

GovRAMP

{Insert Company Name}

Security Policy

Incident Response

**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

[Document Revision History 1](#_Toc196400127)

[Table of Contents 2](#_Toc196400128)

[1 Introduction 3](#_Toc196400129)

[2 Purpose 3](#_Toc196400130)

[3 Scope 3](#_Toc196400131)

[4 Roles and Responsibilities 3](#_Toc196400132)

[5 Management Commitment 4](#_Toc196400133)

[6 Authority 5](#_Toc196400134)

[7 Compliance 5](#_Toc196400135)

[8 Policy Requirements 5](#_Toc196400136)

[8.1 Incident Response Policies and Procedures [IR-1] 5](#_Toc196400138)

[8.2 Incident Response Training [IR-2, {IR-2 (1,2) High Only}] 6](#_Toc196400139)

[8.3 Incident Response Testing [IR-3, IR-3 (2)] 6](#_Toc196400140)

[8.4 Incident Handling [IR-4, IR-4 (1), {IR-4 (2,4,6,11) High Only}] 6](#_Toc196400141)

[8.5 Incident Monitoring [IR-5, {IR-5 (1) High Only}] 7](#_Toc196400142)

[8.6 Incident Reporting [IR-6, IR-6 (1,3)] 7](#_Toc196400143)

[8.7 Incident Response Assistance [IR-7, IR-7 (1)] 8](#_Toc196400144)

[8.8 Incident Response Plan [IR-8] 8](#_Toc196400145)

[8.9 Information Spillage Response [IR-9, IR-9 (2,3,4)] 9](#_Toc196400146)

# 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 Incident Response 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 Incident Response 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. |
|  | 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 Incident Response 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}.

8.1 Incident Response Policies and Procedures [IR-1]

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.

{Insert Company Name} must develop, document, and disseminate to all personnel including the chief privacy officer, ISSO, and/or similar roles or their designees: [IR-1 (a)]

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

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

{Insert Company Name} must review and update the current Incident Response: [IR-1 (c)]

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

8.2 Incident Response Training [IR-2, {IR-2 (1,2) High Only}]

{Insert Company Name} must provide incident response (IR) training: [IR-2 (a) (1)]

* To privileged users with incident response related roles and responsibilities within ten (10) business days of assuming the position
* To users with incident response related roles and responsibilities within thirty (30) business days of assuming the position

Additionally, {Insert Company Name} must provide incident response training at least annually thereafter [IR-2 (a) (3)] or when required by information system changes. [IR-2 (a) (2)] {Insert Company Name} must review and update incident response training content at least annually or in response to the following types of events: [IR-2 (b)]

* Incident response plan testing
* Response to an actual incident
* Assessment or audit findings

**For high impact systems only:**

{Insert Company Name} shall incorporate simulated events into incident response training to personnel who respond in crisis situations. [IR-2 (1)] Incident response training environment may include Computer Based Training, Tabletop Exercises, or instructor led training to develop personnel expertise. [IR-2 (2)]

8.3 Incident Response Testing [IR-3, IR-3 (2)]

{Insert Company Name} must test the incident response capability using NIST Special Publication 800-61 (as amended) to determine the incident response effectiveness and document the results. Incident response testing frequency depends on the impact level of the information system. For high impact systems, incident response testing shall be performed at least every six (6) months with functional testing being performed at least annually. For moderate impact systems, a functional incident response test shall be performed at least annually. [IR-3]

A copy of the incident response test plan will be provided to the Authorizing Official (AO) on an annual basis prior to functional testing. The incident response test must be coordinated with organizational elements responsible for related plans. [IR-3 (2)]

8.4 Incident Handling [IR-4, IR-4 (1), {IR-4 (2,4,6,11) High Only}]

{Insert Company Name} must implement incident handling plans that includes preparation, detection and analysis, containment, eradication, and recovery. [IR-4 (a)] 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 [IR-4 (b)]
* Incorporate lessons learned from ongoing incident handling activities into incident response procedures, training, testing, and exercises, and implements the resulting changes accordingly [IR-4 (c)]
* Ensure the rigor, intensity, scope, and results of incident handling activities are comparable and predictable across the organization [IR-4 (d)]
* {Insert Company Name} supports the incident handling process using automated notifications to provide alert to potential incidents. [IR-4 (1)]
* 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

**For high impact systems only:**

* Where supported, {Insert Company Name} should permit on all network, data storage, and computing devices the dynamic reconfiguration of components to stop attacks, misdirect attackers, and isolate components of systems, to limit the extent of the damage from breaches or compromises [IR-4 (2)]
* {Insert Company Name} should correlate incident information and individual incident responses to achieve an organization-wide perspective on incident awareness and response [IR-4 (4)]
* {Insert Company Name} shall implement an incident handling capability for incidents involving insider threats [IR-4 (6)]
* {Insert Company Name} shall establish and maintain an integrated incident response team that can be deployed (physically or virtually) to any location identified by the organization within 24 hours notice [IR-4 (11)]

8.5 Incident Monitoring [IR-5, {IR-5 (1) High Only}]

{Insert Company Name} must track and document information security incidents. [IR-5] Documenting incidents includes maintaining records about each incident, the status of the incident, and other pertinent information necessary for forensics as well as evaluating incident details, trends, and handling. Incident information can be obtained from a variety of sources, including network monitoring, incident reports, incident response teams, user complaints, supply chain partners, audit monitoring, physical access monitoring, and user and administrator reports.

**For high impact systems only:**

{Insert Company Name} should use automated mechanisms such as SIEM tools to track, collect, and analyze information security events. [IR-5 (1)]

8.6 Incident Reporting [IR-6, IR-6 (1,3)]

{Insert Company Name} requires personnel to report suspected security incidents and/or breaches to the organizational incident response capability. Automated mechanisms must be used to assist in the reporting of security incidents. [IR-6 (b)]

{Insert Company Name} shall provide incident information to the provider of the product or service and other organizations involved in the supply chain or system components related to the incident. [IR-6 (3)]

For systems processing or storing Federal information, reporting must be made within the US-CERT incident reporting timelines as specified in NIST SP 800-61 (as amended) and in accordance with the StateRAMP Incident Communications Procedure. [IR-6 (a)] Additionally, a copy of the security incident report must be sent to the Authorizing Official (AO) in accordance with the StateRAMP Incident Communications Procedure. [IR-6 (1)]

8.7 Incident Response Assistance [IR-7, IR-7 (1)]

{Insert Company Name} must provide an incident response support resource that offers advice and assistance to users of the information system for the handling and reporting of security incidents. [IR-7] Additionally, automated mechanisms are to be employed to increase the availability of incident response related information and support. [IR-7 (1)]

8.8 Incident Response Plan [IR-8]

{Insert Company Name} must develop an incident response plan to be used during a security incident event. Copies of the incident response plan must be distributed and are always available to the {Insert Company Name} Chief Information Officer, {Insert Company Name} Chief Information Security Officer, Incident Response Team, and customer Authorizing Officer (AO). [IR-8 (b)] The incident response plan must:

* Provide the organization with a roadmap for implementing its incident response capability [IR-8 (a) (1)]
* Describe the structure and organization of the incident response capability [IR-8 (a) (2)]
* Provide a high-level approach for how the incident response capability fits into the overall organization [IR-8 (a) (3)]
* Meet the unique requirements of the organization, which relate to mission, size, structure, and functions [IR-8 (a) (4)]
* Define reportable incidents [IR-8 (a) (5)]
* Provide metrics for measuring the incident response capability within the organization [IR-8 (a) (6)]
* Define the resources and management support needed to effectively maintain and mature an incident response capability [IR-8 (a) (7)]
* Address the sharing of incident information [IR-8 (a) (8)]
* Designate responsibility for incident response to the {Insert Company Name} Information Security Management team [IR-8 (a) (10)]

The incident response plan must be protected from unauthorized disclosure and modification [IR-8 (e)] and must be reviewed and approved at least annually by the {Insert Company Name} Chief Information Security Officer, Information Security Manager (ISM), and customer Authorizing Officer (AO). [IR-8 (a) (9)] Updates will be made to the plan to reflect system and/or organizational changes or problems encountered during plan implementation, execution, and/or testing. [IR-8 (c)] Any changes made to the incident response plan must be communicated to the Incident Response Team. [IR-8 (d)]

8.9 Information Spillage Response [IR-9, IR-9 (2,3,4)]

Information spillage refers to instances where information is placed on systems that are not authorized to process such information. At a minimum, {Insert Company Name} must respond to information spills by:

* Assigning {Insert Company Name} Technology Team, Legal Team, and Human Resources (as appropriate) with the responsibility for responding to information spills [IR-9 (a)]
* Identifying the specific information involved in the information system contamination [IR-9 (b)]
* Alerting the {Insert Company Name} IR Team of the information spill using a method of communication not associated with the spill [IR-9 (c)]
* Isolating the contaminated information system or system component [IR-9 (d)]
* Eradicating the information from the contaminated information system or component [IR-9 (e)]
* Identifying other information systems or system components that may have been subsequently contaminated [IR-9 (f)]
* Performing any additional actions, as needed, documented in NIST Special Publication 800-61 (as amended) [IR-9 (g)]

{Insert Company Name} must perform the following actions regarding personnel involved in information spillage:

* Provide information spillage response training at least annually [IR-9 (2)]
* Implement enhanced monitoring to ensure that personnel impacted by information spills can continue to conduct assigned tasks while contaminated systems are undergoing corrective actions [IR-9 (3)]
* Employ reminders of non-disclosure agreements and obligations for personnel exposed to information not within assigned access authorizations of the laws, executive orders, directives, regulations, policies, standards, and guidelines governing the information [IR-9 (4)]