Insert Logo Here

Organization Name

Security Policy

Security Assessment & Authorization

Version 1.0

April 6, 2021

Proprietary and Confidential

For Authorized Use Only

Document Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Description | Author |
| 4/6/2021 | 1.0 | Published CA Policy | Noah Brown, CISO |

Table of Contents

[1 Introduction 1](#_Toc60976762)

[2 Purpose 1](#_Toc60976763)

[3 Scope 1](#_Toc60976764)

[4 Roles and Responsibilities 1](#_Toc60976765)

[5 Management Commitment 2](#_Toc60976766)

[6 Authority 3](#_Toc60976767)

[7 Compliance 3](#_Toc60976768)

[8 Policy Requirements 4](#_Toc60976769)

[8.1 Security Assessment and Authorization Policies and Procedures 4](#_Toc60976770)

[8.2 Security Assessments 4](#_Toc60976771)

[8.3 System Interconnections 4](#_Toc60976772)

[8.4 Plan of Action and Milestones 5](#_Toc60976773)

[8.5 Security Authorization 5](#_Toc60976774)

[8.6 Continuous Monitoring 5](#_Toc60976775)

[8.7 Penetration Testing 6](#_Toc60976776)

[8.8 Internal System Connections 6](#_Toc60976777)

# Introduction

has developed corporate policies that identify the security requirements for its information systems and personnel to ensure the integrity, confidentiality, and availability of its information. These policies are set forth by management and in compliance with the Security Assessment & Authorization family of controls found in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 4.

# Purpose

The purpose of these policies is to establish security assessment and authorization requirements to ensure the confidentiality, integrity, and availability of systems, facilities, and data are protected. These policies are consistent with applicable state and federal laws, Executive Orders, directives, regulations, standards, and guidance.

# Scope

The provisions of these policies pertain to all employees, contractors, third parties, and others who have access to company and customer confidential information within systems and facilities.

# Roles and Responsibilities

These policies apply to all employees, contractors, business partners, third parties, and others who need or have access to systems and our customer's confidential information.

| **Individual or Group** | **Role** | **Responsibility** |
| --- | --- | --- |
|  | CEO | Highest-level official with overall responsibility to develop, implement, and maintain accountability, active support, oversight, and management commitment for information security objectives. |
|  | President | Responsible for developing, implementing, maintaining, and ensuring compliance with information security policies, procedures, and controls. Has final responsibility for information security program. |
|  | Information Owner | Has statutory, management, or operational authority for information. Responsible for developing, implementing, and maintaining policies and procedures governing information generation, collection, processing, dissemination, and disposal. |
|  | Authorizing Official | Responsible for operating information system at an acceptable level of risk to organizational operations and assets. |
|  | Authorizing Official Designated Representative | Acts on behalf of Authorizing Official to coordinate and conduct day-to-day activities associated with security authorization process. |
|  | Information Security Manager | Responsible for conducting information system security engineering activities.  Responsible for providing for appropriate security, to include management, operational, and technical controls. |
|  | Information Technology Manager | Responsible for the procurement, development, integration, modification, operation, maintenance, and disposal of an information system. |
|  | Information System Security Officer | Responsible for ensuring that the appropriate operational security posture is maintained for an information system, responsible for ensuring coordination among groups is managed and maintained for these policies/procedures. |
|  | System Administrator | Responsible for conducting information system security Administration activities. |
|  | Managers | Responsible for understanding, enforcing, and complying with control requirements defined in Policies and Procedures |
|  | Users | Responsible for understanding and complying with Policies and Procedures. |

# Management Commitment

and its management are fully committed to protecting the confidentiality and integrity of corporate proprietary and production systems, facilities, and data as well as the availability of services in the system by implementing adequate security controls.

# Authority

These policies and procedures are issued under the authority of the Information Owner. The following applicable laws, directives, policies, regulations, and standards were used as part of the development for this policy. These include, but are not limited to:

1. E-Government Act of 2002/Federal Information Security Management Act of 2002 (FISMA)
2. The Privacy Act of 1974
3. Clinger-Cohen Act of 1996
4. OMB Circulars and Memoranda
5. Federal Information Processing Standards (FIPS)
6. NIST Special Publications
7. OMB Memorandum for Chief Information Officers and Chief Acquisition Officers: Ensuring New Acquisitions Include Common Security Configurations, June 2007
8. OMB Memorandum for Agency CIOs: Security Authorization of Information Systems in Cloud Computing Environments, December 2011

# Compliance

Compliance with these policies is mandatory. It is ’s policy that production systems meet or exceed the requirements outlined in this document. The Information Owner will periodically assess compliance with these policies by using an independent audit performed annually by an external vendor to identify areas of non-compliance. Any findings identified in the audit will be remediated in accordance with the auditing team’s recommendations.

# Policy Requirements

The following security assessment and authorization requirements, mechanisms, and provisions are to be followed by all employees, management, contractors, and other users who access and support the Organization Name information systems.

## Security Assessment and Authorization Policies and Procedures

This document is intended to serve as the *Security Assessment and Authorization Policy* and is made available to all applicable personnel. The associated procedure(s) to facilitate the implementation of the *Security Assessment and Authorization Policy* and related physical and environmental protection controls have been developed, documented, and disseminated to all applicable personnel.

The Information Owner will review and update the *Security Assessment and Authorization Policy* every three (3) years and the procedure(s) at least annually or any time there are significant changes in software or security. Updates must be made to keep the policy and procedure(s) in alignment with Organization Name overall business goals and risk position. Any updates, improvements, or suggestions regarding the *Security Assessment and Authorization Policy* and/or procedure(s) must be sent to the Information Owner.

## Security Assessments

Organization Name must develop a security assessment plan describing the scope of the assessment, including:

* Security controls and control enhancements under assessment
* Assessment procedures to be used to determine security control effectiveness
* Assessment environment, assessment team, and assessment roles and responsibilities

At least annually, must coordinate with an accredited FedRAMP third party assessment organization (3PAO) to assess the security controls in the information system to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.

The 3PAO will provide a security assessment report that documents the results of the assessment and submit the report to Information Security Officer for review. The results of the security control assessment will also be provided in writing, to the and customer Authorizing Official (AO). The 3PAO who conducts the assessment of the security controls in the information system must be given a sufficient level of independence to conduct the assessment.

As part of the annual security assessments, must conduct announced vulnerability scanning and other defined forms of security assessments. must accept the results of an assessment of the information system performed by an accredited 3PAO when the assessment meets conditions of the customer Authorizing Official (AO).

## System Interconnections

must authorize connections from dotStaff to other information systems outside of the authorization boundary through the use of Interconnection Security Agreements. For each interconnection, the interface characteristics, security requirements, and the nature of the information communicated must be documented.

The Interconnection Security Agreements must be reviewed and updated at least annually and on input from the Authorizing AO. If required by a State government customer, must prohibit direct connection to an unclassified, non-national security system to an external network without the use of boundary protections. A deny-all, permit by exception policy for allowing the information system to connect to external information systems will be employed in the system.

## Plan of Action and Milestones

A plan of action and milestones (POA&M) must be developed for information to document the planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security controls, during continuous monitoring activities, as a result of regular security scans, and as circumstances arise in order to reduce or eliminate known vulnerabilities in the system.

The existing plan of action and milestones must be updated at least monthly based on the findings from security controls assessments, security impact analyses, and continuous monitoring activities. The completed POA&Ms must be delivered to all State customer Authorizing Officials at least monthly.

## Security Authorization

must assign a senior-level executive or manager to the role of authorizing official for information. The authorizing official authorizes information for processing before commencing operations and update the security authorization at least every three (3) years or when a significant change occurs.

## Continuous Monitoring

must work in conjunction with sponsoring agency customers to establish a continuous monitoring strategy and implement a continuous monitoring program that includes:

* Establishment of metrics identified by the FedRAMP Continuous Monitoring Strategy Guide
* Annual monitoring and assessments supporting such monitoring
* Ongoing security control assessments in accordance with the information continuous monitoring strategy
* Ongoing security status monitoring of organization-defined metrics in accordance with the organizational continuous monitoring strategy
* Correlation and analysis of security-related information generated by assessments and monitoring
* Response actions to address results of the analysis of security-related information
* Reporting the security status (POA&M) of the organization and the information system from vulnerability scans performed monthly by and annually performed by an independent assessor to appropriate organizational officials
* Employ assessors or assessment teams to monitor the security controls in the information system on an ongoing basis

## Penetration Testing

must conduct penetration testing at least annually on external-facing components and employ an independent penetration agent or penetration team to perform penetration testing on the information system or system components.

## Internal System Connections

must authorize internal connections of -defined components to the information system and for each internal connection, the interface characteristics, security requirements, and the nature of the information communicated must be documented.