FedRAMP® System Security Plan (SSP) Appendix F: Rules of Behavior (RoB)

for ThreatConnect

ThreatConnect Government Cloud

Version 1.0.1

09.24.2024

Prepared by

Identification of Organization that Prepared this Document	
Organization Name	RISCPoint
Street Address	2814 Detroit Ave
Suite/Room/Building	N/A
City, State, Zip	Cleveland, OH 44113

Prepared for

Identification of Cloud Service Provider	
Organization Name	ThreatConnect
Street Address	3865 Wilson Blvd.
Suite/Room/Building	Suite 550
City, State, Zip	Arlington, VA 22203

Document Revision History

Date	Description	Version	Author
08.23.2024	Initial RoB creation.	1.0.0	RISCPoint
09.24.2024	Updates based upon ThreatConnect Review.	1.0.1	RISCPoint

Table of Contents

1 Introduction

This Rules of Behavior (RoB) document describes how a cloud service provider's (CSP's) personnel and a federal agency's 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.

2 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 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.

3 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.

4 Rules of Behavior

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

a. 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;
b. 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;
c. Review and update the rules of behavior at least annually; and
d. 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**.

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

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

Note: Some Rules of Behavior templates include separate rule listings for privileged and non-privileged users. This approach adds unnecessary administrative overhead and is intentionally reframed in this document. Privileges exist on a spectrum and are dynamic in nature; therefore the distinction is arbitrary and subject to individual interpretation.

- Rules for internal users are denoted in Section 4.1
- Rules for external users are denoted in Section 4.2

4.1 Rules of Behavior for Internal Users

As an individual with or expecting access to ThreatConnect, a product of ThreatConnect, I understand, accept, and agree to the following terms and conditions that apply to my access to, and use of, information, including sensitive information (such as PII, customer data, proprietary information, etc.), or information systems of ThreatConnect.

4.1.1 Access and Use of ThreatConnect Systems

I Agree That I Will:

- Comply with all ThreatConnect and all applicable federal information security, privacy, and records management policies.
- Have NO expectation of privacy in any records that I create or in my activities while accessing or using ThreatConnect.
- Use only ThreatConnect–approved devices, systems, software, services, and data that I am authorized to use, based on my role, when interacting with ThreatConnect.
- Follow established procedures (see ThreatConnect's Policy and Procedure Package) for requesting access to ThreatConnect and for notifying my supervisor or designee when the access is no longer needed.
- Use my access to ThreatConnect systems and/or records for officially authorized and assigned duties only.
- Only use other information systems as expressly authorized by the terms of those systems; personal use is prohibited.
- Use only ThreatConnect–approved solutions for connecting non–ThreatConnect–owned systems to ThreatConnect's network.

I Agree That I Will Not:

- Attempt to probe computer systems to exploit system controls or to obtain unauthorized access to sensitive data.
- Engage in any activity for personal use not expressly approved by policy and procedure.
- Host, set up, administer, or operate any type of Internet server or wireless access point on any ThreatConnect network unless explicitly authorized by the Director of Information Security and Compliance, or designee.
- Utilize social media/networking or public websites, to post or distribute ThreatConnect-specific access credentials, organizational information, system information, or incident-related information without prior approval.
- Disclose any information identified within my required training as sensitive for any reason, except for an explicit business purpose. This includes disclosure of PII, customer data, and other proprietary information.
- Utilize the same password for another system that my ThreatConnect account(s) use(s) for authentication.

4.1.2 Protection of Computing Resources

I Agree That I Will:

- Secure mobile devices and portable storage devices (e.g., laptops, USB flash drives, smartphones, tablets, personal digital assistants (PDA)).
- Remove and securely store any multi factor authentication hard token when not performing my duties.
- Log out of all information systems at the end of each workday.
- Log off or lock any ThreatConnect computer or console before walking away.
- Log out of any ThreatConnect web application or web console when I expect that inactivity will exceed fifteen (15) minutes.

I Agree That I Will Not:

- Swap or surrender ThreatConnect hard drives or other storage devices to anyone other than an authorized ThreatConnect employee.
- Share or otherwise provide my multifactor authentication token or credentials to any other individual.
- Attempt to override, circumvent, alter, or disable operational, technical, or management security configuration controls unless expressly directed to do so by the Director of Information Security and Compliance, Senior Information Security Compliance Analyst, or designee.
- Utilize social media/networking to post or distribute information about ThreatConnect computing resources.

4.1.3 Electronic Data Protection

I Agree That I Will:

- Use only virus protection software, anti-spyware, and firewall/intrusion detection, and any other safeguard software, which is authorized by ThreatConnect.
- Use only components encrypted with FIPS 140–2 (or its successor) validated encryption within the ThreatConnect Authorization Boundary, where possible.
- Use ThreatConnect email in the performance of my duties and never use a non–approved electronic mail system.
- Obtain approval before public dissemination of ThreatConnect information.

I Agree That I Will Not:

- Transmit sensitive information via wireless technologies over an unencrypted or untrusted network.
- Download or store sensitive information (PII, customer data, proprietary information, etc.)) outside of ThreatConnect, for example, corporate-issued laptop or device or any personal devices
- Download software from the Internet, or other publicly available sources, offered as free trials, shareware, or other unlicensed software to a ThreatConnect–owned system

without a business purpose or prior approval, with the understanding that automated restrictions are in place that may restrict access to these tools.
- Disable or degrade software programs used by ThreatConnect that install security software updates to organizational equipment.

4.1.4 Teleworking and Remote Access

I Agree That I Will:

- Keep company furnished equipment and customer information safe, secure, and separated from my personal property and information, regardless of work location. I will protect the equipment that I am issued from theft, loss, destruction, misuse, and emerging threats.
- Obtain approval before using remote access capabilities to connect non–company equipment to ThreatConnect.
- Notify my supervisor or designee before any international travel with a company mobile device (e.g., laptop, smartphone) and upon return. This may include issuing a specifically configured device for international travel and/or inspecting the device or reimaging the hard drive upon return.
- Safeguard sensitive information, in any format, device, system, and/or software in remote locations (e.g., at home and during travel).
- Protect information about remote access mechanisms from unauthorized use and disclosure.
- Exercise a higher level of awareness in protecting ThreatConnect mobile devices when traveling internationally as laws and individual rights vary by country and threats against such devices may be heightened.
- Secure mobile devices and portable storage devices (e.g., laptops, USB flash drives, smartphones, tablets, personal digital assistants (PDA)) when not in use.
- Remove and securely store any multi factor authentication hard token when not performing my duties.
- Log out of all information systems at the end of each workday.
- Log off or lock any ThreatConnect computer or console before walking away.
- Log out of any ThreatConnect web application or web console when I expect that inactivity will exceed fifteen (15) minutes.

I Agree That I Will Not:

- Access non–public technology resources from publicly–available computers, such as remotely connecting to ThreatConnect networks from computers in a public library.
- Access ThreatConnect networks from any foreign country unless approved by my supervisor, Senior Information Security Compliance Analyst, or designee.
- Travel to high-risk designated areas (e.g., those with Level 3 and Level 4 Travel Advisories from the U.S. Department of State) in possession of ThreatConnect assets.

4.1.5 Incident Reporting

I Agree That I Will:

- Report suspected or identified information security incidents including anti-virus, antispyware, firewall or intrusion detection software errors, or significant alert messages (security and privacy) to my supervisor or designee immediately upon suspicion.

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 violates the Computer Fraud and Abuse Act.

4.1.6 Acknowledgment and Acceptance

- I acknowledge that I have received a copy of these Rules of Behavior.
- I understand, accept, and agree to comply with all terms and conditions of these Rules of Behavior.

INTERNAL RoB ACKNOWLEDGEMENT

ACCEPTANCE AND SIGNATURE		
I have read the above Internal Users Rules of Behavior (RoB) for ThreatConnect. By my electronic acceptance and/or signature below, I acknowledge and agree that my access to ThreatConnect 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 ThreatConnect retains the right, at its sole discretion, to terminate, cancel, or suspend my access rights to ThreatConnect systems at any time, without notice.		
User's Legal Name:		(printed)
User's Signature:	X _____	(signature)
Date:	Click here to enter a date.	
Comments:	Click here to enter text.	

4.2 Rules of Behavior for External Users

As an individual, considered customers or partners, with or expecting access to ThreatConnect for Government:

4.2.1 Access and Use of ThreatConnect Systems

I Agree That I Will:

- Attest to the knowledge required and training expertise required by my organization to perform my role.
- Understand and affirm I am aware of the requirements to protect access to and the abilities to utilize protected data within my role responsibilities.
- Understand that authorized ThreatConnect personnel may review my conduct or actions concerning the protection of customer information and information systems and take appropriate action.
- Sign specific or unique RoBs as required for access or use of ThreatConnect. I may be required to comply with a non–ThreatConnect entity's RoB (i.e., that of my employer) when using ThreatConnect. When accessing that entity's tenant of ThreatConnect, I must comply with that entity's RoB.

4.2.2 Sensitive Information

I Agree That I Will:

- Ensure that all material containing ThreatConnect-derived sensitive information is secured when not in use (e.g., encrypted and/or physically secured).
- Provide access to sensitive information only to those who have a need–to–know for their professional duties, including posting sensitive information only to those web-based collaboration tools approved for use and restricted to those individuals who have a need–to–know and when proper safeguards are in place for sensitive information.
- Obtain approval from my supervisor to use, process, transport, transmit, download, print, or store electronic sensitive information remotely (outside of ThreatConnect).
- Protect ThreatConnect-derived sensitive information from unauthorized disclosure, use, modification, or destruction, and will use adequate encryption for the type of information.

I Agree That I Will Not:

- Allow ThreatConnect-derived sensitive information to reside on non–ThreatConnect systems or devices unless specifically designated and authorized in advance by my supervisor.
- If required to download or store sensitive information (PII, customer data, proprietary information, etc.), immediately, upon business purpose expiration, delete all of the sensitive information from the resource.

- Make any unauthorized disclosure of any ThreatConnect-derived sensitive information through any means of communication including, but not limited to, email, instant messaging, online chat, and web bulletin boards or logs.
- Post, utilize or distribute via social media/networking, or public websites information about sensitive data contained within ThreatConnect.

4.2.3 Identification and Authentication

I Agree That I Will:

- Use passwords that meet the ThreatConnect minimum requirements.
- Protect and secure my passwords; verify codes, multi-factor hard or soft tokens, and credentials from unauthorized use and disclosure.

I Agree That I Will Not:

- Remotely access the system via the same mobile device that contains the Multifactor Authentication (MFA) method to access ThreatConnect.
- Hardcode credentials into scripts or programs.
- Utilize the same password for another system that my ThreatConnect account uses for authentication.
- Post, utilize or distribute via social media/networking, or public websites information about my credentials or any identification and authentication mechanism used with or shared with ThreatConnect.

4.2.4 Incident Reporting

I Agree That I Will:

- Report suspected or identified information security incidents including anti-virus, antispyware, firewall or intrusion detection software errors, or significant alert messages (security and privacy) to ThreatConnect immediately upon suspicion following pre-defined notification paths.
- Report any personnel transfer or terminations of personnel who possess ThreatConnect-issued credentials, multifactor hard or soft tokens, or other system access and communicate this transfer or termination to ThreatConnect as early as possible or at least the same day as the transfer or termination.
- Report to my organization’s Incident Response Team, any stolen resources (computers, phones, multifactor hard tokens, etc.) and applicable user accounts that may have ThreatConnect-derived sensitive information or that was previously used to access ThreatConnect.

I Agree That I Will Not:

- Post, utilize or distribute via social media/networking, or public websites information related to incidents reporting, identified, or assumed with regards to ThreatConnect without the express written consent of ThreatConnect.

4.2.5 Acknowledgment and Acceptance

- I acknowledge that I have received a copy of these Rules of Behavior.
- I understand, accept, and agree to comply with all terms and conditions of these Rules of Behavior.

External RoB ACKNOWLEDGEMENT

ThreatConnect links to the latest Rules of Behavior for External Users at the ThreatConnect login page. In line with the NIST 800-53 AC-8 control, continued usage of ThreatConnect constitutes acknowledgement of these rules.