

{Insert Company Name}

Security Policy

Contingency Planning (CP)

**Version:**

{N.N}

**Date:**

{Insert Modified Date}

# Document Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Version** | **Description** | **Author** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Any item that needs to be updated within this document can be found with { } around each item and in (RED) Font. [Delete this for final product submission]

# Table of Contents

1 Introduction ..............................................................................................................................................1

2 Purpose .....................................................................................................................................................1

3 Scope .........................................................................................................................................................2

4 Roles and Responsibilities .........................................................................................................................2

5 Management Commitment ......................................................................................................................2

6 Authority ...................................................................................................................................................3

7 Compliance ...............................................................................................................................................3

8 Policy Requirements .................................................................................................................................4

8.1 Contingency Planning Policies and Procedures [CP-1] ......................................................................4

8.2 Contingency Plan [CP-2, CP-2 (1,2,8), {CP-2 (2,5) High Only}] ...........................................................4

8.3 Contingency Training [CP-3, {CP-3 (1) High Only}] ............................................................................6

8.4 Contingency Plan Testing [CP-4, CP-4 (1), {CP-4 (2) High Only}] .......................................................6

8.5 Alternate Storage site [CP-6, CP-6 (1,3), {CP-6 (2) High Only}] .........................................................6

8.6 Alternate Processing site [CP-7, CP-7 (1,3), {CP-7 (4) High Only}] ....................................................6

8.7 Telecommunication Services [CP-8, CP-8 (1,2), {CP-8 (3,4) High Only}] ...........................................7

8.8 System Backup [CP-9, CP-9 (1,8), {CP-9 (2,3,5) High Only}] ..............................................................7

8.9 System Recovery and Reconstitution [CP-10, CP-10 (2), {CP-10 (4) High Only}] ..............................7

# Introduction

{Insert Company Name} has developed corporate policies that identify the security requirements for its information systems and personnel in order to ensure the integrity, confidentiality, and availability of its information. These policies are set forth by {Insert Company Name}’s management and in compliance with the Access Control family of controls found in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 5.

# Purpose

The purpose of these policies is to establish access control requirements to ensure the confidentiality, integrity, and availability of {Insert Company Name}’s 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 {Insert Company Name} employees, contractors, third parties, and others who have access to company and customer confidential information within {Insert Company Name} systems and facilities.

# Roles and Responsibilities

These policies apply to all {Insert Company Name} employees, contractors, business partners, third parties, and others who need or have access to {Insert Company Name}’s systems and our customer's confidential information. {Insert Company Personnel below and delete this for final product}

|  |  |  |
| --- | --- | --- |
| **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 {Insert Company Name} 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. |
| **Individual or Group** | **Role** | **Responsibility** |
|  | Authorizing Official Designated Representative | Acts on behalf of Authorizing Official to coordinate and conduct day-to-day activities associated with security authorization process. |
|  | Chief Information Security Officer | Responsible for conducting information system security engineering activities.  Responsible for providing for appropriate security, to include management, operational, and technical controls. |
|  | 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 Director | 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 Admin Team | System Administrator | Responsible for conducting information system security Administration activities. |
| Varies | Managers | Responsible for understanding, enforcing, and complying with control requirements defined in Policies and Procedures. |
| Varies | Users | Responsible for understanding and complying with Policies and Procedures. |

# Management Commitment

{Insert Company Name} 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 {Insert Company Name} Information System by implementing adequate security controls.

# Authority

These policies and procedures are issued under the authority of the {Insert Company Name} 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
2. Federal Information Security Modernization Act of 2014 (FISMA)
3. The Privacy Act of 1974
4. Clinger-Cohen Act of 1996
5. OMB Circulars and Memoranda
6. Federal Information Processing Standards (FIPS)
7. NIST Special Publications
8. OMB Memorandum for Chief Information Officers and Chief Acquisition Officers: Ensuring New Acquisitions Include Common Security Configurations, June 2007
9. 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 {Insert Company Name}’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 by an external vendor and/or internal self-assessments 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 personally identifiable information processing and transparency controls requirements, mechanisms, and provisions are to be followed by all employees, management, contractors, and other users who access and support information systems owned and operated by {Insert Company Name}, including its subsidiaries and affiliates, collectively referred to as {Insert Company/Product Name}.

The following access control requirements, mechanisms, and provisions are to be followed by all employees, management, contractors, and other users who access and support the {Insert Company/Product Name} information systems.

8.1 Contingency Planning Control Policies and Procedures [CP-1]

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 controls have been developed, documented, and disseminated to all applicable personnel.

{Insert Company Name} must develop, document, and disseminate to all personnel including the Chief Privacy Officer, Information System Security Officer (ISSO), and/or similar roles or their designees: [CP-1 (a)]

* An organizational-level Contingency Planning Policy that: [CP-1 (a) (1)]
  + Addresses the purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance [CP-1 (a) (1) (a)]
  + Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines [CP-1 (a) (1) (b)]
* Procedures to facilitate the implementation of Contingency Planning Policy and the associated Contingency Planning controls [CP-1 (a) (2)]

{Insert Company Name} must designate a Chief Information Security Officer (CISO) to manage the development, documentation, and dissemination of the Contingency Planning policy and procedures. [CP-1 (b)]

{Insert Company Name} must review and update the current Contingency Planning: [CP-1 (c)]

* Policies at least annually, following a significant change, and/or any compromising event [CP-1 (c) (1)]
* Procedures at least annually, following a significant change, and/or any compromising event [CP-1 (c) (2)]

8.2 Contingency Plan [CP-2, AC-2 (1,3,8), {CP-2 (2,5) High Only}]

{Insert Company Name} must develop a contingency plan for each information system environment in coordination with organizational elements responsible for related plans, that:

* Identifies essential missions, business functions, and associated contingency requirements. [CP-2 (a) (1)]
* Is reviewed and approved by the Contingency Plan Director, Information Owner, and Information Security Manger [CP-2 (a) (7)]
* Provides recovery objectives, restoration priorities, and metrics [CP-2 (a) (2)]
* Addresses contingency roles, responsibilities, and assigned individuals with up-to-date contact information [CP-2 (a) (3)]
* Identify critical information system assets supporting essential missions and business functions [CP-2 (8)]
* Addresses essential missions and business functions despite an information system disruption, compromise, or failure [CP-2 (a) (4)]
* Addresses the eventual full information system restoration without deterioration of the security safeguards originally planned and implemented [CP-2 (a) (5)]
* Addresses the sharing of contingency information [CP-2 (a) (6)]

The contingency plan must be distributed to those with contingency planning roles and responsibilities as documented in each contingency plan [CP-2 (b)] and must be protected from unauthorized disclosure and modification. [CP-2 (h)] Ongoing contingency plan maintenance includes the following activities:

* Coordination of contingency planning activities with incident handling activities [CP-2 (c)]
* Review of the contingency plan for the information system at least annually [CP-2 (d)]
* 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 [CP-2 (e)]
* Communication of any contingency plan changes to the Contingency Plan Director [CP-2 (f)]
* Incorporation of lessons learned from contingency plan testing, training, or actual contingency activities into contingency testing and training [CP-2 (g)]
* Coordinate with contingency related personnel internal to the organization who is responsible for the development of contingency plans [CP-2 (1)]
* Plan for the resumption of all mission essential and business functions within the designated Recovery Time Objective (RTO) of contingency plan activation [CP-2 (3)]

**For high impact systems only:**

* {Insert Company Name} must allocate the minimum number of personnel for information processing, telecommunications, and environmental support exists, during contingency operations [CP-2 (2)]
* {Insert Company Name} must plan for the continuance of all mission and business functions with minimal or no loss of operational continuity and sustains that continuity until full system restoration at primary processing and/or storage sites [CP-2 (5)]

8.3 Contingency Training [CP-3, {CP-3 (1) High Only}]

{Insert Company Name} shall provide contingency training to personnel consistent with assigned roles and responsibilities [CP-3 (a)] within 10 days of assuming the role. [CP-3 (a) (1)] Annual training will be provided thereafter or as required by information system changes. [CP-3 (a) (2, 3)] Contingency training will be reviewed and updated at least annually or after a significant information system change. [CP-3 (b)]

**For high impact systems only:**

{Insert Company Name} shall build simulated events into contingency training to facilitate a real response by personnel in a crisis. [CP-3 (1)]

8.4 Contingency Plan Testing [CP-4, CP-4 (1), {CP-4 (2) High Only}]

The contingency plan shall be tested at least annually using functional exercises to determine the effectiveness of the plan and the organizational readiness to execute the plan. [CP-4 (a)] All contingency plan tests must be coordinated with organizational elements responsible for related plans. [CP-4 (1)] {Insert Company Name} will review the contingency plan test results [CP-4 (b)] within the Contingency Plan-designated Appendix G, Contingency Plan Test Report and initiate corrective actions, if needed. [CP-4 (c)]

For systems storing or processing Federal or State government information, 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 test.

**For high impact systems only:**

{Insert Company Name} must coordinate with organizational elements to test the contingency plan at the alternate processing site [CP-4 (2)] at least once every three years to familiarize contingency personnel with the facility and available resources [CP-4 (2) (a)] and evaluate the capabilities of the alternate processing site to support contingency operations. [CP-4 (2) (b)]

8.5 Alternate Storage site [CP-6, CP-6 (1,3), {CP-6 (2) High Only}]

To reduce susceptibility to threats, {Insert Company Name} must:

* Identify and establish an alternate storage environment, including necessary agreements to permit the storage and retrieval of system backup information [CP-6 (a)]
* Ensure that the alternate storage site provides controls equivalent to that of the primary site [CP-6 (b)]
* Identify an alternate storage site that is sufficiently separated from the primary storage site to reduce susceptibility to the same threats [CP-6 (1)]
* Identify any potential problems related to the accessibility of the alternate environment in the event of an area-wide disruption or disaster and outlined explicit mitigation actions in the ISCP [CP-6 (3)]

**For high impact systems only:**

{Insert Company Name} must obtain the necessary agreements to permit the storage and retrieval of information system backup information from the alternate environment in accordance with recovery time and recovery point objectives. [CP-6 (2)]

8.6 Alternate Processing site [CP-7, CP-7 (1,3), {CP-7 (4) High Only}]

{Insert Company Name} must establish an alternate processing site including necessary agreements to permit the transfer and resumption of the information system for essential missions/business functions within the Recovery Time Objective from disaster declaration when the primary processing capabilities are unavailable. [CP-7 (a)]

{Insert Company Name} must ensure that equipment and supplies required to transfer and resume operations are available at the alternate processing site or contracts are in place to support delivery to the site within the defined period for transfer/resumption. [CP-7 (b)]

{Insert Company Name} must ensure that the alternate processing site provides security controls equivalent to that of the primary [CP-7 (c)] site and is sufficiently separated from the primary processing site to reduce susceptibility to the same threats. [CP-7 (1)] {Insert Company Name} must identify potential accessibility problems to alternate processing sites in the event of an area-wide disruption or disaster and outline explicit mitigation actions. [CP-7 (2)]

{Insert Company Name} must develop alternate processing site agreements that establishes priority-of-service provisions in accordance with essential missions/business functions within the Recovery Time Objective from primary processing site unavailability. [CP-7 (3)]

**For high impact systems only:**

{Insert Company Name} must prepare the alternate processing site so that the site can serve as the operational site supporting essential mission and business functions when a disaster is declared. [CP-7 (4)]

8.7 Telecommunication Services [CP-8, CP-8 (1,2), {CP-8 (3,4) High Only}]

{Insert Company Name} must establish alternate telecommunications services including necessary agreements to permit the resumption of the information system for essential missions and business functions within the Recovery Time Objective from disaster declaration when the primary telecommunications capabilities are unavailable at either the primary or alternate processing or storage sites. [CP-8]

* {Insert Company Name} must develop primary and alternate telecommunications service agreements that contain priority-of-service provisions in accordance with availability requirements within the Recovery Time Objective [CP-8 (1) (a)]
* {Insert Company Name} will request Telecommunications Service Priority for all telecommunications services used for national security emergency preparedness if the primary and/or alternate telecommunications services are provided by a common carrier [CP-8 (1) (b)]
* {Insert Company Name} should obtain alternate telecommunications services to reduce the likelihood of sharing a single point of failure with primary telecommunications services [CP-8 (2)]

For high impact systems only:

* {Insert Company Name} must obtain alternate telecommunications services from providers that are separated from primary service providers to reduce susceptibility to the same threats [CP-8 (3)]
* {Insert Company Name} requires primary and alternate telecommunications service providers to have contingency plans [CP-8 (4) (a)]
* {Insert Company Name} will review provider contingency plans to ensure that the plans meet organizational contingency requirements [CP-8 (4) (b)]
* {Insert Company Name} will obtain evidence of contingency testing and training by providers at least annually [CP-8 (4) (c)]

8.8 System Backup [CP-9, CP-9 (1,8), {CP-9 (2,3,5) High Only}]

{Insert Company Name} must determine what elements of the information system environment require the system backup controls. {Insert Company Name} must determine how the information system backup will be verified and appropriate frequency of the check.

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

* Daily incremental and weekly full backups of user-level [CP-9 (a)], system-level [CP-9 (b)], and system documentation information contained in the information system, including security- and privacy-related documentation [CP-9 (c)]
  + At least three (3) backup copies (at least one of which is available online) are maintained at all times
  + Backups are transferred to the alternate storage site weekly
* Protection of the confidentiality, integrity, and availability of backup information at the storage locations [CP-9 (d)]
* Annual backup testing to verify media reliability and information integrity [CP-9 (1)]
  + For high impact systems, this backup testing is to be performed at least monthly
* Cryptographic mechanisms are implemented to prevent unauthorized disclosure and modification of all user-level, system-level, and system documentation [CP-9 (8)]

**For high impact systems only:**

* {Insert Company Name} must store 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 [CP-9 (3)]
* {Insert Company Name} must use a sample of backup information in the restoration of selected system functions as part of contingency plan test at least annually [CP-9 (2)]
* {Insert Company Name} must transfer system backup information to the alternate storage site consistent with recovery time and recovery point objectives for the information system [CP-9 (5)]

8.9 System Recovery and Reconstitution [CP-10, CP-10 (2), {CP-10 (4) High Only}]

After a disruption, compromise, or failure, {Insert Company Name} must arrange for the recovery and reconstitution of the Information System to a known state within the information system’s recovery time and recovery point objectives [CP-10] and implement transaction recovery for systems that are transaction-based. [CP-10 (2)]

**For high impact systems only:**

{Insert Company Name} provides the capability to restore systems components within the Recovery Time Objective from configuration-controlled and integrity-protected information representing a known, operational state for the components. [CP-10 (4)]