Appendix A: Department of Veterans Affairs Information Security Rules of Behavior For Organizational Users

1. COVERAGE

a. This Department of Veterans Affairs (VA) Information Security Rules of Behavior (ROB) identifies the specific responsibilities and expected behavior for organizational users of VA systems and VA information and information systems as required by OMB Circular A-130, Appendix I, paragraph 4h (6-7) and VA Directive 6500, *VA Cybersecurity Program*.

b. *Organizational users* are VA employees, contractors, researchers, students, volunteers, and representatives of Federal, state, local or tribal agencies who are authorized to access VA information and information systems but do not represent a Veteran or claimant.

c. *Non-organizational users* are users other than users explicitly categorized as organizational users. These include individuals with a Veteran/claimant power of attorney. Change Management Agents at the local facility are responsible for on-boarding power of attorney/private attorneys. The rules of behavior for Non-Organizational Users are identified in the Department of Veterans Affairs Information Security Rules of Behavior for Non-Organizational Users.

d. The ROB provides the minimum requirements with which users -of VA information and information systems must comply and does not supersede any policies of VA facilities or other agency components that provide higher levels of protection to certain information or information systems. When appropriate, users may exceed these minimum requirements to protect VA information and information systems by exercising due diligence and ethical standards.

2. COMPLIANCE

a. Non-compliance with the ROB may be cause for disciplinary actions. Depending on the severity of the violation and management discretion, consequences may include restricting access, suspension of access privileges, reprimand, demotion and suspension from work. Theft, conversion, or unauthorized disposal or destruction of Federal property or information may result in criminal sanctions.

b. Unauthorized access, upload, download, change, circumvention, or deletion of information on VA systems; unauthorized modification VA systems, denying or granting access to VA systems; unauthorized use on VA systems; or otherwise misusing VA systems or resources is strictly prohibited.

_____

Initials

c. The ROB does not create any other right or benefit, substantive or procedural, enforceable by law, by a party in litigation with the U.S. Government.

3. ACKNOWLEDGEMENT

a. The ROB must be signed before access is provided to a new user of VA information and information systems. Thereafter, the VA ROB must be signed annually by all users of VA information and information systems. This signature indicates agreement to comply with the ROB, and refusal to sign VA Information Security ROB will result in denied access to VA information and information systems. Any refusal to sign the VA Information Security ROB may have an adverse impact on employment with VA.

b. The ROB 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 Acknowledgement and Acceptance. For other Federal, state, local, and tribal agency users, documentation of a signed ROB will be provided to the VA requesting official.

4. INFORMATION SECURITY RULES OF BEHAVIOR

Access and Use of VA Information Systems

I Will:

- Comply with all federal VA information security, privacy, and records management policies.
- Have NO expectation of privacy in any records that I create or receive, or in my activities while accessing or using VA information systems.
- 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 for 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 and assigned duties.
- Log out of all information systems at the end of each workday.
- Log off or lock any VA computer or console leaving my workstation.
- Only use other Federal government information systems as expressly authorized by the terms of those systems; personal use is prohibited.
- Only use VA-approved solutions for connecting non-VA-owned systems to VA's network.

_____

Initials

I Will Not:

- Attempt to probe computer systems to exploit system controls or to obtain unauthorized access to VA sensitive information.
- Engage in any activity that is prohibited by VA Directive 6001, Limited Personal Use of Government Office Equipment Including Information Technology.
- 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.
- 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 Area Manager (AM) or designee, and approved by my Information System Security Officer (ISSO).

Protection of VA-Issued Devices

I Will:

- Secure mobile devices (e.g., laptops, tablets, smartphones) and portable storage devices (e.g., compact discs (CD), digital video discs (DVD), universal serial bus (USB) flash drives.

I Will Not:

- Swap or surrender VA hard drives or other storage devices to anyone other than an authorized 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:

- 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 and remotely, using FIPS 140-3 validated encryption (or its successor) unless it is not technically possible.
- Only use VA-owned or approved storage devices encrypted with FIPS 140-3 (or its successor) validated encryption, consistent with VA's approved configuration and security control requirements to perform VA work.

_____

Initials

- Use VA e-mail in the performance of my duties when issued a VA email account.
- Only use non-VA email when use of a non-VA email account is unavoidable.
- Only disseminate VA information to the public via e-mail 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 140-3 (or its successor) validated encryption.
- Auto-forward e-mail messages to addresses outside the VA network.
- Download software from the Internet, or other public 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.

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. I will protect GFE from theft, loss, destruction, misuse, and emerging threats.
- Obtain approval prior to using remote access capabilities to connect non-GFE devices to VA's network.
- Notify my VA supervisor or designee prior to and upon return from any international travel with a GFE mobile device (e.g. laptop, smartphone) and comply with any security measures, including using a specifically configured device issued for international travel and/or surrendering the device for inspection or reimaging.
- Safeguard VA sensitive information, in any format, device, system and/or software in remote locations (e.g., at home and during travel).
- Provide authorized OIT personnel access to inspect the remote location pursuant to an approved telework agreement that includes access to VA sensitive information.
- 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.

_____

Initials

I Will Not:

- Access non-public VA information technology resources from publicly-available IT computers, such as remotely connecting to the internal VA network from computers in a public library.
- Access VA's internal network from any foreign country designated as posing a significant threat unless approved by my VA supervisor, ISSO, local AM, and Information System Owner. 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 role 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 specific ROBs as required for access or use of specific VA systems. I may be required to comply with a non-VA entity's ROB to conduct VA business. While using their system, I must comply with their ROB.

Sensitive Information

I Will:

- 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 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.
- 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. I will act accordingly to ensure the confidentiality and security of these data commensurate with this increased potential risk.

_____

Initials

- Obtain approval from my supervisor to use, process, transport, transmit, download, print 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)).
- 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.
- 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. I will not encrypt email that does not include VA sensitive information, or any email excluded from the encryption requirement.
- Protect VA sensitive information aggregated in lists, databases, or logbooks, and include only the minimum necessary SPI 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 included.

I Will Not:

- Disclose any information protected by any of VA's privacy statutes or regulations without appropriate legal authority. I understand unauthorized disclosure of this information may have a serious adverse effect on agency operations, agency assets, and individuals.
- Allow VA sensitive information to reside on non-VA systems or devices unless specifically designated and authorized in advance by my VA supervisor, ISSO, and Information System Owner, local AM, or designee.
- Make any unauthorized disclosure of any VA sensitive information through any means of communication including, but not limited to verbal communications, e-mail, text messaging, instant messaging, online chat, social media, and web sites.

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.

_____

Initials

I Will Not:

- Store my passwords or verify codes in any file on any IT system, unless that file has been encrypted using FIPS 140-3 (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.

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, Information System Security Officer (ISSO) or designee immediately upon suspicion.

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.
- 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 (OPIA) before establishing a VA social media account.
- Ensure that my use of social media, to conduct VA business, complies with law, guidance, and VA policy.
- Be professional at all times when posting to VA-related social media.
- Use my best judgment when interacting on social media about matters related to VA's mission.
- In my capacity as a VA representative, post only information about which I have actual knowledge.
- Identify myself and my roles as a VA representative when commenting or providing information on matters related to the VA's mission, and ensure that my profile and any related content is consistent with how I wish to present myself to colleagues, Veterans, and the general public.

_____

Initials

- 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.
- If content I publish on blogs, wikis or any other form of user-generated media might reasonably be perceived as the position of VA, publish a disclaimer that the views are my own and do not represent VA.

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.
- In my capacity as a VA representative, comment or provide information on any matter about which I do not have actual, up-to-date knowledge.
- Post information protected by the Privacy Act of 1974, 38 USC 5701, 5705, or 7332, the Health Insurance Portability and Accountability Act (HIPAA) Rules, or VA policy on any non-VA websites, without legal authority and prior approval by an authorized official.
- Use profanity, make libelous statements, 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.

5. ACKNOWLEDGEMENT AND ACCEPTANCE

a. I acknowledge that I have received a copy of VA Information Security Rules of Behavior for Organizational Users.

b. I understand, accept and agree to comply with all terms and conditions of VA Information Security Rules of Behavior for Organizational Users.

c. 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 are controlling.

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

Office Phone _____ **Position Title** _____