Insert Logo Here

Organization Name

Security Policy

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 Policy | Noah Brown, CISO |

Table of Contents

[1 Introduction 1](#_Toc68592610)

[2 Purpose 1](#_Toc68592611)

[3 Scope 1](#_Toc68592612)

[4 Roles and Responsibilities 1](#_Toc68592613)

[5 Management Commitment 2](#_Toc68592614)

[6 Authority 3](#_Toc68592615)

[7 Compliance 3](#_Toc68592616)

[8 Policy Requirements 4](#_Toc68592617)

[8.1 Contingency Planning Policies and Procedures 4](#_Toc68592618)

[8.2 Contingency Plan 4](#_Toc68592619)

[8.3 Contingency Training 5](#_Toc68592620)

[8.4 Contingency Plan Testing 5](#_Toc68592621)

[8.5 Alternate Storage Environment 5](#_Toc68592622)

[8.6 Alternate Processing Environment 5](#_Toc68592623)

[8.7 Telecommunication Services 5](#_Toc68592624)

[8.8 Information System Backup 5](#_Toc68592625)

[8.9 Information System Recovery Reconstitution 6](#_Toc68592626)

# 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 Contingency Planning 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 contingency planning 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 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 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 Planning Policies and Procedures

This document is intended to serve as the *Contingency Planning Policy* and is made available to all applicable personnel. The associated procedure(s) to facilitate the implementation of the *Contingency Planning Policy* and related system maintenance controls have been developed, documented, and disseminated to all applicable personnel.

The Information Owner will review and update the *Contingency Planning 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 overall business goals and risk position. Any updates, improvements, or suggestions regarding the *Contingency Planning Policy* and/or procedure(s) must be sent to the Information Owner.

## Contingency Plan

Organization Name has developed a contingency plan in coordination with organizational elements responsible for related plans, that identifies essential missions, business functions, and associated contingency requirements. Capacity planning was conducted during the development of the contingency plan to ensure the necessary capacity for information processing, telecommunications, and environmental support exists during contingency operations.

The contingency plan is reviewed and approved by the Information Owner and provides the following information:

* Recovery objectives, restoration priorities, and metrics
* Contingency roles, responsibilities, and assigned individuals with up-to-date contact information
* The identification of critical information system assets supporting essential missions and business functions
* Actions necessary for maintaining essential missions and business functions despite an information system disruption, compromise, or failure
* Steps to complete the eventual full information system restoration without deterioration of the security safeguards originally planned and implemented
* A plan for resumption of essential missions and business functions within thirty (30) minutes of contingency plan activation

The contingency plan has been distributed to those with contingency planning roles and responsibilities as documented in the Information System Contingency Plan and is protected from unauthorized disclosure and modification. Ongoing contingency plan maintenance includes the following activities:

* Coordination of contingency planning activities with incident handling activities
* Review of the contingency plan for the information system at least annually
* Regular updates to the contingency plan to address changes to the organization, information system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing
* Communication of any contingency plan changes to the Contingency Plan Director

## Contingency Training

Organization Name will provide contingency training to personnel consistent with assigned roles and responsibilities within 10 days of assuming the role. Annual training will be provided thereafter or as required by information system changes.

## Contingency Plan Testing

All contingency plan testing must be developed in accordance with NIST Special Publication 800-34 (as amended) and all test plans must be approved and accepted by the agency Authorizing Official (AO) prior to initializing the testing.

The contingency plan will be tested at least annually using functional exercises to determine the effectiveness of the plan and the organizational readiness to execute the plan. All contingency plan testing must be coordinated with organizational elements responsible for related plans. will review the contingency plan test results and initiate corrective actions if needed.

## Alternate Storage Environment

In order to reduce susceptibility to threats, has identified and established an alternate storage environment that is separate from the primary storage environment.

The alternate environment provides information security safeguards equivalent to that of the primary environment and has obtained the necessary agreements to permit the storage and retrieval of information system backup information from the alternate environment. Any potential problems related to the accessibility of the alternate environment in the event on an area-wide disruption or disaster have been identified and explicit mitigation actions are outlined in the ISCP.

## Alternate Processing Environment

To reduce susceptibility to threats, alternate processing environment is Azure South Central. When primary processing capabilities are unavailable, the transfer and resumption of system operations for essential missions and business functions will occur within thirty (30) minutes.

## Telecommunication Services

OFFERING NAME resides in IaaS/PaaS PROVIDER NAME, an infrastructure-as-a-service/platform-as-a-service platform which inherently provides the necessary telecommunication services.

## Information System Backup

The following actions have been implemented for those areas of the information system cloud environment that have been determined to require backups:

* Daily incremental and weekly full backups of user-level, system-level, and system documentation information contained in the information system
	+ At least three (3) backup copies (at least one of which is available online) are maintained at all times
* Protection of the confidentiality, integrity, and availability of backup information at the storage locations
* Annual backup testing to verify media reliability and information integrity
* The storage of backup copies of critical information system software and other security-related information in a separate facility or in a fire-rated container that is not collocated with the operational system

## Information System Recovery Reconstitution

After a disruption, compromise, or failure, must provide for the recovery and reconstitution of the information system to a known state and implement transaction recovery for systems that are transaction-based.