StateRAMP

DATA CLASSIFICATION TOOL

VERSION:
1.2

DATE:
April 29, 2022

TABLE OF CONTENTS

1. DOCUMENT REVISION HISTORY

Date	Description	Version	Governance Body
December 2020	Original Publication	1.0	StateRAMP Steering Committee
October 2021	Security status updates	1.1	StateRAMP Staff
April 2022	Updates	1.2	StateRAMP Standards and Technical Committee and Board

2. INTRODUCTION AND PURPOSE

This document is intended to be used by state and local governments and procurement officials as a tool for determining the appropriate StateRAMP security requirements in solicitations with the intent of procuring a service provider using or offering IaaS, SaaS, and/or PaaS solutions that process, store, and/or transmit government data including PII, PHI, and/or PCI.

According to the Federal Information Security Management Act (FISMA) requirements, there are three distinct security objectives for information and information systems: confidentiality, integrity, and availability. These standards are used as the foundation to ensure vendors are providing solutions that meet the minimum security requirements to process, store, and transmit certain types of government data.

It is necessary for States to accurately determine their required security baseline prior to publishing a solicitation so that the State can select a vendor that meets the government's needs and provides the appropriate security controls to protect the government data. This data classification self-assessment is based on the NIST 800-53 Revision 4 requirements and designed to help state and local governments easily identify the appropriate StateRAMP security category to include a solicitation.

3. INSTRUCTIONS

Answer the questions in the survey section to determine what StateRAMP security category requirements you need to include in your solicitation to ensure your data is protected.

4. SURVEY QUESTIONS

1. Will the vendor process, transmit, and/or store non-sensitive State data, metadata, and/or data that may be released to the public that requires no additional levels of protection?
    a. If yes, StateRAMP Low is recommended.
2. Will the vendor process, transmit, and/or store personally identifiable information (PII) as defined by the U.S. Department of Labor (DOL)?
    a. If yes, StateRAMP Moderate is recommended.
3. Will the vendor process, transmit, and/or store protected health information (PHI) as defined by the Health Insurance Portability and Accountability Act (HIPAA)?
    a. If yes, StateRAMP Moderate is recommended
4. Will the vendor process, transmit, and/or store payment card industry (PCI) data as defined by the PCI Security Standards Council (PCI SSC)?
    a. If yes, StateRAMP Moderate is recommended
5. Will the loss or unavailability of the data that is processed, transmitted, and/or stored by the service provider result in a disruption to government operations?
    a. If yes, StateRAMP Moderate is recommended
6. Will the loss or unavailability of the data that is processed, transmitted, and/or stored by the service provider result in a loss of confidence or trust in the government?
    a. If yes, StateRAMP Moderate is recommended
7. Will the vendor process, transmit, and/or store criminal justice information (CJI) data?
    a. If yes, StateRAMP Moderate is recommended.
    b. Note: States may add additional controls to StateRAMP Moderate to comply with the CJIS requirements.

5. NEXT STEPS

Data processed, transmitted, and/or stored by the vendor includes information shared inside and outside of the provider’s cloud service application. Similarly, if state or local laws have identified any other data type not included in the survey above as confidential, a StateRAMP Moderate is recommended. Once a determination has been made regarding the appropriate StateRAMP impact level that should be required from vendors, partner with the information security team, Chief Information Officer, and Chief Information Security Officer to ensure the appropriate standards have been met.