Redacted

# CONFIGURATION MANAGEMENT PLAN (CMP)

Redacted

**VERSION:**
**1.0**
**DATE:**
**20220901**

## EXECUTIVE SUMMARY

This document supports configuration management and contains the CMP for Redacted A CMP describes the measures for establishing the configuration baseline and managing configurations for all information system components. It also describes the change management process and the security considerations that are built into the process to ensure secure configurations are maintained. These configurations and change management efforts are integral to managing security risks for the information system.

## SYSTEM SECURITY PLAN

### PREPARED BY

| IDENTIFICATION OF ORGANIZATION THAT PREPARED THIS DOCUMENT | | | |
|---|---|---|---|
| Redacted | Organization Name | Redacted | |
| | Street Address | | |
| | Suite/Room/Building | | |
| | City, State Zip | | |

### PREPARED FOR

| IDENTIFICATION OF CLOUD SERVICE PROVIDER | | | |
|---|---|---|---|
| Redacted | Organization Name | Redacted | |
| | Street Address | | |
| | Suite/Room/Building | | |
| | City, State Zip | | |

## TEMPLATE REVISION HISTORY

| DATE | DESCRIPTION |
|---|---|
| 9/1/22 | Original publication |

## DOCUMENT REVISION HISTORY

| DATE | DESCRIPTION | VERSION OF CMP | AUTHOR |
|---|---|---|---|
| | | | |
| | | | |
| | | | |

### HOW TO CONTACT US

For technical questions about this document contact Redacted

# TABLE OF CONTENTS



## LIST OF TABLES

# 1. INTRODUCTION & PURPOSE

Information systems are vital to Redacted mission/business functions; therefore, it is critical that the information system components are securely configured and that all changes to the system are strictly controlled. This CMP describes the comprehensive procedures used to establish secure configurations and subsequently coordinate, manage, control, test, implement, and validate all changes to the system. An information system is typically in a constant state of change in response to new, enhanced, corrected, or updated hardware and software capabilities, patches for correcting software flaws, and other errors to existing components, new security threats, changing business functions, etc.

Implementing information system changes almost always results in some adjustment to the system configuration. To ensure that the required adjustments to the system configuration do not adversely affect the security of the information system or the organization from operation of the information system, a well-defined configuration management process that integrates information security is needed. One of the goals of a CMP is to manage and monitor the configurations of information systems to achieve adequate security and minimize organizational risk while supporting the desired business functionality and services. This includes configuration management activities at both the organizational and system levels.

# 2. SCOPE

This CMP has been developed for [redacted], which is classified as a **Category 2** system, in Section 15 of the StateRAMP SSP Data classification tool. The procedures in this CMP have been developed for a **Category 2** system and are designed to ensure control over any changes made to the system.

This CMP does not include customer responsibilities.

# 3. SYSTEM DESCRIPTION

Redacted an SaaS feedback analytics solution for higher education. With specialized modules, including Redacted empowers your institutional research efforts with survey tools that engage diverse perspectives, and analytics that maximize effectiveness.

# 4. CONFIGURATION MANAGEMENT POLICY

Redacted configuration management policy can be found in SSP_A_CMP as SE_SSP_A_CMP_V1_20220901.

# 5. ROLES AND RESPONSIBILITIES

Redacted establishes multiple roles and responsibilities to establish secure configurations and subsequently coordinate, manage, control, test, implement, and validate all changes to the information system.

| ROLE | RESPONSIBILITIES |
|---|---|
| Programming Lead | • Review of change request tickets<br>• Peer review of change |
| President | • Approve or deny a change to information system |
| Programmer | • Have access to the configuration items in change management system<br>• Code approved change requests |

*Table 2-3. Roles and Responsibilities*

# 6. BASELINE CONFIGURATION MANAGEMENT

All system baselines are created and maintained by the System Administrator. Changes are requested and approved through the System Administrator with override approval at the discretion of the Company President.

# 7. REQUESTING A CHANGE

## 7.1 CHANGE TYPES AND SCHEDULES

Information systems are made up of different deployment models. The deployment models of the [redacted] system that are defined in this SSP and are not leveraged by any other StateRAMP Authorizations, are indicated in Table 8-2 Cloud Deployment Model Represented in this SSP that follows.

| CHANGE TYPE | TIMELINE | REQUIRED APPROVALS |
|---|---|---|
| Normal | 1-2 weeks | System Administrator |
| Expedited | Less 1 week | System Administrator or Company President |
| Emergency | Immediate/same day | System Administrator |
| Routine | Ongoing and new entries added to change schedule | System Administrator |

*Table 8-2. Cloud Deployment Model Represented in this SSP*

## 7.2 CHANGE PLANNING

Planning considers if the requested change is appropriate for the environment, is it necessary, who it will impact, when will it be completed, what is the desired outcome, what constitutes a successful

change, who needs to approve the change, and will other plans such as Disaster Recovery or Incident Response Management require updating based on this change.

1. Summary
2. Planning
3. Impact
4. Schedule
5. Assessment
6. Authorize
7. Schedule
8. Implement
9. Review
10. Close/cancel

## 7.3 CHANGE TESTING AND SECURITY IMPACT ANALYSIS

*Proposed changes are presented through the internal ticket system. Software and Security audits of proposed changes are handled by the System Administrator. Any concerns are presented to the Company Owner for final approval.*

## 7.4 CHANGE IMPLEMENTATION

*After a change is approved it is first staged in a test environment mirroring the production systems. Based on potential impact of changes it may be tested in a virtual machine environment as part of the production system. It is ultimately applied to the appropriate production system(s).*

## 7.5 CHANGE CONTROL AND DOCUMENTATION

*Major changes are documented in the internal ticketing system. This and any additional required information are also added to the internally maintained document repository.*

## 7.6 CHANGE MONITORING

*All changes are monitored and reviewed as part of the existing system for this functionality. New controls may be created in the event that changes cause major impacts on underlying structure.*

## 7.7 COMMUNICATION AND REPORTING OF CHANGES

*Major changes are discussed between senior programming staff and the system administrator directly. This information is then presented in an email and depending on the extent of changes a department wide (or company wide) meeting.*

## 7.8 MAINTENANCE WINDOW

Redacted *is a high availability platform. Maintenance is conducted on individual components ation system outside of standard business hours based on the PST timezone to impact as few clients as possible and to have the smallest amount of load. General maintenance generally runs from 2030 EST until 2330 EST. Additional automated maintenance tasks run in the window of 0200 EST until 0530 EST*