|  |  |  |  |
| --- | --- | --- | --- |
|  |  | |  |
|  |  | |  |
|  | FedRAMP® System Security Plan (SSP)  Appendix F: Rules of Behavior (RoB) Template  for <Insert CSP Name>  <Insert CSO Name>  <Insert Version X.X>  <Insert MM/DD/YYYY> | |  |
|
|  |  | |  |
|  |  | info@fedramp.gov  fedramp.gov |  |

TEMPLATE REVISION HISTORY

This document is required to be fully populated for the *FedRAMP SSP All Baselines Template*, Appendix F, <CSO Name> Rules of Behavior (ROB). This document is not required for a LI-SaaS submission.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Date | Version | Pages | Description | Author |
| 05/2/2012 | 1.0 | All | Original publication | FedRAMP PMO |
| 05/18/2016 | 2.0 |  | Reformatted to FedRAMP Document Standard, added repeated text schema, and content fields to tables, revised cover page, changed document designation to Unclassified Confidential Information (CUI), added instruction to complete SSP 15.5 Attachment 5 - Revision History in the System Security Plan, removed front matter section How This Document is Organized, revised Section 1 Introduction. | FedRAMP PMO |
| 09/30/16 | 2.1 |  | Removed Acronyms and referenced FedRAMP Master Acronyms and Glossary resource document | FedRAMP PMO |
| 03/9/2017 | 2.2 |  | Renamed document from "FedRAMP Rules of Behavior (RoB) Template" to "SSP ATTACHMENT 5 - FedRAMP Rules of Behavior (RoB) Template" | FedRAMP PMO |
| 06/6/2017 | 2.2 |  | Updated logo | FedRAMP PMO |
| 06/30/2023 | 3.0 |  | Updated to reflect FedRAMP Rev. 5 baselines. | FedRAMP PMO |

**How to contact us**

For questions about FedRAMP, or for questions about this document including how to use it, contact [info@FedRAMP.gov.](mailto:info@FedRAMP.gov)

For more information about FedRAMP, see [www.FedRAMP.gov](http://www.fedramp.gov).

|  |
| --- |
| ***Instructions:*** |
| *Delete this Record of Changes for Template table and this instruction from your final version of this document.*  *Before delivering the final version of the RoB, be sure to delete all italicized instructional text.*  Delete instruction text after completion. |

Prepared by

|  |  |
| --- | --- |
| Organization Name that prepared this document | |
| **Street Address** | <Enter Street Address> |
| **Suite/Room/Building** | <Enter Suite/Room/Building> |
| **City, State, Zip** | <Enter City, State, and Zip Code> |

Prepared for

|  |  |
| --- | --- |
| Organization Name for whom this document was prepared | |
| **Street Address** | <Enter Street Address> |
| **Suite/Room/Building** | <Enter Suite/Room/Building> |
| **City, State, Zip** | <Enter City, State, and Zip Code> |

Document Revision History

This document is required to be fully populated for the FedRAMP SSP All Baselines Template, Appendix F, <CSO Name> Rules of Behavior (ROB). This document is not required for a LI-SaaS submission.

| **Date** | **Description** | **Version** | **Author** |
| --- | --- | --- | --- |
| <Date> | <Revision Description> | <Version> | <Author> |
| <Date> | <Revision Description> | <Version> | <Author> |
| <Date> | <Revision Description> | <Version> | <Author> |

TABLE OF CONTENTS

[1 Introduction 5](#_Toc135152741)

[2 Purpose 5](#_Toc135152742)

[3 Scope 5](#_Toc135152743)

[4 Rules of Behavior 6](#_Toc135152744)

[4.1 Rules of Behavior for Internal Privileged Users 7](#_Toc135152745)

[4.2 Rules of Behavior for Internal Non-Privileged Users 10](#_Toc135152746)

[4.3 Rules of Behavior for External Privileged Users 12](#_Toc135152747)

[4.4 Rules of Behavior for External Non-Privileged Users 14](#_Toc135152748)

# Introduction

This Rules of Behavior (RoB) document describes how a cloud service provider’s (CSP’s) privileged/non-privileged personnel and a federal agency’s privileged personnel/customers should behave when interacting with their respective cloud service offerings (CSOs) in accordance with the security controls relevant to the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53.

# Purpose

This document describes specific CSO and agency user behaviors that should be followed in order for the system to attain and maintain security control compliance with the FedRAMP baselines. The CSO and agency user is the greatest asset and greatest liability to all cloud services. It is human nature to make things easier to access, easier to reach, and easier to remember. This document helps to define security controls that will regulate user behavior.

# Scope

The security controls associated with user responsibilities and certain expectations of behavior for following security policies, standards, and procedures are required for every CSO based on the 800-53 control PL-04 Planning | Rules of Behavior. This requires CSPs to establish and provide, to individuals requiring access to the system, the rules that describe their responsibilities and expected behavior for information and system usage, security, and privacy. This RoB applies to all CSO administrators with privileged access to the system, CSO users with non-privileged access to the system, federal agency administrators, and federal agency users. However, federal agency users are subject to the United States Government (USG) Agency RoB and a CSP may not require a RoB for federal agency users.

|  |
| --- |
| ***Instructions:*** |
| *Sample sets of Rules of Behavior, based on the FedRAMP 800-53 requirements, are on the pages that follow. Modify these sets of rules to match the Rules of Behavior that are necessary to secure the system. FedRAMP recognizes that the Rules of Behavior for a CSO’s privileged admins will differ from a CSO’s non-privileged internal users, an agency’s admins appointed for specific duties, and an agency’s users/customers. When defining Rules of Behavior for the various roles, the CSP should be able to identify that each “Role” falls into a category of user that may or may not follow a specific set of behavioral rules.*  *The “rules” provided below are offered as examples. Keep in mind that certain rules that apply to internal users may not apply to external users and vice versa.*  *Before delivering the final version of the RoB, be sure to delete all italicized instructional text.*  Delete instruction text after completion. |

# Rules of Behavior

The planning (PL) control - 04, Rules of Behavior, applies to the FedRAMP High, Moderate, and Low baselines. This control requires that each CSP:

1. Establish and provide to individuals requiring access to the system, the rules that describe their responsibilities and expected behavior for information and system usage, security, and privacy;
2. Receive a documented acknowledgment from such individuals, indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the system;
3. Review and update the rules of behavior at least annually; and
4. Require individuals who have acknowledged a previous version of the rules of behavior to read and re-acknowledge annually and when the rules are revised or updated.

Based on individual user roles and responsibilities, CSPs must differentiate between rules that apply to privileged users and rules that apply to general users, internal and external.

PL-04 (01) then requires that minimally the following are included in each set of Rules of Behavior for each category of user (i.e., internal privileged users, internal non-privileged users, external privileged users, and external non-privileged users).

1. Use of social media, social networking sites, and external sites/applications;
2. Posting organizational information on public websites; and
3. Use of organization-provided identifiers (e.g., email addresses) and authentication secrets (e.g., passwords) for creating accounts on external sites/applications.

## Rules of Behavior for Internal Privileged Users

|  |
| --- |
| ***Instructions:*** |
| *In each of the following sections, there is a sample set of Rules of Behavior based on the FedRAMP 800-53 requirements. Modify these sample sets to align with the CSO. Additional rules may be added based on the situation. Ensure that the RoB for the role intended is comprehensive. The Acceptance and Signature box can be modified as needed to align with CSO requirements.*  *Before delivering the final version of the RoB, be sure to delete all italicized instructional text.*  Delete instruction text after completion. |

<CSP Name> employees who have access to the <CSO Name> must sign Internal Rules of Behavior for Privileged Access prior to gaining access to the <CSO Name>. Rules of Behavior may be signed on paper, or electronically at first login. Either way, the organization must retain artifacts to enable an independent assessor to verify that Rules of Behavior have been signed for all users.

As an Internal Privileged User, <Firstname MI Lastname> has administrative privileges to the <CSO Name> and is required to minimally follow the FedRAMP security controls baseline assigned to this CSO.

Additionally, when acting in this role, you shall abide by the <CSO Name> principles of Separation of Duties and Least Privilege.

You must comply with copyright and site licenses of proprietary software.

You must process only data that pertains to official business and is authorized to be processed on this system in my capacity as an internal privileged administrator.

You must ensure that proper protocol is followed for reporting all security incidents or suspected incidents to your superior(s) as assigned in the <CSO Name> Incident Response Procedures and in accordance with the FedRAMP Incident Communications Procedures.

You must ensure that proper protocol is followed for all change management and configuration management efforts over which I have authority.

You must ensure that due care is exercised to keep unauthorized personnel off of this system and to keep my superiors informed of such attempts.

You must allow only the software, systems, components, and/or devices named in the Integrated Inventory Workbook to execute in the manner for which these are determined, on this system.

You must remain cognizant of the changing technological advancements so that you can better serve as administrator of this system, and see to it that the system remains secure.

You must use only your provided authentication method to access the administrative components of this system, and not attempt to log in to this administrative role using the same authentication method with which you log in as a regular internal user.

You must regularly attend computer security awareness and privacy training as requested by your superiors.

You must keep all of your required certifications current.

You must ensure that access to application-specific sensitive data is limited solely to your job function.

You must follow all special requirements for accessing, protecting, and utilizing data, including Privacy Act and Supply Chain requirements, copyright requirements, and procurement of sensitive data.

You must safeguard all resources for which you are responsible against waste, loss, abuse, unauthorized users, and misappropriation. Thus ensure the confidentiality, integrity, availability and security of all system components commensurate with the CSO requirements for storing, processing, and transmitting all federal data.

You must ensure both electronic and hardcopy official records (including attachments) are stored and disposed of, per CSP policies and standards.

You must not process U.S. classified national security information on any component of <CSO Name>, for any reason.

By your signature or electronic acceptance (such as by clicking an acceptance button on the screen), you agree to these rules.

You understand that any person who obtains information from a computer connected to the Internet in violation of his or her employer’s computer-use restrictions is in violation of the Computer Fraud and Abuse Act.

|  |  |  |  |
| --- | --- | --- | --- |
| **ACCEPTANCE AND SIGNATURE** | | | |
| I have read the above Internal Privileged Users Rules of Behavior (RoB) for <CSO Name> systems and networks. By my electronic acceptance and/or signature below, I acknowledge and agree that my access to all <CSO Name> systems and networks is covered by, and subject to, such rules. Further, I acknowledge and accept that any violation by me of these RoB may subject me to civil and/or criminal actions and that CSP retains the right, at its sole discretion, to terminate, cancel, or suspend my access rights to the <CSP Name> systems at any time, without notice. | | | |
|  | | | |
| User’s Legal Name: |  | | (printed) |
| User’s Signature: |  | | (signature) |
| Date: | Click here to enter a date. |  |  |
|  | | | |
| Comments: | Click here to enter text. | | |

## Rules of Behavior for Internal Non-Privileged Users

As an Internal Non-Privileged User, <Firstname MI Lastname> has general user privileges to the <CSO Name> and is required to minimally follow the FedRAMP security controls baseline assigned to this CSO, acting in this general capacity.

Additionally, when acting in this role:

You must not install unapproved software onto this system. You shall inform the IT Security Desk if unapproved software appears on your device.

You must not add additional hardware or peripheral devices to this system. Only designated personnel can direct the installation of hardware and peripheral devices on this system.

You must not reconfigure hardware, software, or firmware on any <CSO Name> components and you must report this as a finding to the IT Security Desk if reconfiguration or manipulation is in any way possible.

You must follow all <CSO Name> wireless access policies.

You must not share information with someone who does not have authority to access that information.

You must not remove computer resources from the facility without prior approval.

You must ensure that your use of the <CSO Name> device is for the purposes for which it is intended and you will not attempt to access any websites that your organization will not allow you access.

You must ensure that you will not circumvent the security policies set up on your device. If you determine there might be a misconfiguration, you will inform the IT Security Desk immediately.

You must ensure both electronic and hardcopy official records (including attachments) are stored and disposed of according to <CSO Name> policies and standards.

You must safeguard all resources for which you are responsible against waste, loss, abuse, unauthorized users, and misappropriation. Thus ensure the confidentiality, integrity, availability and security of all system components commensurate with the CSO requirements for storing, processing, and transmitting all federal data.

You must ensure that sensitive information processed and stored within your devices and components is restricted to team members via least privilege and separation of duties.

You must report all security incidents or suspected incidents (e.g., lost passwords, lost tokens, improper or suspicious acts) related to <CSO Name> components and networks to the <CSP Name> Operations Center <Operations Center Phone Number>.

By your signature or electronic acceptance (such as by clicking an acceptance button on the screen), you agree to these rules.

You understand that any person who obtains information from a computer connected to the Internet in violation of his or her employer’s computer-use restrictions is in violation of the Computer Fraud and Abuse Act.

|  |  |  |  |
| --- | --- | --- | --- |
| **ACCEPTANCE AND SIGNATURE** | | | |
| I have read the above Rules of Behavior (RoB) for Internal Non-Privileged Users for <CSO Name> systems and networks. By my electronic acceptance and/or signature below, I acknowledge and agree that my access to all <CSO Name> systems and networks is covered by, and subject to, such rules. Further, I acknowledge and accept that any violation by me of these RoB may subject me to civil and/or criminal actions and that CSP retains the right, at its sole discretion, to terminate, cancel, or suspend my access rights to the <CSP Name> systems at any time, without notice. | | | |
|  | | | |
| User’s Legal Name: |  | | (printed) |
| User’s Signature: |  | | (signature) |
| Date: | Click here to enter a date. |  |  |
|  | | | |
| Comments: | Click here to enter text. | | |

## Rules of Behavior for External Privileged Users

As an external privileged user for <CSO Name>, you are required to follow specific Rules of Behavior when interacting with this system.

You must conduct only authorized <CSO Name>-related business while logged into the administrative functional area assigned to you.

You must ensure your level of access to components and networks owned by <CSO Name> is limited to ensure your access is no more than necessary to perform your legitimate tasks and assigned duties. If you believe you are being granted access that you should not have, you must immediately notify the <CSP Name> Operations Center <Operations Center Phone Number>.

You must maintain the confidentiality of your authentication credentials such as any passwords or passcodes granted to you. Do not reveal your authentication credentials to anyone; a <CSO Name> employee should never ask you to reveal them.

You must follow proper logon/logoff procedures. You must manually login to your session; do not store your password locally on your system or utilize any automated logon capabilities. You must promptly logout when session access is no longer needed. If a logout function is unavailable, you must close your browser. Never leave your computer unattended while logged into the <CSO Name>.

You must report all security incidents or suspected incidents (e.g., lost passwords, lost tokens, improper or suspicious acts) related to <CSO Name> components and networks to the <CSP Name> Operations Center <Operations Center Phone Number>.

You must not establish any unauthorized interfaces between systems, networks, and applications owned by <CSO Name>. You must immediately report any potential misconfigurations.

You must acknowledge that your access to systems and networks owned by <CSO Name> is governed by, and subject to, all federal laws, including, but not limited to, the Privacy Act, 5 U.S.C. 552a, if the <CSO Name> maintains individual Privacy Act information. Your access to <CSO Name> constitutes your consent to the retrieval and disclosure of the information within the scope of your authorized access, subject to the Privacy Act, and applicable state and federal laws.

You must safeguard all resources for which you are responsible against waste, loss, abuse, unauthorized users, and misappropriation. Thus ensure the confidentiality, integrity, availability and security of all system components commensurate with the CSO requirements for storing, processing, and transmitting all federal data. Commensurate security protocols are followed at all times.

You must not browse, search, or reveal information hosted by <CSO Name> except in accordance with that which is required to perform your legitimate tasks or assigned duties.

You must not retrieve information, or in any other way disclose information, for any person or process who/that does not have authority to access that information.

You must not process U.S. classified national security information on any component of <CSO Name> for any reason.

You must agree to contact the <CSP Name> Chief Information Security Officer or the <CSP Name> Operations Center <Operations Center Phone Number> if you do not understand any of these rules.

By your signature or electronic acceptance (such as by clicking an acceptance button on the screen), you agree to these rules.

You understand that any person who obtains information from a computer connected to the Internet in violation of his or her employer’s computer-use restrictions is in violation of the Computer Fraud and Abuse Act.

|  |  |  |  |
| --- | --- | --- | --- |
| **ACCEPTANCE AND SIGNATURE** | | | |
| I have read the Rules of Behavior (RoB) for External Privileged Users for <CSO Name> systems and networks. By my electronic acceptance and/or signature below, I acknowledge and agree that my access to all <CSO Name> systems and networks is covered by, and subject to, such rules. Further, I acknowledge and accept that any violation by me of these RoB may subject me to civil and/or criminal actions and that CSP retains the right, at its sole discretion, to terminate, cancel, or suspend my access rights to the <CSP Name> systems at any time, without notice. | | | |
|  | | | |
| User’s Legal Name: |  | | (printed) |
| User’s Signature: |  | | (signature) |
| Date: | Click here to enter a date. |  |  |
|  | | | |
| Comments: | Click here to enter text. | | |

## Rules of Behavior for External Non-Privileged Users

As an External Non-Privileged User, <Firstname MI Lastname> has general user privileges to the <CSO Name> and is required to minimally follow the FedRAMP security controls baseline assigned to this CSO, acting in this general capacity.

You must not interact with <CSO Name> in any way other than prescribed by the agency administrator.

You must inform the IT Security Desk if unapproved software appears on your device. Only <CSP Name> designated personnel are authorized to load software.

You must not add additional software, hardware, or peripheral devices to <CSO Name>. Only designated personnel can direct the installation of hardware and peripheral devices on this system.

You must not reconfigure hardware, software, or firmware on any <CSO Name> components. You must report this as a finding to the IT Security Desk if reconfiguration or manipulation is in any way possible.

You must not share information with someone who does not have authority to access that information.

You must not remove computer resources without prior approval.

You must use the <CSO Name> device for the purposes for which it is intended.

You must not circumvent the security policies configured on your device. If you determine there might be a misconfiguration, you must inform the IT Security Desk immediately.

You must not process U.S. classified national security information on any component of <CSO Name> for any reason.

You must follow all <CSO Name> wireless access policies.

You must ensure both hardcopy and electronic official records (including attachments) are stored and disposed of according to <CSO Name> policies and standards.

You must safeguard all resources for which you are responsible against waste, loss, abuse, unauthorized users, and misappropriation. Thus ensure the confidentiality, integrity, availability and security of all system components commensurate with the CSO requirements for storing, processing, and transmitting all federal data.

You must agree to contact the <CSP Name> Chief Information Security Officer or the <CSP Name> Operations Center <Operations Center Phone Number> if you do not understand any of these rules.

By your signature or electronic acceptance (such as by clicking an acceptance button on the screen), you agree to these rules.

You understand that any person who obtains information from a computer connected to the Internet in violation of his or her employer’s computer-use restrictions is in violation of the Computer Fraud and Abuse Act.

|  |  |  |  |
| --- | --- | --- | --- |
| **ACCEPTANCE AND SIGNATURE** | | | |
| I have read the Rules of Behavior (RoB) for External Non-Privileged Users for <CSO Name> systems and networks. By my electronic acceptance and/or signature below, I acknowledge and agree that my access to all <CSO Name> systems and networks is covered by, and subject to, such rules. Further, I acknowledge and accept that any violation by me of these RoB may subject me to civil and/or criminal actions and that CSP retains the right, at its sole discretion, to terminate, cancel, or suspend my access rights to the <CSP Name> systems at any time, without notice. | | | |
|  | | | |
| User’s Legal Name: |  | | (printed) |
| User’s Signature: |  | | (signature) |
| Date: | Click here to enter a date. |  |  |
|  | | | |
| Comments: | Click here to enter text. | | |