Federal Retirement Thrift Investment Board's
Rules of Behavior for Accessing IT Systems

All data contained on information systems in support of the Federal Retirement Thrift Investment Board (FRTIB or Agency) is owned by the FRTIB. User activity may be monitored, intercepted, recorded, read, copied, captured, or disclosed by authorized FRTIB personnel. FRTIB may give law enforcement officials any potential evidence of crime, fraud, or employee misconduct found on FRTIB information systems. Furthermore, law enforcement officials may be authorized to access and collect evidence from these systems. **USE OF THIS SYSTEM BY ANY USER, AUTHORIZED OR UNAUTHORIZED, CONSTITUTES EXPRESS CONSENT TO MONITORING.**

I understand and acknowledge:

1. Policies and Procedures:
    a. Federal Employees: I will abide by all Agency policies and procedures.
    b. Contractor Employees: I will abide by the Agency policies and procedures applicable to me in connection with the services provided to the Agency under the scope of my employer's contract. The Agency will provide me with access to all applicable policies and procedures.
2. **I HAVE NO REASONABLE EXPECTATION OF PRIVACY** while using any information system that processes, transmits, or stores FRTIB data.
3. I understand and acknowledge monitoring includes, but is not limited to the review of:
    a. Audit logs of any IT device used to support FRTIB;
    b. Access and use of the Internet while on the FRTIB network;
    c. Electronic communication activity; or
    d. Any device used to process FRTIB data (regardless of device ownership).
4. I shall successfully complete FRTIB Cyber Security Awareness training and Privacy Awareness training at the time of onboard and on an annual basis. I shall also complete any additional information technology, security, records management, and privacy training as required. If any required training is not completed, access to FRTIB information systems will be suspended.
5. I may have access to Controlled Unclassified Information (CUI) depending on my job duties. I shall protect the confidentiality[1], integrity[2], and availability[3] of FRTIB information in a manner consistent with its sensitivity.
6. I will use FRTIB information only in connection with the performance of my official duties. I will not disclose FRTIB information to unauthorized persons. I will not use non-FRTIB email, social media accounts (e.g., Outlook, Instagram, Gmail, Twitter, Facebook), or other external resources to conduct FRTIB business, thereby ensuring that official business is never confused with personal business.
7. I will encrypt all CUI using an Agency approved tool that is:

[1] NISTIR 7298, Revision 2 "Glossary of Key Information Security Terms" defines confidentiality as "The property that sensitive information is not disclosed to unauthorized individuals, entities, or processes."
[2] NISTIR 7298, Revision2 "Glossary of Key Information Security Terms" defines integrity as "The property that sensitive data has not been modified or deleted in an unauthorized and undetected manner."
[3] NISTIR 7298, Revision 2 "Glossary of Key Information Security Terms" defines availability as "The property of being accessible and useable upon demand by an authorized entity."

   a. Downloaded from FRTIB information systems onto a FRTIB authorized portable storage device;
   b. Downloaded to any FRTIB authorized device; or
   c. Emailed to any entity external to the FRTIB organization (to non -"TSP.GOV" or "FRTIB.GOV" email address.)

8. I will only access CUI when I am authorized to do so. I will only access the minimal amount of CUI needed, and I will delete my copy of CUI data downloaded from FRTIB information systems immediately when its official use is no longer required.
9. I will protect my passwords and/or authentication tokens from disclosure and loss at all times. I will utilize the Agency provided password manager and I will never reveal my passwords, write them down, or store them in clear-text. I will not construct my password from obvious personal data (e.g., social security number, telephone numbers, relative's names, pet's name).
10. I will only create passwords that are unrelated to any existing password and I will not reuse a password from any other account, system, website, or application.
11. I am accountable for all actions taken under my User ID. I will not allow others to use my User ID and I will not access other users' accounts. I will not attempt to access accounts or data that are not expressly authorized to me.
12. When logged on, I will lock my workstation and remove my PIV (Personal Identity Verification) card prior to leaving my workstation. All activity occurring when the workstation is active is the responsibility of the logged-on user.
13. I will not install, use, or reproduce unauthorized or illegally obtained software. Privately-owned software is prohibited from being used. FRTIB employees and contractors are only permitted to use FRTIB-approved applications and software. Employees and contractors must go through the Service Desk or ServiceNow to request applications and software.
14. I shall not connect unauthorized devices to FRTIB information systems under any circumstance. Examples include, but are not limited to: personal external hard drives, personal phones, unauthorized flash/thumb drives, networked cameras, or microphones.
15. Changes in my employment status or changes in my job responsibilities may require my access to be modified or terminated.
16. I am using a CUI system. I am NEVER authorized to originate, process, and/or store classified information on an unclassified system.
17. This agreement shall not nullify or affect in any manner any other confidentiality or nondisclosure agreement which I have executed or may execute with FRTIB.
18. I shall never attempt to tamper with, circumvent, or otherwise impede the security of any FRTIB system. I shall never install or utilize any tools designed to assist in doing the same.
19. I am not authorized to post organizational data to social media or social networking sites. Only authorized users with cleared content by the Office of External Affairs, the Office of Resource Management, or the Office of Communications and Education may post to social media or social networking sites as required to support the organizational mission. Personal use of social media while on work time or equipment must be limited with minimal cost to the government (see "Limited Personal Use" Policy) and must not interfere with my duties and responsibilities. I must seek approval from the Office of General Counsel prior to using or referencing my formal position when writing in a

nonofficial capacity. I will never use my FRTIB e-mail address to register on social networks, blogs, or other online tools utilized for personal use and that any misconduct committed on social media that has a nexus to my position at FRTIB may result in appropriate discipline, up to and including removal from Federal service. As an employee of the Federal Government, when using social medial tools, whether on behalf of FRTIB or on my own time, I am bound by the Standards of Ethical Conduct for Employees of the Executive Branch, 5 C.F.R. Part 2635 and the Hatch Act (5 U.S.C. §§ 7321-7326).

20. I will immediately report a potential incident[4], password compromise, anomaly in system performance, or suspicious activity to IncidentResponse@tsp.gov.
21. I shall not take any government-furnished equipment (including, but not limited to an FRTIB-issued laptop or phone) outside the United States or the territories of the United States without prior written approval from the Chief Technology Officer or designee.
22. Users are prohibited from sharing any FRTIB passwords with any other person or entity.
23. Viewing of pornographic or other offensive content is strictly prohibited on FRTIB furnished equipment and networks.
24. I shall promptly report lost, stolen or misplaced Government Furnished Equipment (e.g., laptop, phone, PIV card) to the FRTIB Service Desk, IT Asset Management Team and my supervisor (or Contracting Officer Representative if applicable). Users may be financially liable for lost, stolen or misplaced Government Furnished Equipment[5].
25. Any user who does not comply with or violates these rules may be subject to appropriate administrative action, including suspension or cancellation of system privileges and/or disciplinary action up to and including removal from the Federal service. Under some circumstances, noncompliance or violation of these rules may result in criminal prosecution. FRTIB will enforce the use of appropriate penalties against any user who fails to comply or violates IT Security Management policies.

Remote Access

FRTIB Rules of Behavior for Remote Access apply to remote access connections used to do work on behalf of FRTIB, including reading or sending email and viewing Intranet web resources. Remote access implementations that are covered include, but are not limited to, dial-in modems, frame relay, ISDN, DSL, VPN, SSH, and cable modems, etc.

These rules of behavior apply to all users which include FRTIB staff, contractors, vendors, and agents with remote access privileges to FRTIB's network.

1. The user is responsible for ensuring that their remote access connection is given the same security considerations as the user's on-site connection when connecting to FRTIB. For example, if an individual is processing sensitive (e.g., For Official Use Only, Controlled Unclassified Information) information via remote access, the individual will ensure unauthorized individuals cannot view the content. The user is responsible for ensuring unauthorized users do not access the FRTIB network, do not perform illegal activities, and do not use the access for outside business interests. The user bears responsibility for

[4] NISTIR 7298, Revision 2 "Glossary of Key Information Security Terms" defines incident as "An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies."

[5] OTS.501 IT Asset Management Procedures, Section 4.6 Lost and Stolen Assets

the consequences if the access is misused. Misuse of the user's access by a non-FRTIB employee may result in disciplinary action, up to and including removal from Federal service.

2. The user must strictly secure remote access. FRTIB will enforce access control public/private keys with strong pass-phrases.
3. Users with remote access privileges must ensure that their host is not connected to any other network at the same time. Reconfiguration of a home user's equipment for the purpose of split-tunneling or dual homing is not permitted at any time. Split-tunneling is having simultaneous direct access to a non-FRTIB network (such as the Internet, or a home network) from a remote device (PC, PDA, WAP phone, etc.) while connected into FRTIB's network via a VPN tunnel. Dual homing is having concurrent connectivity to more than one network from a computer or network device. Examples include being logged into the FRTIB network via a local ethernet connection and then dialing into an Internet Service Provider; or being on a FRTIB-provided VPN tunnel and then connecting into a spouse's remote access tunnel to their employment.
4. All hosts (e.g., laptops, desktops, workstations) that are connected to FRTIB networks via remote access technologies must use the most up-to-date anti-virus software and definitions, this includes non-FRTIB owned hosts.

Federal Retirement Thrift Investment Board's
Rules of Behavior for Accessing IT Systems

Addendum: FRTIB Rules of Behavior for Privileged User Accounts

The FRTIB Rules of Behavior for Privileged User Accounts is an addendum to the FRTIB Rules of Behavior for Accessing IT Systems and provides common rules on the appropriate use of FRTIB information technology resources for FRTIB privileged users, including Federal employees, interns, and contractors. Privileged user account roles have elevated privileges above those in place for general user accounts regardless of account scope (e.g., including both local and domain administrator accounts). Potential compromise of privileged user accounts carries a risk of substantial damage and therefore privileged user accounts require additional safeguards.

All users of privileged accounts must read these rules and sign the accompanying acknowledgement form in addition to the FRTIB Rules of Behavior for Accessing IT Systems before accessing FRTIB information, systems and/or networks in a privileged role.

I understand and acknowledge that as a Privileged User, I shall:

1. Use my privileged user account(s) for official administrative actions only.
2. Protect all privileged account credentials (e.g., passwords, tokens) at a security level commensurate with the highest level of data that the privileged account can access on the associated information system.
3. Protect the administrative or root-level authentication information at the highest level demanded by the sensitivity of the system.
4. Comply with all system/network administrator responsibilities in accordance with IT Security Management policies.
5. Use special access privileges only when they are needed to carry out a specific system function that requires elevated privileges on assigned systems.
6. Use a non-privileged (i.e., general user) account whenever administrative privileges are not required (e.g., e-mail, web browsing).
7. Log on to my non-privileged account and then from that log in to my privileged account to perform actions requiring privileges (to the maximum extent possible). For example, on a UNIX operating system, the user must log in to a non-privileged account before logging in as "root," and on a Microsoft Windows computer, the user must log in to a non-privileged account before performing a privileged function that requires authentication as a privileged user.
8. Notify the respective system owner immediately when privileged access is no longer required.
9. Use precautionary procedures to protect a privileged account from fraudulent use.
10. Watch for signs of inappropriate or illegal (i.e., hacker) activities or other attempts at unauthorized access and report them to the IncidentResponse@tsp.gov immediately upon discovery.
11. Read and enforce the system security controls as defined in the system security plan.
12. Complete any specialized role-based security or privacy training as required before receiving privileged system access, or refresher trainings thereafter. Failure to do so may result in suspension of administrative privileges, as well as suspension to FRTIB information systems.

Federal Retirement Thrift Investment Board's
Rules of Behavior for Accessing IT Systems

As a Privileged User, I shall not:

1. Share privileged user account(s) or password(s).
2. Create or log on to a group or shared user account.
3. Reuse passwords from any other account, system, website or application.
4. Store any password for accounts or services in clear-text.
5. Remove or destroy system audit, security, event, or any other log data unless authorized by the system owner in writing.
6. Acquire, possess, trade, or use hardware or software tools that could be employed to evaluate, compromise, or bypass information systems security controls.
7. Introduce unauthorized or malicious code into FRTIB information systems or networks.
8. Knowingly write, code, compile, store, transmit, or transfer malicious software code, including, but not limited to viruses, logic bombs, worms, and macro viruses.
9. Use privileged user account(s) for day-to-day communications and accessing the Internet.
10. Use privileged user account(s) to access data or other information unless I am explicitly authorized to do as part of my official duties.
11. Elevate the privileges of any user without prior approval from the system owner.
12. Use special privileges for personal business, gain, or entertainment.
13. Use privileged access to circumvent IT Security Management policies or security controls.
14. Use default, generic or pre-set passwords after their initial use/logon.

My signature below affirms that I have read all articles of the *FRTIB Rules of Behavior with Remote Access* and that I understand and acknowledge my responsibilities under these rules of behavior and will comply with these rules of behavior whenever accessing FRTIB systems or Information. I understand and acknowledge that any exceptions to the *FRTIB Rules of Behavior with Remote Access* must be authorized in advance in writing by the Chief Information Security Officer or his/her designee.

I have read the Addendum: *FRTIB Rules of Behavior for Privileged User Accounts.* I understand and acknowledge that any user who does not comply with or violates these rules may be subject to appropriate administrative action, including suspension or cancellation of system privileges and/or disciplinary action up to and including removal from the Federal service. Under some circumstances, noncompliance or violation of these rules may result in criminal prosecution. FRTIB will enforce the use of appropriate penalties against any user who fails to comply or violates policies. I understand and acknowledge that exceptions to the *FRTIB Rules of Behavior for Privileged User Accounts* must be authorized in advance in writing by the Chief Information Security Officer or his/her designee.

_____	_____	_____
Printed Name	Title	Department
_____	_____	
Signature	Date	