DATA CLASSIFICATION TOOL

VERSION:
1.0

DATE:
December 17, 2020

TABLE OF CONTENTS

1. DOCUMENT REVISION HISTORY

Date	Description	Version	Governance Body
12/17/2020	Original Publication	1.0	StateRAMP Steering Committee

2. INTRODUCTION AND PURPOSE

This document is intended to be used by state governments and procurement officials as a tool for determining the appropriate StateRAMP or FedRAMP security requirements in a request for proposal (RFP) 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 service providers 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 an RFP so that the State can select a service provider that meets the State's needs and provides the appropriate security controls to protect the State's 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 in an RFP.

3. INSTRUCTIONS

Answer the questions in the survey section to determine what StateRAMP security category requirements you need to include in your RFP to ensure your data is protected. Because of the level of reciprocity between StateRAMP and FedRAMP, a StateRAMP Category 1 requirement is equivalent to a FedRAMP Low Impact and a StateRAMP Category 3 requirement is equivalent to a FedRAMP Moderate Impact.

4. SURVEY QUESTIONS

1. Will the service provider 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 Category 1 is required.
2. Will the service provider process, transmit, and/or store personally identifiable information (PII) as defined by the U.S. Department of Labor (DOL)?
    a. If yes, StateRAMP Category 3 is required.
3. Will the service provider process, transmit, and/or store protected health information (PHI) as defined by the Health Insurance Portability and Accountability Act (HIPAA)?
    a. If yes, StateRAMP Category 3 is required.
4. Will the service provider process, transmit, and/or store payment card industry (PCI) data as defined by the PCI Security Standards Council (PCI SSC)?
    a. If yes, StateRAMP Category 3 is required.
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 Category 3 is required.
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 Category 3 is required.
7. Will the service provider process, transmit, and/or store criminal justice information (CJI), foreign affairs information, federal critical infrastructure information, national security information, and/or global trade information?
    a. If yes, FedRAMP High Impact is required.

5. NEXT STEPS

Remember that data processed, transmitted, and/or stored by the service provider 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 Category 3 is required. Once a determination has been made regarding the appropriate StateRAMP or FedRAMP security category that should be required from service providers, be sure to partner with the information security team, Chief Information Officer, and Chief Information Security Officer to ensure the appropriate standards have been met.