Insert Logo Here

Organization Name

Security Procedure

Contingency Planning

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 CP Procedure | Noah Brown, CISO |

Table of Contents

[1 Introduction 1](#_Toc68605489)

[2 Purpose 1](#_Toc68605490)

[3 Scope 1](#_Toc68605491)

[4 Roles and Responsibilities 1](#_Toc68605492)

[5 Management Commitment 2](#_Toc68605493)

[6 Authority 3](#_Toc68605494)

[7 Compliance 3](#_Toc68605495)

[8 Procedural Requirements 4](#_Toc68605496)

[8.1 CONTINGENCY PLAN 4](#_Toc68605497)

[8.1.1 Disaster Recovery Team Lead 4](#_Toc68605498)

[8.1.2 War Room Establishment and Activities 4](#_Toc68605499)

[8.1.3 Customer Communication 4](#_Toc68605500)

[8.2 Review and Distribution 5](#_Toc68605501)

[8.3 Incident Response and Capacity Planning 5](#_Toc68605502)

[8.4 Resuming Essential Missions and Business Functions 5](#_Toc68605503)

[8.5 Identifying Critical Assets 5](#_Toc68605504)

[8.6 TRAINING and TESTING 5](#_Toc68605505)

[8.7 ALTERNATE STORAGE and PROCESSING SITES 6](#_Toc68605506)

[8.7.1 Site Locations 6](#_Toc68605507)

[8.8 TELECOMMUNICATIONS 7](#_Toc68605508)

[8.9 BACKUPS 7](#_Toc68605509)

[8.10 Backup Testing 8](#_Toc68605510)

[8.11 RECOVERY AND RECONSTITUTION 8](#_Toc68605511)

# Introduction

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

# Purpose

This document defines the information contingency planning procedures. These procedures are in place to facilitate the implementation of the Contingency Planning Policy and associated access controls. In accordance with the policy, these procedures detail how information shall implement and maintain secure access controls on all applicable information systems.

# 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 procedures is mandatory. It is 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.

# Procedural Requirements

The following contingency planning requirements, mechanisms, and provisions are to be followed by all employees, management, contractors, and other users who access and support the information systems.

## CONTINGENCY PLAN

In the event of a disaster or emergency, the {SSP\_A\_ISCP\_VX.X\_YYYYMMDD} will be used to maintain the essential missions and business functions of dotStaff, security measures, and to facilitate communicate with internal stakeholders and external users.

* Recovery objectives and restoration priorities: dotStaff provides for the recovery and reconstitution of its StateRAMP Cloud Services to the most recent available state following a disaster.

### Disaster Recovery Team Lead

If the contingency plan is activated, the following individuals are responsible for managing the execution of the recovery process:

|  |  |  |  |
| --- | --- | --- | --- |
| Title | Name | Responsibilities | Contact |
| Disaster Recovery Team Lead |  | Notify organizational officials of a disaster and rally team members. |  |
| Assistant Disaster Recovery Lead |  | Coordinate contingency response activities |  |

### War Room Establishment and Activities

Once a war room has been established, the following activities will take place:

* Determination of initial message to customers
* The development of a communication timeline for Program Managers to follow to begin notifying customers via email of the disruption and recovery actions being taken
* Identification of the communication owners
* The restoration of complete information system security for complete details, see {SSP\_A\_ISCP\_VX.X\_YYYYMMDD}

### Customer Communication

Communication with customers will be conducted via email by the appropriate {Role}. Customers will receive an initial notice of the disruption and follow-up communication detailing the outcome of the recovery activities, including the following information:

* Initial notification of the disruption and recovery activities will include the following information:
	+ Reason for disruption
	+ Impact result of the failover
	+ Expected timing for the restoration of the system
	+ A high-level testing summary
	+ Plans for expected follow-up communications once the restoration is complete
* Communication sent after the completion of the recovery will include the following information:
	+ Detailed incident information
	+ Confirmation of the system restoration
	+ A testing summary
	+ Outline of expected future failback timing and coordination

## Review and Distribution

It is the responsibility of Contingency Plan Coordinator to distribute the contingency plan to the following individuals, including any changes to the plan:

* Contingency Plan Director
* Contingency Plan Coordinator
* Contingency Team Members (Identified in ISCP)

It is the responsibility of the {Role/Team} in coordination with the Contingency Plan Coordinator to review the contingency plan on an annual basis, whenever there are changes to the information system infrastructure and environment or problems identified during testing phases.

 shall protect the contingency plan from unauthorized disclosure and modification, and upon changes to the contingency plan, {Department} shall be notified.

## Incident Response and Capacity Planning

Contingency personnel will meet with incident response personnel to coordinate activities, including other organizational elements responsible for related plans at least once a year.

It is the responsibility of the {Role} to conduct capacity planning on the information system processing, telecommunications, and environmental support. Results should be documented and stored.

## Resuming Essential Missions and Business Functions

Organization Name plans for the resumption of essential missions and business functions within a period of contingency plan activation.

The Recovery Time Objective (RTO) the maximum period between decision to activate the recovery processes and the point at which a customer can resume operations in the secondary environment.

## Identifying Critical Assets

Critical information system assets supporting essential missions and business functions are documented in the {SSP\_A\_ISCP\_VX.X\_YYYYMMDD}

## TRAINING and TESTING

 will train contingency personnel in their roles and responsibilities on an annual basis and as required by information system changes. When a new employee assumes a role outlined in the contingency plan, training will be conducted within fourteen (14) business days.

 will test the contingency plan annually using a live exercise or a table-top test. Special consideration will be taken to ensure testing is coordinated with elements responsible for related plans. During the annual test, the following actions will be taken:

* Coordination of the testing and exercises with other personnel responsible for related plans
* Documentation of testing information, including:
	+ Test scenario details
	+ A list of individuals participating
	+ The testing method
	+ Results from the exercise
	+ Lessons learned
	+ Corrective action to be taken as a result of the test
* Upload the results of the testing exercises to the Security Offices secure online document repository

## ALTERNATE STORAGE and PROCESSING SITES

### Site Locations

The Contingency Planning Team, will establish and document the alternate storage and processing sites for . All alternate sites will provide information security safeguards equivalent to those of the primary site. The current primary and alternate storage and processing sites are the locations listed below. Since the dotStaff primary and alternate storage and processing sites are separated they are therefore not susceptible to the same threats.

* Primary storage and processing site: **{Hosting Name/Region}**
* Alternate storage and processing site: **{Hosting Name/Region}**

**Accessibility Problems**

 has identified the following potential accessibility problem to the alternate storage and processing sites:

* The alternate storage facility is co-located at the alternate processing facility and delivery of backups is electronic. For complete details, see the {SSP\_A\_ISCP\_VX.X\_YYYYMMDD}

**Remediation Actions to the Accessibility Problems**

No remediation actions need to be taken to address accessibility problems for the storage and processing sites listed above.

**Agreements**

The Contingency Planning Team will ensure that alternate storage and processing site agreements are in place, are current, and accurately reflect the information system environment and contingency planning needs to resume essential functions within the Recovery Time Objective (RTO).

The RTO is the maximum period of time between decision to activate the recovery processes and the point at which the customer can resume operations in the standby environment. Organization Name will also ensure that necessary equipment and supplies are available at the alternate site or ready to be in place within the defined time period. Additionally, alternate sites will provide information security safeguards equivalent to those of the primary site.

Priority-of-service provisions are included in all alternate processing site agreements and reflect the time periods of resumption for essential Organization Name business functions.

## TELECOMMUNICATIONS

 in coordination with {IaaS/PaaS Provider}, has implemented alternate telecommunication services for the information system environment and maintains service agreements containing priority of service provisions and RTOs.

## BACKUPS

When conducts information system backups, the following types of information will be gathered and stored:

* User-level information is replicated to the alternate site on a daily basis
* System-level information is replicated in full and incremental backups to {Hosting Name/Region} and replicated to the alternate site in {Hosting Name/Region}
	+ {Backup/Recovery Solution} is continuously replicating the system backups and configuration
* Security related documentation is backed up to document repository

The following configuration requirements must be implemented on all current and future backup mechanisms:

* Configure each of the solution(s) to perform backups for user and system information, as well as documentation, as a daily incremental backup
* Configure each of the above solution(s) to perform backups for user and system information, as well as documentation as a weekly full backup
* Configure each of the backups to maintain at least three (3) copies with at least one (1) copy available online

{Hosting Name/Region}provides both physical and logical controls that protect the confidentiality and integrity of backups. All equipment, including disk-to-disk backups reside in physically controlled spaces that require approved personnel to access through multiple concentric perimeter security rings using multi-factor authentication.

Specific and relevant aspects of logical security around backups, to include backup confidentiality and integrity, are performed locally via the {Backup/Recovery Solution}, which allows for encryption algorithms to secure data in transit, as well as data hashing to helps ensure the integrity of data written inside dedicated space on the disk array.

 backup records for the daily incremental and weekly full processes are reviewed by the {Role/Team} on an Monthly basis to validate that backups are operating as intended. Issues or findings are to be remediated as soon as possible.

## Backup Testing

The {Role/Team}, in coordination with the {Role/Team}, test backup information on an annual basis to verify media reliability and information integrity using the following test method:

* All backups are tested as part of the Contingency Plan test and related training activities. will store backup copies of critical information system software and security related information is stored in a separate facility that is not co-located within the operational system.

## RECOVERY AND RECONSTITUTION

The complete details of the phases of the recovery and reconstitution of the information system can be found in the {SSP\_A\_ISCP\_VX.X\_YYYYMMDD}, Section 4.1 and Section 5. For transaction-based systems, database replication will restore transactional customer data.