PROGRAM MANAGEMENT OFFICE CHARTER

VERSION:
2.0

DATE:
February 2021

TABLE OF CONTENTS

1. DOCUMENT REVISION HISTORY

Date	Description	Version	Governing Body
8/20/2020	Original Publication	1.0	StateRAMP Steering Committee
9/24/2020	Amended for Policy Consistency	1.1	StateRAMP Steering Committee
01/08/2021	CSP definition update (Technical Correction)	1.2	StateRAMP Staff
02/15/2021	Amended to meet 501c(6) requirements	2.0	StateRAMP Board of Directors

2. PURPOSE

The purpose of this Charter is to define the requirements, standards, and responsibilities associated with any Program Management Office (PMO) doing business with the StateRAMP organization.

3. BACKGROUND

Using the Federal Risk and Authorization Management Program (FedRAMP) and the National Institute of Standards and Technology (NIST) as models, Chief Information Officers (CIOs) from private industries and state governments in partnership with Chief Information Security Officers (CISOs), non-governmental organizations, and national associations worked to develop StateRAMP—a nonprofit whose mission is to bring together state and local governments, cybersecurity experts, and service providers to develop industry best practices, policies, and education to promote the integrity and ongoing protection of citizen and government data.

To ensure the technical standards published by StateRAMP and adopted by state and local governments are being upheld, StateRAMP will appoint up to three PMOs who are responsible for the assessment and verification of security packages submitted by StateRAMP members for review.

4. ORGANIZATIONAL REQUIREMENTS

Organizations who wish to be appointed by StateRAMP as a preferred PMO must meet the following minimum requirements and standards:

1. Possess the necessary technical knowledge and capabilities to provide States, agencies, local governments, third party assessment organizations (3PAOs) and service providers with a standard approach and guidance related to the security authorization process
2. Use the templates and forms provided by StateRAMP
3. A minimum of 5 years serving state and local governments as a Managed Service Provider (MSP)
4. Actively manage within their government MSP programs a minimum of 1,000 vendors
5. Possess a minimum of one State government cooperatively awarded contract
6. Agree to adopt and implement the StateRAMP PMO pricing model
7. Possess the necessary cybersecurity staff with the appropriate minimum credentials as W2 employees
8. Agree to the StateRAMP Conflict of Interest Policy wherein conflicts will be managed by the StateRAMP Board or Board-delegated committee using a 3PAO to act as the PMO as needed
9. Ability to comply with StateRAMP key performance indicators (KPIs) and quality metrics, understanding a failure to meet StateRAMP performance standards may result in the remedial activities
10. Agree to serve as a non-voting member on the StateRAMP Standards & Technical Committee
11. Agree to work with the StateRAMP Appeals Committee as required
12. Pay PMO Membership fee, as prescribed by the Board of Directors, to StateRAMP

5. TECHNOLOGY REQUIREMENTS

Organizations who wish to be appointed by StateRAMP as a preferred PMO must agree to use the StateRAMP Technology, tool(s) and software selected by the StateRAMP Board of Directors, to manage service provider accounts, documentation, compliance, and reporting.

StateRAMP is responsible for providing accounts within the StateRAMP Technology with the appropriate access and permissions to the PMO.

Any information stored, transmitted, or managed by the PMO outside of the StateRAMP Technology must be maintained in a secure credentialing repository which is FedRAMP Authorized at the Moderate Impact Level or higher.

The Board shall select a technology solution for the StateRAMP Technology which meets the following requirements:

1. Must be a cloud-based system with compliance management functionality
2. Must be FedRAMP Ready, In Process or ATO at the Moderate Impact Level or higher or have been assigned a StateRAMP Authorized Status at Category 2 or higher
3. Must be an awardee of a State Government Cooperative publicly competed procurement

6. OBJECTIVES

The PMO will work to execute the following activities which include, but are not limited to:

1. The creation of processes to allow agencies, state and local governments, and service providers to comply with StateRAMP security authorization requirements approved by the Board, including:
    a. A system for aligning agency-specific security and privacy requirements with the StateRAMP authorization standards
    b. A method for agencies, state and local governments, and service providers to request to begin the security authorization process
    c. Guidance for agencies and States to satisfy StateRAMP security requirements when a desired service provider has not been prioritized for review by the PMO
2. Gather and prioritize authorization requests and authorization assessment results for review in accordance with the authorization prioritization criteria provided by the Board
3. Maintain the StateRAMP approval que on an ongoing basis
4. Adopt and/or implement a secure credentialing management system to catalogue authorization requests, government-preferred security packages, and security packages approved by the Board
5. Utilize StateRAMP approved templates that can satisfy security authorization requirements using standard contract language and service level agreements (SLAs) for use in the acquisition of cloud services
6. Attend required committee meetings, including but not limited to StateRAMP Standards & Technical Committee and StateRAMP Appeals Committee

7. CHARTER REVIEW

This Charter will be reviewed annually to evaluate its accuracy, effectives, and relevancy. Changes and improvements to the Charter must be approved by a majority consensus among all StateRAMP Governing Board members.

8. CHARTER ADOPTION

This Charter was adopted by the StateRAMP Board of Directors on the [date].