Rules of Behavior for Privileged Users v. 3.0

The following *HHS/OpDiv Rules of Behavior (RoB) for Privileged Users* is an addendum to the *Rules of Behavior for General Users* and provides mandatory rules on the appropriate use and handling of HHS/OpDiv information technology (IT) resources for all HH privileged users, including federal employees, interns, contractors, and other staff who possess privileged access to HHS/OpDiv information systems.[1] Privileged users have network accounts with elevated privileges that grant them greater access to IT resources than non-privileged users. These privileges are typically allocated to system, network, security, and database administrators, as well as other IT administrators.[2] The compromise of a privileged user account may expose HHS/OpDiv to a high-level of risk; therefore, privileged user accounts require additional safeguards.

A privileged user is authorized (and therefore, trusted) to perform security-relevant functions that ordinary users are not authorized to perform. System accounts and level of privilege vary dependent upon the role being fulfilled. A privileged user has the potential to compromise the three security objectives of confidentiality, integrity, and availability. Such users include, for example, security personnel or system administrators who are responsible for managing restricted physical locations or shared IT resources and have been granted permissions to create new user accounts, modify user privileges, as well as make system changes. Examples of privileged users include (but are not limited to):

1. Application developer
2. Database administrator
3. Domain administrator
4. Data center operations personnel
5. IT tester/auditor
6. Helpdesk support and computer/system maintenance personnel
7. Network engineer
8. System administrator
9. Security Stewards

Privileged users must read, acknowledge, and adhere to the RoB for Privileged User and any other HHS/OpDiv policy or guidance for privileged users, prior to obtaining access and using HHS/OpDiv information, IT resources and information systems and/or networks in a privileged role. The same signature acknowledgement process followed for the Appendix D, General User RoB, applies to the privileged user accounts. Each OpDiv must maintain a list of privileged users, the privileged accounts those users have access to, the permissions granted to each privileged account, and the authentication technology or combination of technologies required to use each privileged account[3].

[1] Per NIST SP 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations*, privileged roles include, for example, key management, network and system administration, database administration, and Web administration.
[2] OMB-16-04 available at Review-Doc-2015-ITOR-315-1.docx (whitehouse.gov), October 30, 2015.
[3] Per NIST White Paper, *Best Practices for Privileged User PIV Authentication,* April 21, 2016, available at https://csrc.nist.gov/publications/detail/white-paper/2016/04/21/best-practices-for-privileged-user-piv-authentication/final.

Following is the RoB for a privileged user.

I understand that as a privileged user, I must:

1. Use privileged user accounts appropriately for their intended purpose and only when required for official duties.
2. Comply with all privileged user responsibilities in accordance with the HHS Policy for Information Security and Privacy Protection (IS2P) and any other applicable HHS and OpDiv policies.
3. Notify system owners immediately when privileged access is no longer required.
4. Properly protect all information, including media, hard copy reports and documentation as well as system information in a manner commensurate with the sensitivity of the information and securely dispose of information and GFE that are no longer needed in accordance with HHS/OpDiv sanitization policies.
5. Report all suspected or confirmed information security incidents and privacy breaches to the OpDiv Helpdesk, HHS/OpDiv CSIRC, or OpDiv CSIRT as soon as possible, without unreasonable delay and no later than within ***one (1) hour*** of occurrence/discovery.
6. Complete any specialized role-based security or privacy training as required before receiving privileged system access.

I understand that as a privileged user, I must **not:**

1. Share privileged user account(s), password(s)/passcode(s)/PIV PINs, and other login credentials, including to other system administrators.
2. Conduct official HHS/OpDiv business using personal email or personal online storage account.
3. Use privileged user access to log into any system for non-elevated duties.
4. Install, modify, or remove any system hardware or software unless it is part of my job duties and the appropriate approvals have been obtained or with official written approval.
5. Access the internet for any reason while using my privileged account. This includes downloading of files (including patches or updates), etc.
6. Remove or destroy system audit logs or any other security, event log information unless authorized by appropriate official(s) in writing.
7. Tamper with audit logs of any kind. Note: In some cases, tampering can be considered evidence and can be a criminal offense punishable by fines and possible imprisonment.
8. Acquire, possess, trade, or use hardware or software tools that could be employed to evaluate, compromise, or bypass information systems security controls for unauthorized purposes.
9. Introduce unauthorized code, Trojan horse programs, malicious code, viruses, or other malicious software into HHS/OpDiv information systems or networks.
10. Knowingly write, code, compile, store, transmit, or transfer malicious software code, to include viruses, logic bombs, worms, and macro viruses.
11. Use privileged user account(s) for day-to-day communications and other non-privileged transactions and activities.
12. Elevate the privileges of any user without prior approval from the system owner.
13. Use privileged access to circumvent HHS/OpDiv policies or security controls.

14. Access information outside of the scope of my specific job responsibilities or expose non-public information to unauthorized individuals.
15. Use a privileged user account for web access except in support of administrative related activities.
16. Use any unknown website(s) which may be infected with malware and responding to phishing emails. If I use, I will report to OpDiv Helpdesk, HHS/OpDiv CSIRC, or OpDiv CSIRT as soon as possible, without unreasonable delay and no later than within ***one (1) hour*** of occurrence/discovery.
17. Use any file sharing program without HHS/OpDiv's permission.
18. Modify security settings on system hardware or software without the approval of a system administrator and/or a system owner.
19. Use systems (either government issued or non-government) without the following protections in place to access sensitive HHS/OpDiv information:
    - Antivirus software with the latest updates
    - Anti-spyware and personal firewalls
    - A time-out function that requires re-authentication after no more than 30 minutes of inactivity on remote access
    - Approved encryption to protect sensitive information stored on recordable media, including laptops, USB drives, and external disks; or transmitted or downloaded via e-mail or remote connections.

SIGNATURE

I have read the above *Rules of Behavior (RoB) for Privileged User*s and understand and agree to comply with the provisions stated herein. I understand that violations of these RoB or HHS/OpDiv information security policies and standards may result in disciplinary action and that these actions may include reprimand, suspensive of access privileges, revocation of access to federal information, information systems, and/or facilities, deactivation of accounts, suspension without pay, monetary fines, termination of employment; removal or debarment from work on federal contracts or projects; criminal charges that may result in imprisonment. I understand that exceptions to these RoB must be authorized in advance in writing by the designated authorizing official(s).

User's Name: _____

(Print)

User's Signature: _____

Date Signed: _____