Office of Technology and Innovation

Rules of Behavior for Privileged Users

Guideline

TI-G-40-006

August 24, 2021

Consumer Financial Protection Bureau

Table of Contents

Table of Tables

Revision History

Table 1: Revision History

Effective	Version	Change Summary	Point of Contact
05/20/2013	1.0	Initial release	Cybersecurity
07/11/2014	2.0	Annual Review	Cybersecurity
05/31/2016	3.0	Update to address DO Independence and Annual Review	CPM
05/14/2018	4.0	Major change to look and content.	CPM
08/24/2021	5.0	Major rewrite and transition to the new T&I template	CPM

1 Introduction

Consumer Financial Protection Bureau (CFPB) employees and contractors who require elevated information-systems privileges are granted information technology (IT) system accounts that are separate from their general user accounts to perform their duties.

Privileged accounts have elevated access or permissions that allow users to access and alter system functions, configurations, and data. Privileged accounts can pose a significant risk to the Bureau, if mismanaged or compromised. Individuals with privileged accounts have increased responsibility for maintaining the confidentiality, integrity, and availability of CFPB information systems and services because of their duties. Requesting privileged access can be accomplished by following the step(s) listed in the guidance section of this document.

1.1 Purpose

The Bureau's Rules of Behavior (ROB) for privileged users provides guidance and specific rules on the appropriate use of CFPB information systems for individuals that possess elevated access.

1.2 Intended Audience

These rules of behavior apply to privileged users, as defined in this publication.

1.3 Background

Developing guidance for the identification and accountability of privileged users and their assigned responsibilities are mandated in the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Revision 5, *Security and Privacy Controls for Federal Information Systems and Organizations*. In response, the CFPB Office of Cybersecurity developed the Rules of Behavior for Privileged Users in accordance with the *CFPB Information Security Program Policy* and *Acceptable Use of CFPB Information Technology Resources Policy*.

1.4 Roles and Responsibilities

Table 2: Roles and Responsibilities Summary

Role	Responsibility
Chief Information Security Officer (CISO)	• Reviews document when a material revision is required. • Ensures that approval for privileged access follows the principle of least privilege as defined in this document. • Serves as the final level signatory and provides feedback where applicable.
Privileged User	• Completes any role-based training prior to requesting privileged access. • Reviews document to ensure understanding of roles and responsibilities as defined in Appendix B: Rules of Behavior for Privileged Users Statement of Acceptance of Responsibilities. • Signs the bottom of this document and the associated privileged access request form, hereafter referred to as PUA. • Submits PUA and this document through the CFPB Service and Support Portal. • Submits a request for privileged access annually. • Reports incidents to the CFPB Security and Operations Center as outlined in Appendix B: Rules of Behavior for Privileged Users Statement of Acceptance of Responsibilities.
CFPB Service Desk	• Receives signed rules of behavior for privileged users and PUA from CFPB personnel requesting access.
CFPB Security Operations Center	• Serves as the primary point of contact for privileged users as outlined in Appendix B: Rules of Behavior for Privileged Users Statement of Acceptance of Responsibilities.
Cybersecurity Program Management (CPM)	• Serves as the primary point of contact for any document update requests. • Revises document when applicable.

1.5 Primary Points of Contact

Table 3: Document Points of Contact Summary

Role	Point of Contact	Contact Topics
Document Owner	Name: Tacy Summersett Title: Cybersecurity Program Management Director T&I Office: Cybersecurity Email: Tacy.Summersett@cfpb.gov Group Email: CFPB_Cybersecurity_ProgramManagement@cfpb.gov	• Request for document updates. • Questions related to this document.

1.6 Related Documents

Table 4: Related Documents Summary

Document Name	Brief Description	Location or Link
NIST SP 800-53, Revision 5, Security and Privacy Controls for Federal Information Systems and Organizations	Provides a catalog of security and privacy controls for information systems and organizations to protect organizational operations and assets, individuals, other organizations, and the Nation from a diverse set of threats.	https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final
CFPB Information Security Program Policy	The Information Security Program Policy establishes the uniform information security principles, practices, and standards that govern how the Bureau protects information and systems from unauthorized access, use, disclosure, misuse, disruption, modification, or destruction.	https://team.cfpb.local/wiki/index.php/Cybersecurity
Acceptable Use of CFPB Information Technology Resources Policy	The Acceptable Use of CFPB Information Technology Resources policy (AUP) describes how to use and not use your CFPB computing devices and technology. It provides information on acceptable user behavior regarding system and network activities, email communications, blogging, social networks, auditing and privacy, and other important details.	https://team.cfpb.local/wiki/index.php/Cybersecurity

Information Security Standards (ISS) and Annex	Establishes minimum security control standards for all CFPB owned and/or operated information systems.	https://team.cfpb.local/wiki/index.php/Cybersecurity
Privileged User Access Request Form	Used to request elevated/privileged access rights to Infrastructure systems.	Privileged User Access Request Form

2 Guidance

Eligibility for privileged access is determined according to the principle of "least privilege." According to the principle of least privilege, personnel are authorized to receive the minimal level of access required to accomplish assigned core job functions. If a personnel's core job functions do not require elevated access, then they are not eligible. All CFPB personnel that are eligible must complete any role-based training prior to submitting a request for privileged access.

After all role-based training requirements are completed, users must review, acknowledge, and sign that they understand the rules outlined in Appendix B, the Rules of Behavior for Privileged Users Statement of Acceptance of Responsibilities. Additionally, users must complete and sign the Privileged User Access Request Form. Once completed, privileged users must submit this document and the privileged access request form to the CFPB Service Desk through the CFPB Service and Support Portal.

To maintain privileged access, users must adhere to the guidelines set forth in this document and the signed agreement. Any privileged access shall be re-authorized annually.

It is important to note that access can be revoked for privileged users at any time by the Chief Information Security Officer if a violation of this agreement or the Acceptable Use Policy occurs. Furthermore, if any privileged user is found to have violated the requirements outlined in this document, privileged access will be revoked, and elevated access may need to be re-authorized. Subsequent violations may result in administrative corrections or a suitability review.

3 Approvals

Dr. Tiina K.O. Rodrigue

Digitally signed by Dr. Tiina K.O. Rodrigue
Date: 2021.08.24 18:45:02 -04'00'

Dr. Tiina K.O. Rodrigue Date

Chief Information Security Officer

APPENDIX A: KEY TERMS AND ACRONYMS

Table 5: Key Teams and Acronyms

Term/Acronym	Definition
Privileged User	A privileged user is defined as an individual who has been granted elevated privileges or access, which are typically allocated to system administrators, network administrators, and others who are responsible for system/application control, monitoring, or administration functions. Individuals with elevated access have increased responsibility for maintaining the confidentiality, integrity, and availability of CFPB information systems and services because of their duties.
Multifactor Authentication	Allows users to enter a combination of something they know (e.g., password), something they have (e.g., a one-time passcode or token), and something they are (e.g., biometric). At CFPB, Multifactor Authentication involves the use of Okta Verify tokens, Personal Identification Verification (PIV) Card, Google Authenticator, and other MFA.
Least Privilege	Allowing only the level of access (or processes acting on behalf of users) that is necessary to accomplish assigned organizational tasks.
Insider Threat	A malicious threat to an organization that comes from people within the organization, such as employees, former employees, contractors, or business associates, who have inside information concerning the organization's security practices, data, and computer systems.
System Owner	An organizational official who is responsible for the procurement, development, integration, modification, operation, maintenance, and disposal of a system. This person is often also a privileged user, as well as the detection and notification element on a per-system basis. The system owner is a signator for the security of the system and the adherence to the Acceptable Use Policy and enforcement of appropriate PUA and behavior.

APPENDIX B: RULES OF BEHAVIOR FOR PRIVILEGED USERS STATEMENT OF ACCEPTANCE OF RESPONSIBILITIES

A privileged user is defined as an individual who has been granted elevated privileges or access, which is typically allocated to database, network or system administrators, and others who are responsible for system/application control, monitoring, or administration functions. Individuals with elevated access have increased responsibility for maintaining the confidentiality, integrity, and availability of CFPB information systems and services as a result of their duties. The following list depicts the explicit rules that privileged users must adhere to.

I understand that as a privileged user, I must:

- Use privileged accounts only in the performance of official duties and only as necessary to complete assigned tasks.
- Utilize multi-factor authentication (i.e., PIV) to access my privileged accounts.
- Always protect my credentials and passwords.
- Not use group account(s).
- Notify the appropriate System Owner(s) if my access is no longer needed.
- Complete any required role-based training before receiving elevated rights to any information systems and annually thereafter.
- Complete refresher Cybersecurity role-based training and awareness training if I violate CFPB policies. During this time, my privileged access will be suspended until the refresher training is complete. Upon completion of training, a new PUA and ROB must be signed before the privileged access is regained.
- Not use my privileged account for functions that can be done using my general user account (e.g., email, creating documents, internet browsing).
- Not attempt to circumvent CFPB policies or security controls.
- Report to the CFPB Computer Security Incident Response Team if any of the following occurs:

  - A suspected insider threat is identified
  - Notice a user has access beyond "Need to Know."
  - Notice a user is violating the terms of this agreement
  - A user's privileges need to be changed
  - Any other suspicious activity upon discovery
- Have written approval from the Bureau's change control process before making changes to the Bureau's infrastructure and environment. This includes but is not limited to:
  - Installing software that is not licensed and approved, modifying system settings, or decommissioning a system or service.
- Do not write, compile, store, or transmit software/system codes that are malicious (e.g., viruses and worms).
- Do not use organization-provided credentials (i.e., email addresses) for creating accounts on external sites/applications.

I have read the required rules above regarding expected privileged user behavior on CFPB information systems, and by electronically signing below, I agree to comply with them. I understand that refusing to sign this agreement renders me ineligible for privileged access. I understand that failure to comply with these rules may result in the loss of or limitations on, the use of information resources, as well as disciplinary and/or legal action, including, but not limited to, termination of employment or referral for criminal prosecution.

DANY GARCIA (Affiliate)

Digitally signed by DANY GARCIA (Affiliate)
Date: 2024.05.14 13:48:08 -04'00'

Privileged user's electronic signature