

Elevated Privileges Rules of Behavior

I understand, accept, and agree to the following terms and conditions that apply to my use of elevated privileges on information systems of the U.S. Department of Veterans Affairs.

The Elevated Privileges Rules of Behavior apply in addition to the National Rules of Behavior signed by all individuals authorized access to VA information systems.

1. I understand the VA systems are property of the United States (U.S.) Government and are considered Federal Information Technology (IT) systems subject to all applicable U.S. Federal IT laws and policies.
2. I understand that when I receive elevated privileges to a VA system I have been granted significant trust to use these privileges appropriately for their intended purpose and only when required to maintain the system(s) under my purview. I understand that operating in a mode where elevated privileges are enabled when not required is an unacceptable risk, is a violation of policy and subject to administrative action.
3. I understand that elevated privileges to VA resources should only be used for official VA business. I understand that limited personal use, as permitted by VA Directive 6001, *Limited Personal Use of Government Office Equipment Including Information Technology*, does not apply to use of administrator access and that I must not be operating in a mode where elevated privileges are enabled during limited personal use as this is an unacceptable risk, is a violation of policy and subject to administrative action.
4. I understand that elevated access to VA resources should only be used when such access is necessary to carry out specific duties related to my position. I will not use my elevated access to conduct duties that do not specifically require elevated privileges. On some systems, a separate account will be established and used for duties requiring elevated access. A normal user account with limited privileges should be used for all duties that do not specifically require elevated privileges including routine email access, web browsing, etc.
5. My email-enabled, non-privileged account will be my default account for normal daily use and my privileged account will be used only for accessing functions where elevated privileges are required for performing my duties. I will use the 'run as' function rather than logging into the system as an administrator wherever possible to limit my privileged account use.
6. I understand that elevated privileges are provided to me only for the performance of standard system-related duties on machines and networks for which I am responsible as part of my assigned job duties.
7. I understand that I am responsible for protecting the security of the account and the confidentiality of information encountered in the use of the account and will protect all passwords and authentication tokens from disclosure and loss at all times.
8. I agree that in my use of elevated privileges access:

- a. I will not use elevated privileges access to circumvent VA policies or security controls.
- b. I will not employ hardware or software tools to evaluate, compromise, bypass or in other way modify or remove information system security controls, except in support of authorized functions only when the action is specifically approved by my supervisor, ISO and CIO. Any such action must be properly documented and recorded for future external audit before or immediately following such action.
- c. Except as required by my duties or as authorized by VA national, regional or local policy, I will not review, access or modify individual accounts, systems devices or shares. I will not modify another user's files or other data, nor will I access a user's files or email or files unless specifically requested by the user or otherwise requested by and authorized in writing or email by appropriate senior management officials and the appropriate level ISO or a properly credentialed Law Enforcement Officer under a properly-scoped subpoena. I will only delete a user's mailbox or home directory in accordance to policy.
- d. I will not make unauthorized changes to systems. I will follow established procedures for installing, modifying, or removing system hardware or software and for deploying patches, updates, or upgrades.
- e. I will grant, change, or deny resources, access, or privileges to another individual only for authorized account management activities for which I have been specifically assigned responsibility.
- f. I will not access information outside of the scope of my specific job responsibilities or expose non-public information to unauthorized individuals.
- g. I will not remove or destroy system audit, security, event, or any other log data unless authorized by the system owner in writing. Tampering with audit logs of any kind in some cases can be considered evidence tampering which can be a criminal offense punishable by large fines and possible imprisonment.
- h. I will report all suspected or identified information security incidents (security and privacy) to my Operating Unit's Information Security Officer (ISO), Privacy Officer (PO), and my supervisor as appropriate.

Date