SSP ATTACHMENT 5 – FedRAMP Rules of Behavior (RoB) Template

CSP Name

Information System Name

Version #.#

Version Date

Controlled Unclassified Information

Prepared by

| Organization Name that prepared this document | | |
| --- | --- | --- |
|  | Street Address | Click here to enter text. |
| Suite/Room/Building | Click here to enter text. |
| City, State, ZIP | Click here to enter text. |

Prepared for

| Organization Name for whom this document was prepared | | |
| --- | --- | --- |
|  | Street Address | Click here to enter text. |
| Suite/Room/Building | Click here to enter text. |
| City, State, ZIP | Click here to enter text. |

Instruction: Delete this Record of Changes for Template table and this instruction from your final version of this document.

Record of Changes for Template

| Date | Description | Version | Author |
| --- | --- | --- | --- |
| 5/2/2012 | Original publication | 1.0 | FedRAMP PMO |
| 5/18/2016 | 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. | 2.0 | FedRAMP PMO |
| 9/30/16 | Removed Acronyms and referenced FedRAMP Master Acronyms and Glossary resource document | 2.1 | FedRAMP PMO |
| 3/9/2017 | Renamed document from "FedRAMP Rules of Behavior (RoB) Template" to "SSP ATTACHMENT 5 - FedRAMP Rules of Behavior (RoB) Template" | 2.2 | FedRAMP PMO |
| 6/6/2017 | Updated logo | 2.2 | FedRAMP PMO |

Revision History

Complete 15.5 Attachment 5 - Rules of Behavior Revision History in the System Security Plan. Detail specific changes in the table below.

| Date | Version | Page(s) | Description | Author |
| --- | --- | --- | --- | --- |
| Click here to enter a date. | Click | Click | Click here to enter text. | Click |
| Click here to enter a date. | Click | Click | Click here to enter text. | Click |

How to contact us

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

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

Table of Contents

[1 Introduction and Purpose 1](#_Toc476809473)

[2 Rules of Behavior for Internal Users 2](#_Toc476809474)

[3 Rules of Behavior for External Users 5](#_Toc476809475)

[4 Acronyms and Definitions 7](#_Toc476809476)

# Introduction and Purpose

Rules of Behavior describe security controls associated with user responsibilities and certain expectations of behavior for following security policies, standards, and procedures. Security Control Planning (PL)-4 requires Cloud Service Providers (CSP) to implement Rules of Behavior. It is often the case that different Rules of Behavior apply to internal and external users. Internal users are employees of your organizations, including contractors. External users are anyone who has access to a system that you own that is not one of your employees or contractors. External users might be customers or partners, or customer prospects that have been issued demo accounts.

CSP Name employees who have access to the Information System Name must sign Internal Rules of Behavior. If CSP Name provisions accounts for customers, including management accounts, it is CSP Name’s responsibility to ensure that whoever CSP Name provisions an account to signs an External Rules of Behavior. If CSP Name provisions a management account to an individual customer, and then that manager in turn provisions subsequent customer accounts, it is the responsibility of the customer manager to ensure that users that he/she has provisioned sign the CSP Name provided Rules of Behavior. Ultimately, whoever provisions the account owns the responsibility for getting users to sign the Rules of Behavior for the accounts that they have provisioned.

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.

Instruction: A sample set of Rules of Behavior have been provided for both Internal Users and External Users on the pages that follow. The CSP should modify these sets of rules to match the Rules of Behavior that are necessary to secure the system. You do not need to use these exact rules – they have been provided as examples. Please keep in mind that certain rules that apply to internal users may not apply to external users and vice versa.

Delete this instruction from your final version of this document.

# Rules of Behavior for Internal Users

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 the system.

You must report all security incidents or suspected incidents to the IT department.

You must discontinue use of any system resources that show signs of being infected by a virus or other malware and report the suspected incident.

You must challenge unauthorized personnel that appear in your work area.

You must use only the CSP Name data for which you have been granted authorization.

You must notify your CSP Name manager if access to system resources is beyond that which is required to perform your job.

You must attend computer security awareness and privacy training as requested by CSP Name.

You must coordinate your user access requirements, and user access parameters, with your CSP Name manager.

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

You must safeguard resources against waste, loss, abuse, unauthorized users, and misappropriation.

You must ensure that access is assigned based on your CSP Name manager’s approval.

You must familiarize yourself with any special requirements for accessing, protecting, and utilizing data, including Privacy Act requirements, copyright requirements, and procurement of sensitive data.

You must ensure electronic official records (including attachments) are printed and stored according to CSP Name policy and standards.

You must ensure that sensitive, confidential, and proprietary information sent to a fax or printer is handled in a secure manner, e.g., cover sheet to contain statement that information being faxed is Confidential and Proprietary, For Company Use Only, etc.

You must ensure that hard copies of Confidential and Proprietary information is destroyed (after it is no longer needed) commensurate with the sensitivity of the data.

You must ensure that Confidential and Proprietary information is protected against unauthorized access using encryption, according to CSP Name standards, when sending it via electronic means (telecommunications networks, e-mail, and/or facsimile).

You must not process U.S. classified national security information on any system at CSP Name for any reason.

You must not install CSP Name unapproved software onto the system. Only CSP Name designated personnel are authorized to load software.

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

You must not reconfigure hardware or software on any CSP Name systems, networks, or interfaces.

You must follow all CSP Name wireless access policies.

You must not retrieve information for someone who does not have authority to access that information.

You must not remove computer resources from the facility without prior approval. Resources may only be removed for official use.

You must ensure that web browsers check for a publisher’s certificate revocation.

You must ensure that web browsers check for server certificate revocation.

You must ensure that web browsers check for signatures on downloaded files.

You must ensure that web browsers empty/delete temporary Internet files when the browser is closed.

You must ensure that web browsers use Secure Socket Layer (SSL) version 3.0 (or higher) and Transport Layer Security (TLS) 1.0 (or higher). SSL and TLS must use a minimum of 128-bit encryption.

You must ensure that web browsers warn about invalid site certificates.

You must ensure that web browsers warn if the user is changing between secure and non-secure mode.

You must ensure that web browsers warn if forms submittal is being redirected.

You must ensure that web browsers do not allow access to data sources across domains.

You must ensure that web browsers do not allow the navigation of sub-frames across different domains.

You must ensure that web browsers do not allow the submission of non-encrypted critical form data.

You must ensure that your CSP Name Web browser window is closed before navigating to other sites/domains.

You must not store customer information on a system that is not owned by CSP Name.

You must ensure that sensitive information entered into systems is restricted to team members on a need-to-know basis.

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 for Internal Users for CSP Name systems and networks. By my electronic acceptance and/or signature below, I acknowledge and agree that my access to all CSP Name systems and networks is covered by, and subject to, such Rules. Further, I acknowledge and accept that any violation by me of these Rules may subject me to civil and/or criminal actions and that CSP Name 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 Users

You must conduct only authorized business on the system.

Your level of access to systems and networks owned by CSP Name is limited to ensure your access is no more than necessary to perform your legitimate tasks or assigned duties. If you believe you are being granted access that you should not have, you must immediately notify the CSP Name Operations Center *Enter phone number*.

You must maintain the confidentiality of your authentication credentials such as your password. Do not reveal your authentication credentials to anyone; a CSP Name employee should never ask you to reveal them.

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

You must report all security incidents or suspected incidents (e.g., lost passwords, improper or suspicious acts) related to CSP Name systems and networks to the CSP Name Operations Center *Enter phone number*.

You must not establish any unauthorized interfaces between systems, networks, and applications owned by CSP Name.

Your access to systems and networks owned by CSP 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 applicable CSP Name system maintains individual Privacy Act information. Your access to CSP Name systems 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 system resources against waste, loss, abuse, unauthorized use or disclosure, and misappropriation.

You must not process U.S. classified national security information on the system.

You must not browse, search or reveal information hosted by CSP 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 someone who does not have authority to access that information.

You must ensure that Web browsers use Secure Socket Layer (SSL) version 3.0 (or higher) and Transport Layer Security (TLS) 1.0 (or higher). SSL and TLS must use a minimum of 128-bit, encryption.

You must ensure that your web browser is configured to warn about invalid site certificates.

You must ensure that web browsers warn if the user is changing between secure and non-secure mode.

You must ensure that your web browser window used to access systems owned by CSP Name is closed before navigating to other sites/domains.

You must ensure that your web browser checks for a publisher’s certificate revocation.

You must ensure that your web browser checks for server certificate revocation.

You must ensure that web browser checks for signatures on downloaded files.

You must ensure that web browser empties/deletes temporary Internet files when the browser is closed.

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

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

You agree to contact the CSP Name Chief Information Security Officer or the CSP Name Operations Center *Enter phone number* if you do not understand any of these rules.

|  |  |  |  |
| --- | --- | --- | --- |
| ACCEPTANCE AND SIGNATURE | | | |
| I have read the above Rules of Behavior for External Users for CSP Name systems and networks. By my electronic acceptance and/or signature below, I acknowledge and agree that my access to all CSP Name systems and networks is covered by, and subject to, such Rules. Further, I acknowledge and accept that any violation by me of these Rules may subject me to civil and/or criminal actions and that CSP Name 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. | | |

# Acronyms and Definitions

The master list of FedRAMP acronym and glossary definitions for all FedRAMP templates is available on the FedRAMP website [Documents](https://www.fedramp.gov/resources/documents-2016/) page under Program Overview Documents.

Please send suggestions about corrections, additions, or deletions to info@fedramp.gov.