

{Insert CompanY Name}

Security Procedures

Contingency Planning Procedures [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 Procedures Requirements [CP-1] ............................................................................................................. 6

8.1 Contingency Plan [CP-2] ................................................................................................................... 6

8.1.1 Disaster Recovery Team Lead .................................................................................................... 7

8.1.2 War Room Establishment and Activities ................................................................................... 7

8.1.3 Customer Communication ......................................................................................................... 8

8.2 Review and Distribution [CP-2, CP-2 (1)] .......................................................................................... 8

8.3 Incident Response and Capacity Planning [CP-2] ............................................................................. 9

8.4 Resuming Essential Missions and Business Functions [CP-2, CP-2 (3)] ............................................ 9

8.5 Identifying Critical Assets [CP-2 (8)] ................................................................................................. 9

8.6 Training and Testing [CP-2, CP-3, CP-4 ............................................................................................. 9

8.7 Alternate Storage and Processing Sites and Telecommunications Services [CP-6, CP-7, CP-8, CP-9 (3)] ........................................................................................................................................................ 10

8.7.1 Site Location ............................................................................................................................ 10

8.7.2 Site Safeguards and Geographic Separation [CP-6, CP-6 (1), CP-7, CP-7(1)] ........................... 10

8.7.3 Accessibility Problems [CP-6 (3), CP-7 (2)] ............................................................................... 10

8.7.4 Remediation Actions to the Accessibility Problems ................................................................ 11

8.7.5 Agreements [CP-7, CP-7 (3)] .................................................................................................... 11

8.7.6 Telecommunications [CP-8, CP-8 (1,2)] ................................................................................... 11

8.8 Backups [CP-9, CP-9 (3)] ................................................................................................................. 11

8.9 Backup Testing [CP-9 (1)] ............................................................................................................... 12

8.10 Recovery and Reconstitution [CP-10, CP-10 (2)] .......................................................................... 12

9 Addendum A: Information System Contingency Plan Location ............................................................. 13

# 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.

# Procedural Requirements [CP-1]

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 {Insert Company Name} information systems.

8.1 Contingency Plan [CP-2]

In the event of a disaster or emergency, the {Insert Product Name} Information System Contingency Plan (ISCP), dated {mm/dd/yyyy}, will be used to maintain the essential missions and business functions of the {Insert Product Name} Information System, maintain security measures, and facilitate communication with internal stakeholders and external users. The contingency plan was developed in conjunction with team members responsible for related plans, [CP-2 (a) (1)] and reviewed and approved by the Contingency Plan Coordinator, Information Owner, and Information Security Owner. [CP-2 (a) (7)] The sharing of contingency information is addressed in the ISCP. [CP-2 (a) (6)] The location of the ISCP can be found in Addendum A of this document.

To facilitate swift recovery, all the networks, subnets, VNets, load balancers, and Network Security Groups (NSGs) have been defined in the recovery location. Additionally, an {Insert Documentation Repository Name} and {Insert Device Name} node are pre-staged in the recovery environment and actively participating in replication with the primary site.

* The {Insert Vendor(s) Name or Location} (secondary site) contains the base infrastructure for a recovery of the {Insert Product Name} Information System from the primary {Insert Vendor(s) Name} to the secondary {Insert Vendor(s) Name}. Similar to the {Insert Vendor(s) Name} (primary site), the {Insert Vendor(s) Name} Production VNet consists of {Insert number of} subnets: {Insert names of each subnet e.g., Application Gateway Subnet, WWW Subnet, Services Subnet, etc.}.
* The {List each subnet along with functionality of subnet}.
* The {List each subnet along with functionality of subnet equal to number of subnets controlled}.
* The {Continue until complete}.

8.1.1 Disaster Recovery Team Lead

If the contingency plan is activated, the following individuals are responsible for managing the execution of the recovery process: [CP-2 (a) (3)]

|  |  |  |  |
| --- | --- | --- | --- |
| **Title** | **Name** | **Responsibilities** | **Contact (Email/Cell/Home)** |
| Disaster Recovery Team Lead |  | Notify organizational officials of a disaster and rally team members. | {EMAIL @ Company.com}  {XXX-XXX-1234} |
| Assistant Disaster Recovery Lead |  | Coordinate contingency response activities | {EMAIL @ Company.com}  {XXX-XXX-1234} |

8.1.2 Access Enforcement [AC-3]

To facilitate communications and distillation of information, a “war room” will be established upon plan activation. The war room may be a physical conference room, a virtual room in {Insert Vendor(s) Name}, or both. Details regarding the war room will be sent by email, text message, and/or instant message from the Disaster Recovery Team Lead or Assistant Disaster Recovery Lead to the team members, as required.

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 controls. For complete details, see the {Insert Product Name} Incident Response Plan [CP-2 (a) (5)]

8.1.3 Customer Communication

Communication with customers will be conducted via email by the appropriate Program Manager. 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, if known:
  + Reason for disruption
  + Impact result of the failover
  + Expected timeline for the restoration of the system
  + A high-level testing summary
  + Plans for expected follow-up communications before the restoration is complete
* Incremental communications will include, if known:
  + Any updates to the timeline for the restoration of the system
  + Any new information that was not known during the initial communication
  + Plans for expected follow-up communications before 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

8.2 Review and Distribution [CP-2, CP-2 (1)]

It is the responsibility of Contingency Plan Coordinator to distribute the contingency plan to the following individuals, including any changes to the plan: [CP-2 (b)]

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

It is the responsibility of the Information Security Team in coordination with the Contingency Plan Coordinator to review [CP-2 (1)] and update the contingency plan: [CP-2 (d)] [CP-2 (e)]

* On an annual basis
* Whenever there are changes to the information system infrastructure or environment
* If problems identified during the implementation, execution, or testing phases.

{Insert Company Name} uses {Insert Vendor(s) Name} to protect the contingency plan from unauthorized disclosure and modification. Individuals with contingency plan responsibilities are notified by {Insert Vendor(s) Name} upon any changes to the contingency plan. [CP-2 (f)]

8.3 Incident Response and Capacity Planning [CP-2]

Contingency personnel will meet with incident response personnel, including other organizational elements responsible for related plans at least once a year to coordinate activities. [CP-2 (c)]

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

The {Insert Product Name} Information System Contingency Plan (ISCP) will outline the actions necessary for maintaining essential missions and business functions in the event of a disruption, compromise, or failure. [CP-2 (a) (4)] The location of the ISCP can be found in Addendum A of this document.

8.4 Resuming Essential missions and Business Functions [CP-2, CP-2 (3)]

The Recovery Time Objective (RTO) is the maximum period between {Insert Company Name}’s decision to activate the recovery processes and the point at which a customer can resume operations in the secondary environment. {Insert Company Name} plans for the resumption of essential {Insert Product Name} Information System missions and business functions within {Insert organization RTO timeframe} of contingency plan activation. [CP-2 (a) (2)] [CP-2 (3)]

8.5 Identifying Critical Assets [CP-2 (8)]

Critical {Insert Product Name} assets supporting essential missions and business functions are documented in the {Insert Product Name} Information System Contingency Plan, Addendum H, Hardware and Software Inventory. [CP-2 (8)]

8.6 Training and Testing [CP-2, CP-3, CP-4]

{Insert Company Name} will use {Insert Vendor(s) Name} to train contingency personnel in their roles and responsibilities: [CP-3 (a)]

* within ten (10) business days of assuming a contingency role; [CP-3 (a) (1)]
* on an annual basis thereafter; or [CP-3 (a) (3)]
* as required by information system changes. [CP-3 (a) (2)]

Contingency training is reviewed and updated at least annually or after a significant change to the {Insert Product Name} Information System. [CP-3 (b)] Team members must review the current contingency plan and the previous year’s contingency plan test results. Once a contingency plan team member completes the training modules, the {Insert Vendor(s) Name} automatically records the training completion.

Privileged admins and engineers must take the basic contingency training within 10 days. Consideration must be given for those privileged admins and engineers with critical contingency-related roles, to gain enough system context and situational awareness to understand the full impact of contingency training as it applies to their respective level. Newly hired critical contingency personnel must take this more in-depth training within 60 days of hire-date when the training will have more impact. [CP-3 (a)]

{Insert Company Name} tests the contingency plan annually by conducting either a live exercise or a table-top test. [CP-4 (a)] Special consideration will be taken to ensure testing is coordinated with elements responsible for related plans. [CP-4 (1)] During the annual test, the following actions will be taken:

* Coordination of the testing and exercises with other {Insert Company Name} 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, which are reviewed by the Contingency Team Members [CP-4 (b)]
  + Lessons learned
* Corrective actions to be taken as a result of the test [CP-4 (c)]
* Upload the results of the testing exercises to the Information Security team’s {Insert Name of} document repository
* Incorporate lessons learned from contingency plan testing, training, or actual contingency activities into contingency testing and training [CP-2 (g)]

8.7 Alternate Storage and Processing Sites and Telecommunication Services [CP-6, CP-7, CP-8, CP-9 (3)]

8.7.1 Site Locations

The {Insert Company Name} Contingency Planning Team has established and documented the alternate storage and processing sites for the {Insert Product Name} Information System. [CP-6 (a)]

* Primary storage and processing site: {Insert Primary Name and Region Location}
* Alternate storage and processing site: {Insert Alternate Name and Region Location}

8.7.2 Site Safeguards and Geographic Separation [CP-6, CP-6 (1), CP-7, CP-7 (1)]

The alternate site will provide information security safeguards and controls equivalent to those of the primary site. [CP-6 (b)] [CP-7 (c)] Since the {Insert Vendor(s) Name} primary and alternate storage and processing sites are separated by over {Distance over 100} miles, they are not susceptible to the same environmental threats. [CP-6 (1)] [CP-7 (1)]

8.7.3 Accessibility Problems [CP-6 (3), CP-7 (2)]

{Insert Company Name} has identified the following potential accessibility problem to the alternate storage and processing sites: [CP-6 (3)] [CP-7 (2)]

* {Insert Vendor(s) Name} does not permit clients to visit any of the {Insert Vendor(s) Name} data centers, including both the primary and secondary sites.
* The alternate storage facility is co-located at the alternate processing facility and delivery of backups is electronic. For complete details, see the {Insert Product Name} Information System Contingency Plan (ISCP) {Insert inherited control language if applicable}. Location of the ISCP can be found in Addendum A of this document.

8.7.4 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.

8.7.5 Agreements [CP-7, CP-7 (3)]

The {Insert Company Name} Contingency Planning Team ensures that alternate storage and processing site agreements are in place, are current, and accurately reflect the {Insert Product Name} Information System environment and contingency plan requirements for resumption of essential functions within the Recovery Time Objective (RTO). [CP-7 (a)] This includes having either priority-of-service provisions or staging stand-by equipment resumption for essential {Insert Company Name} {Insert Product Name} business functions. [CP-7 (3)] Additionally, the alternate site provides information security safeguards equivalent to those of the primary site.

{Insert Company Name} ensures that necessary equipment and supplies are available at the alternate site or ready to be in place within the defined time period. [CP-7 (b)] This includes staging an {Insert Vendor(s) Name} and a {Insert Type of Server Name} with full replication with production at the recovery site to facilitate rapid recovery. {Insert Company Name} has also pre-built the necessary networking VNets and Subnets at the recovery site. [CP-7 (c)]

8.7.6 Telecommunications [CP-8, CP-8 (1,2)

{Insert Company Name} in coordination with {Insert Vendor(s) Name}, has implemented alternate telecommunication services for the {Insert Product Name} environment and maintains service agreements containing priority of service provisions and RTOs. [CP-8] [CP-8 (1) (a)] [CP-8 (1) (b)] [CP-8 (2)]

8.8 Backups [CP-9, CP-9 (3)]

{Insert Company Name} system backups gather and store the following types of information:

* User-level information is replicated daily to the alternate site [CP-9 (a)]
* System-level information is replicated in full and incremental backups to {Insert Vendor(s) Data-Center Regional Location} and replicated to the alternate site in {Insert Vendor(s) Data-Center Regional Location} [CP-9 (b)]
  + {Insert Vendor(s) Name} is {Insert organization control language if applicable} continuously replicating the system backups and configuration
* Security related documentation is backed up to {Insert Company Name}’s document repository [CP-9 (c)]

The following configuration requirements are implemented on all current and must be implemented on all future {Insert Company Name} backup mechanisms:

* Configure each of the above solution(s) to perform backups {Insert organization Control Language and how often for a} full backup
* Configure each of the above solution(s) to perform backups {Insert organization Control Language and how often for a} incremental backup
* Configure each of the backups to maintain at least three (3) copies with at least one (1) copy available online
  + At least one backup copy of critical information system software and security related information is stored in a separate facility that is not co-located within the operational system.

{Insert Vendor(s) Name along with control language if applicable} provides {Insert Organizational Control Language if applicable} controls that protect the confidentiality integrity, and availability of backups. [CP-9 (d)] 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 {Insert Vendor(s) Name}, which are configured for FIPS 140-2 certified encryption algorithms to secure data in transit, as well as data hashing to helps ensure the integrity of data written inside dedicated LUN's on the disk array. [CP-9 (8)]

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

8.9 Backup Testing [CP-9 (1)]

The IT Team, in coordination with the Information Security Team, test backup information on at least an annual basis to verify media reliability and information integrity. All backups are tested as part of the Contingency Plan test and related training activities. [CP-9 (1)]

8.10 Recovery and Reconstitution [CP-10, CP-10 (2)]

The complete details of the phases of the recovery and reconstitution of the information system can be found in the {Insert Product Name} Information System Contingency Plan (ISCP). [CP-10] The location of the ISCP can be found in Addendum A of this document. For transaction-based systems, database replication will restore transactional customer data. [CP-10 (2)]

Addendum A: Information System Contingency Plan Location

The most recent version of the {Insert Product Name} Information System Contingency Plan is located in the {Insert Company Name} {Document Repository Name}:

{Fill in location or URL}