Last Name, First Name (Please print clearly)
_____

Appendix B: Rules of Behavior for Privileged Users

The following *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 Centers for Medicare & Medicaid Services (CMS) information technology (IT) resources for all CMS privileged users, including federal employees, interns, contractors, and other staff who possess privileged access to CMS information systems.

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. The compromise of a *Privileged User* account may expose CMS to a high-level of risk; therefore, *Privileged User* accounts require additional safeguards.

A **Privileged User** is a user who has been granted significantly elevated privileges for access to protected physical or logical resources. A *Privileged Use*r 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:

A. Application developer
B. Database administrator
C. Domain administrator
D. Data center operations personnel
E. IT tester/auditor
F. Helpdesk support and computer/system maintenance personnel
G. Network engineer
H. System administrator

Privileged Users shall read, acknowledge, and adhere to the *RoB for Privileged User* and any other CMS policy or guidance for *Privileged Users*, prior to obtaining access and using CMS information and information systems and/or networks in a privileged role.

The same signature acknowledgement process followed for the Appendix A, General 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.

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 administrative actions;
2. Protect all *Privileged User* account passwords/passcodes/Personal Identity Verification (PIV)/ personal identified numbers (PINs) and other login credentials used to access CMS information systems;

3. Comply with all system/network administrator responsibilities in accordance with the CMS IS2P and any other applicable policies;
4. Notify system owners immediately when privileged access is no longer required;
5. Properly protect all sensitive information and securely dispose of information and GFE that are no longer needed in accordance with CMS/OpDiv sanitization policies;
6. Report all suspected or confirmed information security incidents (security and privacy) to the OpDiv Helpdesk and/or the OpDiv Security Incident Response Team (CSIRT) and my supervisor as appropriate; and
7. 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 <u>not</u>:**

1. Share *Privileged User* account(s), password(s)/passcode(s)/PIV PINs and other login credentials;
2. Install, modify, or remove any system hardware or software without official written approval or unless it is part of my job duties;
3. Remove or destroy system audit logs or any other security, event log information unless authorized by appropriate official(s) in writing;
4. 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;
5. 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;
6. Introduce unauthorized code, Trojan horse programs, malicious code, viruses, or other malicious software into CMS information systems or networks;
7. Knowingly write, code, compile, store, transmit, or transfer malicious software code, to include viruses, logic bombs, worms, and macro viruses;
8. Use Privileged User account(s) for day-to-day communications or other non-privileged transactions and activities;
9. Elevate the privileges of any user without prior approval from the system owner;
10. Use privileged access to circumvent CMS policies or security controls;
11. Access information outside of the scope of my specific job responsibilities or expose non-public information to unauthorized individuals;
12. Use a *Privileged User* account for Web access except in support of administrative related activities;
13. Modify security settings on system hardware or software without the approval of a system administrator and/or a system owner; and
14. Use systems (either government issued or non-government) without the following protections in place to access sensitive CMS information:
    a. Antivirus software with the latest updates,
    b. Anti-spyware and personal firewalls,
    c. A time-out function that requires re-authentication after no more than 30 minutes of inactivity on remote access, and
    d. 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 Users, September 6, 2019* and understand and agree to comply with the provisions stated herein. I understand that violations of these *RoB* or CMS information security policies and standards may result in disciplinary action and that these actions may include termination of employment; removal or disbarment from work on federal contracts or projects; revocation of access to federal information, information systems, and/or facilities; criminal penalties; and/or imprisonment. I understand that exceptions to these *RoB* must be authorized in advance in writing by the designated authorizing official(s). I also understand that violation of federal laws, such as the Privacy Act of 1974, copyright law, and 18 USC 2071, which these *RoB* draw upon, can result in monetary fines and/or criminal charges that may result in imprisonment.

User's Name:

_____

Employee ID #:

_____

User's Signature: If not signed digitally.

_____

Date Signed:

_____

Digital Signature (optional):

Click or tap here to enter text.