging.
- Safeguard electronic and physical VA sensitive information while working at home or during travel.
- Provide VA authorized personnel access to inspect the remote location as allowed and included in an approved VA telework agreement.
- Protect information about remote access mechanisms from unauthorized use and disclosure.
- Exercise a higher level of awareness in protecting GFE mobile devices when traveling internationally as laws and individual rights vary by country and threats against Federal employee devices may be heightened.

I Will Not:

- Access non-public VA information technology (IT) resources from publicly available IT 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 and complete any additional role-based security training required for 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.
- Have my GFE scanned and serviced by VA authorized personnel. This may require me to return it promptly to a VA facility upon demand.
- Permit only those authorized by OIT to perform maintenance on IT components, including installation or removal of hardware or software.
- Sign VA Information Security ROBs required for access or use of specific VA systems.
- Comply with any requirement to sign a non-VA entity's ROB to conduct VA business.

Sensitive Information

I Will:

- Access VA sensitive information only if I have a need for the information to accomplish officially authorized and assigned duties.
- Ensure responsible practices whenever Veteran data is accessed or used in accordance with VA policy and guidance.
- Ensure that all printed material containing VA sensitive information is physically secured when not in use (e.g., locked cabinet, locked door).
- Only provide access to VA sensitive information to those whom I verify have a need-to-know of this information for their official duties.
- Only post sensitive information to web-based collaboration tools restricted to those who have a need-to-know and when proper safeguards are in place.
- Recognize that access to certain databases 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.
- Act accordingly to ensure the confidentiality and security of sensitive records in a database is commensurate with the increased potential risk.
- Obtain approval from my supervisor to use, process, transport, transmit, download, print or store VA sensitive information remotely (outside of VA-owned or managed facilities (e.g., medical centers, Community-Based Outpatient Clinics, or Regional Offices)).
- Protect VA sensitive information from unauthorized disclosure, use, modification, or destruction and use encryption products approved and provided by VA to protect sensitive data.

I Will (Continued)

- Transmit VA sensitive information via fax only when no other reasonable means exist and when either someone is at the receiving machine to receive the transmission, or the receiving machine is in a secure location.
- Encrypt email, including attachments, that contain VA sensitive information.
- Protect VA sensitive information aggregated in lists, databases or logbooks and include only the minimum necessary VA sensitive information to perform a legitimate business function.
- Ensure fax transmissions are sent to the appropriate destination. This includes double-checking the fax number, confirming delivery, and using a fax cover sheet with the required notification message.

I Will Not:

- Access VA sensitive information out of curiosity or concern, or for any purpose that is not direct related to officially authorized and assigned duties.
- Encrypt emails that do not include VA-sensitive information, or any email excluded from the encryption requirement.
- Disclose information protected by VA's privacy statutes or regulations without appropriate legal authority. Unauthorized disclosure of this information may have an adverse effect on agency operations, agency assets and individuals, including myself.
- Allow VA sensitive information to reside on non-VA systems or devices unless designated and authorized in advance by all appropriate individuals, including my VA supervisor and Information System Owner.
- Make unauthorized disclosure of VA sensitive information through any means of communication, including but not limited to, verbal communications, email, text messaging, instant messaging, online chat, social media, websites, and collaboration tools/platforms.
- 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; verify codes, tokens and credentials from unauthorized use and disclosure.
- Maintain possession and display my VA credentials as required by VA policy.

I Will Not:

- Store my passwords or verify codes in any format on an IT system, unless it 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 on an IT system.
- Divulge a personal username, password, access code, verification code or other access credentials to anyone.

Incident Reporting

I Will:

- Report suspected or identified information security incidents, including unauthorized disclosures of VA information, or 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) to my VA supervisor and the Enterprise Service Desk immediately or as soon as reasonably feasible.

Social Media & Networking to Conduct Official VA Business

I Will:

- Use the VA intranet to conduct VA business on social media/networking sites wherever possible, while ensuring that my use of social media to conduct VA business complies with law, guidance, and VA policy.
- 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, in accordance with VA Directive 6001, *Limited Personal use of Government Office Equipment Including Information Technology*.
- Obtain approval from the Office of Public and Intergovernmental Affairs before establishing a VA social media account.
- In my capacity as a VA representative, post only information about which I have actual knowledge.
- Ensure that my use of social media for officially authorized VA purposes complies VA Handbook 8502, Use of Social Media, 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 VA.

_____
Initials

I Will Not:

- Comment on VA mission-related legal matters unless I am the VA official spokesperson for the matter and have management approval to do so.
- Comment or provide information on any matter I do not have actual, up-to-date knowledge in my capacity as a VA representative.
- 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 Rules; or against VA policy on any non-VA websites, without legal authority and prior approval by an authorized official.
- Use profanity, make libelous statements, make threats, or use privately created works without the express, written permission of the author.
- Quote more than short excerpts of another person's work unless the source is properly credited.
- Publish personal views in blogs, wikis, or any other form of user-generated media while conducting officially authorized VA business.

Identification Persona and Branding

I Will:

- Use display names and branding that are professional, appropriate for the context, and align with VA values and mission.
- Be aware that display names and branding may be visible to external audiences and act accordingly to represent VA positively.
- Follow the Department of Veterans Affairs Email Signature Block and Microsoft Office 365 Profile Picture Guidance.
- 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 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.
- Use controversial or polarizing display names or branding that could negatively affect VA or create conflicts.
- Use display names and branding that contains offensive language, can be perceived as discriminatory content or, misrepresents one's identity.
- Use display names and branding that contain personal or sensitive information.

5. ACKNOWLEDGEMENT AND ACCEPTANCE

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

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

C. I will provide a supervisor or appropriate designee a signed copy of this document in a timely manner to ensure awareness and compliance.

D. These provisions are consistent with and do not supersede, conflict with, or otherwise alter the employee 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 controlling Executive Orders and statutory provisions are incorporated into this agreement and control.

Print or type your full name: _____

Signature: _____

Date: _____

Office Phone: _____

Position/Title: _____