# FedRAMP Recommended Secure Configuration Standard

- **Release:** 25.00A DRAFT
- **Published:** 2025-00-00
- **Designator:** RSC
- **Description:** THIS IS A DRAFT AND IS NOT FINALIZED, USE AT YOUR OWN RISK. Initial DRAFT release of the Recommended Secure Configuration Standard (RSC) after public comment.

## Front Matter

### Effective Date(s) & Overall Applicability

- **FedRAMP 20x**:
  - This release is effective **2025-00-00** for **20x**.
  - This policy applies to all FedRAMP 20x authorizations.
- **FedRAMP Rev5**:
  - This release is effective **2026-03-01** for **Rev5 (Wide Release)**.
  - This policy applies to all FedRAMP Rev5 authorizations as a supplement to SSP Appendix J: CSO CIS and CRM Workbook (both are required).
  - All cloud service offerings seeking FedRAMP Rev5 authorization MUST implement the Recommended Secure Configuration Standard (RSC) starting on the Effective Date for Rev5 authorizations.
  - All cloud service offerings with an active FedRAMP Rev5 authorization MUST implement the Recommended Secure Configuration Standard (RSC) no later than their next annual assessment that begins after the Effective Date for Rev5 authorizations.

### Documentation Guidelines

The following FedRAMP documentation guidelines apply to this document:

- The capitalized key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in IETF RFC 2119.
- FedRAMP-specific terms defined in FRD-ALL (FedRAMP Definitions) are italicized throughout this document for reference.

## Background & Authority

- Executive Order 14144 Strengthening and Promoting Innovation in the Nation's Cybersecurity Section 3 (d), as amended by Executive Order 14306 Sustaining Select Efforts to Strengthen the Nation's Cybersecurity and Amending Executive Order 13694 and Executive Order 14144 to Section 3 (b), states "the Administrator of General Services, acting through the Director of the Federal Risk and Authorization Management Program (FedRAMP), in coordination with the Secretary of Commerce, acting through the Director of NIST, and the Secretary of Homeland Security, acting through the Director of CISA, shall develop FedRAMP policies and practices to incentivize or require cloud service providers in the FedRAMP Marketplace to produce baselines with specifications and recommendations for agency configuration of agency cloud-based systems in order to secure Federal data based on agency requirements."

### Purpose

All customers benefit from simple, easy to follow, easy to understand instructions for securely configuring a cloud service offering. Cloud service providers often provide a wide range of configuration options to allow individual customers to pick

and choose their security posture based on their individual customer needs and are best positioned to provide instructions about the overall security impacts of many of these choices.

This standard outlines simple requirements for FedRAMP authorized cloud service providers to effectively communicate the security impact of common settings to new and current agency customers.

---

## Requirements and Recommendations

### FRR-RSC

**These requirements and recommendations apply ALWAYS to ALL FedRAMP Authorized cloud services based on the current Effective Date(s) and Overall Applicability of this standard.**

#### FRR-RSC-01

*Applies to:* Low, Moderate, High

> Providers MUST create and maintain guidance that includes instructions on how to securely access, configure, operate, and decommission *top-level administrative accounts* that control enterprise access to the entire *cloud service offering*.
>
> *Note: This guidance should explain how _top-level administrative accounts* are named and referred to in the *cloud service offering._*

#### FRR-RSC-02

*Applies to:* Low, Moderate, High

> Providers MUST create and maintain guidance that explains security-related settings that can be operated only by *top-level administrative accounts* and their security implications.

#### FRR-RSC-03

*Applies to:* Low, Moderate, High

> Providers SHOULD create and maintain guidance that explains security-related settings that can be operated only by *privileged accounts* and their security implications.

#### FRR-RSC-04

*Applies to:* Low, Moderate, High

> Providers SHOULD set all settings to their recommended secure defaults for *top-level administrative accounts* and *privileged accounts* when initially provisioned.

#### FRR-RSC-05

*Applies to:* Low, Moderate, High

> Providers SHOULD offer the capability to compare all current settings for *top-level administrative accounts* and *privileged accounts* to the recommended secure defaults.

**FRR-RSC-06**

*Applies to:* Low, Moderate, High

> Providers SHOULD offer the capability to export all security settings in a *machine-readable* format.

**FRR-RSC-07**

*Applies to:* Low, Moderate, High

> Providers SHOULD offer the capability to view and adjust security settings via an API or similar capability.

**FRR-RSC-08**

*Applies to:* Low, Moderate, High

> Providers SHOULD provide recommended secure configuration guidance in a *machine-readable* format that can be used by customers or third-party tools to compare against current settings.

**FRR-RSC-09**

*Applies to:* Low, Moderate, High

> Providers SHOULD make recommended secure configuration guidance available publicly.

**FRR-RSC-10**

*Applies to:* Low, Moderate, High

> Providers SHOULD provide versioning and a release history for recommended secure default settings for *top-level administrative accounts* and *privileged accounts* as they are adjusted over time.

---