Insert Logo Here

Organization Name

Security Policy

Incident Response

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 IR Policy | Noah Brown, CISO |

Table of Contents

[1 Introduction 1](#_Toc68593073)

[2 Purpose 1](#_Toc68593074)

[3 Scope 1](#_Toc68593075)

[4 Roles and Responsibilities 1](#_Toc68593076)

[5 Management Commitment 2](#_Toc68593077)

[6 Authority 3](#_Toc68593078)

[7 Compliance 3](#_Toc68593079)

[8 Policy Requirements 4](#_Toc68593080)

[8.1 Incident Response Policies and Procedures 4](#_Toc68593081)

[8.2 Incident Response Training 4](#_Toc68593082)

[8.3 Incident Response Testing 4](#_Toc68593083)

[8.4 Incident Handling 4](#_Toc68593084)

[8.5 Incident Monitoring 4](#_Toc68593085)

[8.6 Incident Reporting 5](#_Toc68593086)

[8.7 Incident Response Assistance 5](#_Toc68593087)

[8.8 Incident Response Plan 5](#_Toc68593088)

[8.9 Information Spillage Response 5](#_Toc68593089)

# Introduction

Organization Name 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 Organization Name management and in compliance with the Incident Response 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 Incident Response requirements to ensure the confidentiality, integrity, and availability of Organization Name 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 Organization Name employees, contractors, third parties, and others who have access to company and customer confidential information within Organization Name systems and facilities.

# Roles and Responsibilities

These policies apply to all Organization Name employees, contractors, business partners, third parties, and others who need or have access to Organization Name 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 Organization 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. |
|  | 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

Organization 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 Organization Name system by implementing adequate security controls.

# Authority

These policies and procedures are issued under the authority of the Organization 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/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 Organization Name 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 incident response 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.

## Incident Response Policies and Procedures

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

The Information Owner will review and update the *Incident Response 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 *Incident Response Policy* and/or procedure(s) must be sent to the Information Owner.

## Incident Response Training

Organization Name must provide incident response training to users with incident response related roles and responsibilities within six (6) weeks of assuming the position and at least annually thereafter or when required by information system changes.

## Incident Response Testing

Organization Name will test the incident response capability of the information system at least annually using NIST Special Publication 800-61 (as amended) to determine the incident response effectiveness and document the results.

A copy of the incident response test plan will be provided to the Authorizing Official (AO) on an annual basis prior to conducting an incident response test. The incident response test will be coordinated with organizational elements responsible for related plans.

## Incident Handling

Organization Name has implemented incident handling plans that includes preparation, detection and analysis, containment, eradication, and recovery. In addition to automated mechanisms used to support the incident handling process, the following actions must be completed:

* Coordinate incident handling activities with contingency planning activities
* Incorporate lessons learned from ongoing incident handling activities into incident response procedures, training, testing, and exercises, and implements the resulting changes accordingly
* Ensure that individuals conducting incident handling meet personnel security requirements commensurate with the criticality and/or sensitivity of the information being processed, stored, and transmitted by the information system

## Incident Monitoring

Organization Name must track and document information security incidents.

## Incident Reporting

Organization Name requires personnel to report suspected security incidents and/or breaches to the organizational incident response capability within US-CERT incident reporting timelines as specified in NIST SP 800-61 (as amended). Automated mechanisms will be used to assist in the reporting of security incidents and a copy of the security incident report must be sent to the Authorizing Official (AO) in accordance with the FedRAMP Incident Communications Procedure.

## Incident Response Assistance

Organization Name must provide an incident response support resource that offers advice and assistance to users of information for the handling and reporting of security incidents. Additionally, automated mechanisms are to be employed to increase the availability of incident response related information and support.

A direct, cooperative relationship between Knowledge Services’ incident response capability and external providers of information protection capability must be established and maintained. Members of Knowledge Services’ Incident Response Team will be identified to the external providers.

## Incident Response Plan

Organization Name has developed an incident response plan to be used during a security incident event. Copies of the incident response plan have been distributed and are always available to [Roles] The incident response plan provides the following information:

* A roadmap for implementing and metrics for measuring Organization Name incident response capability, and a high-level description of how the incident response capabilities fit into Organization Name overall organizational structure related to mission, size, structure, and functions
* Definitions of reportable incidents
* A list of resources and management support needed to effectively maintain and mature an incident response capability

The incident response plan is protected from unauthorized disclosure and modification and must be reviewed and approved annually by the [Roles]. Updates will be made to the plan to reflect system and/or organizational changes or problems encountered during plan implementation, execution, and/or testing. Any changes made to the incident response plan must be communicated to the required personnel.

## Information Spillage Response

Information spillage occurs when classified or sensitive data is accidentally uploaded or saved to the information system. At a minimum, Organization Name must:

* Respond to information spills by identifying the specific information involved and isolating and eradicating the contaminated information system or component and performing other specific actions
* Alert the Organization Name Information Security Manager and State agency customer of the information spill using a method of communication not associated with the spill
* Assign personnel or roles with responsibility for responding to information spills
* Provide information spillage response training at least annually
* Implement procedures to ensure that personnel impacted by information spills can continue to carry out assigned tasks while contaminated systems are undergoing corrective actions
* Employ specific safeguards for personnel exposed to information not within assigned access authorizations