

{Insert CompanY Name}

Security Procedures

Incident Response [IR]

**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 Procedural Requirements [IR-1] ............................................................................................................... 4

8.1 Incident Response Training and Testing [IR-2, IR-3, IR-3 (2)] ........................................................... 4

8.2 Incident Handling [IR-4] ................................................................................................................... 4

8.3 Incident Monitoring [IR-5] ............................................................................................................... 6

8.4 Reporting Security Incidents [IR-6, IR-6 (1), IR-6 (3)] ....................................................................... 6

8.5 Incident Response Assistance [IR-7, IR-7 (1)] ................................................................................... 6

8.6 Incident Response Plan [IR-8] .......................................................................................................... 6

8.7 Information Spillage Response [IR-9] ............................................................................................... 7

8.7.1 Information Spillage [IR-9 (1), IR-9 (2), IR-9 (3)] ............................................................................ 7

8.7.2 Information Spillage Response Overview [IR-9, IR-9 (4)] .............................................................. 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}’ 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}’ 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}’ 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}’ 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 [IR-1]

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 {Insert Company Name} information systems.

8.1 Incident Response Training and Testing [IR-2, IR-3, IR-3 (2)]

It is the responsibility of the Incident Response Team (IRT) Program Manager (PM) to provide incident response training to personnel:

* Within ten (10) business days of acquiring system access for privileged users [IR-2 (a) (1)]
* Within thirty (30) business days for individuals assuming a Incident Response role [IR-2 (a) (1)]
* When required by system changes, [IR-2 (a) (2)]
* At least annually thereafter [IR-2 (a) (3)]

Incident Response Plan (IRP) training will be performed by each individual IRT member through the {Insert Organization Training Repository}, {Insert Product Name}. The {Insert Organization Training Repository} will require individual acknowledgement that the Incident Response Plan (IRP) was reviewed.

{Insert Company Name} reviews and updates 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

{Insert Company Name} assigns the IRT Program Manager to oversee the annual incident response testing for the {Insert Product Name} Information System. The annual incident response tests are conducted by {Insert Company Name}’ IRT and tested in accordance with NIST 800-61 (as amended). [IR-3] When scheduling an annual incident response test, the IRT Program Manager coordinates a tabletop exercise. The IRT conducts the annual incident response test by:

* Simulating the defined scenario
* Following the prescribed actions within the IRP

Once the annual incident response test is completed, the members of the IRT document lessons learned that can be incorporated to improve the IRP. All artifacts and documents pertaining to the annual incident response test are stored within {Insert Company Name}’ SharePoint site. Incident Response testing will also be coordinated with other elements responsible for related plans, such as the contingency planning team to simulate a failover to the recovery site. [IR-3 (2)] {Insert Company Name} uses tabletop exercises to test the IRP.

For {Insert Company Name}’ training and testing purposes, the following steps for testing will be taken:

* Coordination of the testing and exercises with other {Insert Company Name} personnel responsible for related plans
* Documentation of the scenario, the list of individuals participating, and the training or testing method used
* Documentation of the results from the exercise
* Documentation of lessons learned and corrective action to be taken
* Implementation of any necessary adjustments to the IRP
* Retention of the results of the training/testing exercises within the {Insert Company Name} {Insert Organization Training Repository}

8.2 Incident Handling [IR-4]

{Insert Company Name} has implemented an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery. An overview of the {Insert Company Name} IR capability is provided in the {Insert Company Name} Incident Response Plan (IRP), {MM/DD/YYYY}, version {X.X}. [IR-4 (a)]

* **Preparation:** Activities include designating specific IRT members to be on-call, having them review the incident response procedures, and ensuring they are trained by shadowing existing team members. Preparation also includes annual IR testing, which involves scenario-based tabletop exercises covering a broad scope of security events.
* **Detection and Analysis:** Achieved through the use of monitoring as well as log collection, aggregation, and correlation tools such as {Insert Logging Repository Name} and {Insert Documentation Repository Name}. {Insert Company Name} centrally manages log correlation using {Insert Logging Repository Name} and alerting via {Insert Documentation Repository Name}. Suspicious events detected trigger alerts in {Insert Documentation Repository Name} for the Information Security Team. A member of the Information Security Team creates a “Report a Security Incident” {Insert Documentation Repository Name} ticket and notifies the appropriate personnel to investigate and analyze the event. All details of incidents are documented within the {Insert Documentation Repository Name} ticket.
* **Containment:** Affected components will be isolated and contained for analysis and investigation – this could be isolating the component or removing it from the network. The precise containment strategy varies depending on the specifics of the security incident.
* **Eradication:** The cause of the incident is remediated. Mitigating exploited vulnerabilities, removing malware, or disabling compromised accounts are all potential remediations depending on the specifics of the security incident.
* **Recovery:** Once the incident has been resolved and the affected component(s) cleared, normal operation for the component will resume.

Customer-reported incidents are initially validated by the {Insert Role or Team Name} and then are escalated to the Information Security Team for handling. All other reported incidents are validated by the IRT in either the production or non-production environments, depending on the nature of the incident. In either case, part of the validation includes a preliminary categorization of the incident type. The IRT in consultation with the IRT PM, as needed, makes the final decision on incident type at this stage of the investigation.

All evidence concerning the incident and incident handling activities are collected and stored in a secure repository. During the post-incident investigation, these records are analyzed to gather insight into areas that require improvement. Post-incident activities (e.g. follow-up) include performing a root cause analysis and the strengthening or implementation of additional controls to prevent recurrences.

{Insert Company Name} coordinates incident handling activities with contingency planning activities by designating the IR Team leaders with the additional role of Contingency Plan (CP) Team leader, allowing the IR Team leaders to switch to a contingency event and activate the contingency plan in the event of a required failover. [IR-4 (b)]

The {Insert Company Name} has a standard incident handling process and ensure that process and the results are predictable and comparable across the {Insert Product Name} Information System. [IR-4 (d)]

{Insert Company Name} incorporates lessons learned from ongoing incident handling activities into incident response procedures, training, and testing/exercises, and implements the resulting changes accordingly. Lessons learned are captured in the after-action report form, where the IR Team documents successes and areas for improvement following an incident. The after-action reports are stored in the {Insert Company Name} secure SharePoint site. [IR-4 (c)]

{Insert Company Name} monitors the {Insert Product Name} Information System for any potential security incidents using multiple security and monitoring tools. Events and logs from these tools are rolled up to {Insert Logging Repository Name} for automatic correlation and analysis by {Insert Documentation Repository Name}. Suspicious events, that may indicate unauthorized use from internal and external sources (such as elevated permissions, {Insert Documentation Repository Name}, and file integrity issues), are identified by {Insert Documentation Repository Name}, which alerts the Information Security Team. [IR-4 (1)]

The {Insert Company Name} IRT uses {Organization Defined} to communicate with team members. The {Insert Documentation Repository Name} ticketing system is used to document and support the incident tracking process. All members of the incident response team are responsible for ensuring tickets remain updated throughout the incident lifecycle.

#### Planning [IR-4 (b)]

The {Insert Company Name} Information Security and Information Technology Leads will coordinate incident handling activities with contingency planning activities using the {Insert Documentation Repository Name} incident system, {Insert Documentation Repository Name}, and {Organization Defined Communications} via pre-configured IRTs. Any collaborative documentation is recorded and will be reviewed for lessons learned and documentation process updates. [IR-4 (b)]

{Insert Company Name} is to ensure that individuals conducting incident handling meet personnel security requirements commensurate with the criticality and sensitivity of the information being processed, stored, and transmitted by the information system.

#### Lessons Learned [IR-4 (c)]

All testing or training of the incident response handling capabilities, including actual incident response events, will include a Lessons Learned section. The Information Security Team documents lessons learned and any recommendations should be incorporated into the incident response capability. If the IRP is updated as a result of the lessons learned, all IRT members will have to review and acknowledge the updated IRP inside of the {Insert Organization Training Repository}, {Insert Product Name}. [IR-4 (c)]

8.3 Incident Monitoring [IR-5]

In the event a system security incident occurs, {Insert Company Name} Information Security Manager will use the {Insert Documentation Repository Name} incident system to track and document all system security incidents, and to record the cause, timeline, and next steps. [IR-5] At a minimum, the following information is included in the ticket when documenting an incident:

* Name of user reporting the incident or method of detection
* Date and time of the incident
* Description of incident
* Categorization of the incident
* Analysis, containment, eradication, and recovery actions

8.4 Reporting Security Incidents [IR-6, IR-6 (1), IR-6 (3)]

If {Insert Company Name} users suspect a security incident, users will contact the {Insert Company Name} Information Security Team via email ({Organization Defined eMail}) or via {Organization Defined Communication}. The Information Security Manager will then decide if this is a legitimate security incident and will open an {Insert Documentation Repository Name} record if necessary. {Insert Documentation Repository Name} will then automatically generate an email alert to the Information Security Team for review of the new {Insert Documentation Repository Name} incident record. [IR-6 (1)]

In the event of a security incident notification, an automated alert, or a suspicious continuous monitoring discovery the {Insert Company Name} Information Security Manager, or delegate, must document a description of the security incident within an {Insert Documentation Repository Name} incident record, the suspected date and time, the individual or system reporting the incident, the level of urgency (if applicable), and report the incident to the Incident Response Team (IRT). The Information Security Manager notifies the agency (or agencies) affected, along with StateRAMP PMO and US-CERT based on the US-CERT incident reporting timelines and in accordance with NIST SP 800-61: [IR-6 (a)]

* CAT 1 - Unauthorized Access: Within one (1) hour of discovery/detection
* CAT 2 - Denial of Service (DOS): Within two (2) hours of discovery/detection if the successful attack is still ongoing and the agency is unable to successfully mitigate activity
* CAT 3 - Malicious Code: Within one (1) hour of discovery/detection if widespread across agency and daily
* CAT 4 - Improper Usage: Weekly
* CAT 5 - Scans/Probes/Attempted Access: Monthly

{Insert Company Name} will provide incident information to: [IR-6 (3)]

* The provider of the product or service for systems or system components related to the incident
* Other organizations involved in the supply chain for systems or system components related to the incident

Information provided to the product or service provider may be useful in preventing incidents for other clients. {Insert Company Name} will use the product or service support portal to report the incident to the product or service provider. Providing incident information to organizations involved in the supply chain, a reseller for example, can raise awareness of the potential for a similar incident type for other clients. {Insert Company Name} will communicate the incident through the supply chain organization’s support portal or via e-mail to a representative of the organization.

Security incidents involving personally identifiable information or unauthorized access to the {Insert Product Name} Information System are reported within one hour of awareness to the government customer Authorizing Official (AO) to support agency compliance to US-CERT (required by OMB Memo M-07-16). The {Insert Company Name} Information Security Manager also reports security incident information according to the *StateRAMP Incident Communications Procedure*. All other security incidents should be reported to the AO within the timeframes specified in the customer SLA or contract. [IR-6 (b)]

* Notifications are done via telephone and followed up with an email
* Phone numbers and email addresses should be used as provided by the agency AO designee
* If necessary, assistance should be requested from the US-CERT
* Procedures in the Incident Response Plan should be followed
* All incident details should be logged in an {Insert Documentation Repository Name}

Upon the resolution of a security incident, the Information Security Manager will verify that all follow-up or remedial actions have been completed.

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

{Insert Company Name} IRT Program Manager provides support to assist users of the {Insert Product Name} Information System in the handling and reporting of all security issues. {Insert Company Name} employees receive mandatory annual security awareness training, which covers privacy, security, information security policies and how to report suspected security incidents. To support automated mechanisms, {Insert Company Name} will have incident response plans (IRPs) and procedures made readily available to personnel via {Insert Company Name} {Insert Documentation Repository Name} and this will be available via the {Insert Organization Training Repository}, {Insert Product Name} for review and acknowledgement by the IRT members. [IR-7]

{Insert Company Name} relies on external partners to augment its incident response capabilities. In addition to the information generated from {Insert Vendor(s) Name}, {Insert Vendor(s) Name}, and {Insert Vendor(s) Name}, {Insert Company Name} has a direct, cooperative relationship with {Organization Defined} to provide additional incident response services such as:

* Triage and identification of incident including live response and analysis
* Development of Indicators of Compromise (IOCs) to be utilized during containment and remediation
* Development of a containment approach and strategy
* Assistance with containment
* Development of remediation/eradication strategy and process
* Incident Response Report that includes investigation findings, investigative steps, containment, and remediation
* Additional remediation recommendations, if applicable

The Information Security Manager communicates with {Insert Vendor(s) Name} throughout a security incident first remotely, and then on-premises if necessary.

{Insert Company Name} implements automated mechanisms to aid in the response to incidents. Automated alerts are configured in {Insert Vendor(s) Name} to send emails to the Information Security Team when {Insert Vendor(s) Name} detects malware, other suspicious files, and unexpected activity. {Insert Vendor(s) Name} is configured to send alerts via email to the Information Security team when various indicators of compromise are detected in the {Insert Product Name} Information System. [IR-7 (1)]

8.6 Incident Response Plan [IR-8]

The {Insert Company Name} {Insert Product Name} Information System Incident Response Plan (IRP): [IR-8 (a)]

* Provides the organization with a roadmap for implementing its incident response capability [IR-8 (a) (1)]
* Describes the structure and organization of the incident response capability [IR-8 (a) (2)]
* Provides a high-level approach for how the incident response capability fits into the overall organization [IR-8 (a) (3)]
* Meets the unique requirements of the organization, which relate to mission, size, structure, and functions [IR-8 (a) (4)]
* Defines reportable incidents [IR-8 (a) (5)]
* Provides metrics for measuring the incident response capability within the organization [IR-8 (a) (6)]
* Defines the resources and management support needed to effectively maintain and mature an incident response capability [IR-8 (a) (7)]
* Addresses the sharing of incident information [IR-8 (a) (8)]
* Is reviewed and approved by the Information Security Manager annually [IR-8 (a) (9)]
* Designates responsibility for incident response to the Information Security Team [IR-8 (a) (10)]

{Insert Company Name} distributes copies of the IRP to all IR Team Members using the {Insert Company Name} secure {Insert Documentation Repository Name}. The IRP is available to Agency customers via {Organization Defined}. Read access is restricted to those with incident response roles and responsibilities. Read-Write access is restricted to Information Security Team members. [IR-8 (b) (e)]

The IRP is reviewed by key personnel at least annually and updated when required. The IRP is tested annually with tabletop, simulated, and functional exercises to ensure the incident handling procedures are up to date. Lessons learned from tabletop exercises, simulations, and actual incidents are also considered when implementing changes to the IRP that provide more effective incident handling procedures. [IR-8 (c)]

The IRP may also be updated based upon changes made to the {Insert Product Name} Information System throughout the Software Development Lifecycle (SDLC) including the planning, the implementation, and the execution phases. The required changes in policy, procedures, plans, or processes are documented in the Incident Response Test Report.

All updates to the IRP are uploaded to the {Insert Product Name} {Insert Organization Training Repository} and assigned to the IRT members for review. All IRT personnel are required to review and acknowledge the updated IRP to ensure that they are knowledgeable of any changes made to the plan. [IR-8 (d)]

8.7 Information Spillage Plan [IR-9]

#### Information Spillage [IR-9 (1), IR-9 (2), IR-9 (3)]

{Insert Company Name} conducts information spillage response training for incident spillage response team members within thirty (30) days of role assignment and conducts annual refresher training thereafter. Proof of this training is retained within {Insert Product Name} for at least one (1) year. [IR-9 (2)]

{Insert Company Name} assigns the following employees to the information spillage response team: [IR-9 (a)]

* {Organization Defined Role or Team}
* {Organization Defined Individual or Team}
* {Organization Defined Role or Team}

{Insert Company Name} contacts potentially affected customers via e-mail in the event of an information spillage. The {Organization Defined Roles or Teams} work with {Insert Product Name} customers regarding contracts and human resources activities to respond to the spillage.

In an information spillage event, the Information Security Team will enact enhanced monitoring to manually continue working while spillage sanitization is completed. [IR-9 (g)] [IR-9 (3)]

#### Information Spillage Response Overview [IR-9, IR-9 (4)]

{Insert Company Name} has documented specific database fields that contain Personal Health Information (PHI) and Personally Identifiable Information (PII) and has labeled these fields as confidential or highly confidential. Updates and reads of these confidential and highly confidential fields are recorded and can be reviewed in the event of information spillage. In the event of an information spillage, internal {Insert Company Name} communications regarding the spill will occur through {Organization Defined Communications}.

Once an information spillage event has been reported to or detected by the Information Security Team, the incident response capability will be initiated to identify and remediate the issue. In the case of an information spillage response, the following steps will be performed:

* All specific information involved will be identified using categorized fields within the {Insert Product Name} Information System. [IR-9 (b)]
* IRT members are notified of the initiation of the incident response plan via {Organization Defined Communications} using a dedicated channel for information spillage incidents within {Organization Defined}. [IR-9 (c)]
* All components and information affected by the information spill are isolated by closing the application gateway to the affected database tenant; blocking all traffic into the information system for the affected tenant, which prevents other information system components from being impacted. [IR-9 (d)]
* The information is eradicated from the contaminated system or components. [IR-9 (e)]
* If the event is a spillage within the {Insert Product Name} Information System database, a rollback of the database to the last known good state will be performed
* If the event is outside of the database (such as a file attachment), {Insert Company Name} will delete the spilled information from the {Insert Product Name} Information System.
* The IRT will conduct reviews within the database transaction logs and within the SIEM, {Organization Defined}, to determine if any other components or systems were affected by the spill and take the necessary actions to contain and eradicate the spill [IR-9 (f)]

The Information Security Manager, the IRT, and specific members of the Information Technology Team such as Database Administrators and Systems Administrators, have been assigned the responsibility of responding to information spills, as well as the {Organization Defined} teams as appropriate. [IR-9 (a)]

All {Insert Company Name} personnel are reminded by {Insert Role Name} that they have signed non-disclosure agreements in the event they are exposed to information not within their assigned access authorization. [IR-9 (4)] All users have been provided basic security awareness training requiring the reporting of an incident. [IR-9 (2)]