Insert Logo Here

Organization Name

Security Procedure

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 Procedure | Noah Brown, CISO |

Table of Contents

[1 Introduction 1](#_Toc68606938)

[2 Purpose 1](#_Toc68606939)

[3 Scope 1](#_Toc68606940)

[4 Roles and Responsibilities 1](#_Toc68606941)

[5 Management Commitment 2](#_Toc68606942)

[6 Authority 3](#_Toc68606943)

[7 Compliance 3](#_Toc68606944)

[8 Procedural Requirements 4](#_Toc68606945)

[8.1 INCIDENT RESPONSE TRAINING AND TESTING 4](#_Toc68606946)

[8.1.1 Information Spillage 4](#_Toc68606947)

[8.2 INCIDENT HANDLING 4](#_Toc68606948)

[8.2.1 PHASES 4](#_Toc68606949)

[8.3 PLANNING 5](#_Toc68606950)

[8.4 LESSONS LEARNED 5](#_Toc68606951)

[8.5 INCIDENT MONITORING 5](#_Toc68606952)

[8.6 REPORTING SECURITY INCIDENTS 5](#_Toc68606953)

[8.7 INCIDENT RESPONSE ASSISTANCE 6](#_Toc68606954)

[8.7.1 INCIDENT RESPONSE ASSISTANCE PERSONNEL 6](#_Toc68606955)

[8.8 INCIDENT RESPONSE PLAN 6](#_Toc68606956)

[8.8.1 INCIDENT RESPONSE PLAN OVERVIEW 6](#_Toc68606957)

[8.8.2 REVIEW AND DISTRIBUTION 7](#_Toc68606958)

[8.9 INFORMATION SPILLAGE RESPONSE 8](#_Toc68606959)

[8.9.1 INFORMATION SPILLAGE RESPONSE OVERVIEW 8](#_Toc68606960)

# Introduction

has developed procedures that identify the security requirements for its information systems and personnel to ensure the integrity, confidentiality, and availability of its information. These procedures are set forth by 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

This document defines the information incident response procedures. These procedures are in place to facilitate the implementation of the Incident Response Policy and associated access controls. In accordance with the policy, these procedures detail how information shall implement and maintain secure access controls on all applicable information systems.

# Scope

The provisions of these policies pertain to all employees, contractors, third parties, and others who have access to company and customer confidential information within systems and facilities.

# Roles and Responsibilities

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

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 system by implementing adequate security controls.

# Authority

These policies and procedures are issued under the authority of the 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 procedures is mandatory. It is 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.

# Procedural 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 TRAINING AND TESTING

It is the responsibility of the {Role} to provide incident response training to personnel within ten (10) business days assuming a position, when required by system changes, as well as refresher training on an annual basis. Incident Response Plan (IRP) training will be performed by each individual IRT member through the {Tool}. The {Tool} will require individual acknowledgement that the IRP was reviewed.

As part of Organization Name testing and training, incident response capabilities will be tested on an annual basis. Incident Response testing will also be coordinated with other elements responsible for related plans. Organization Name uses tabletop exercises to test the IRP.

For Organization Name training and testing purposes, the following steps for test will be taken:

* Coordination of the testing and exercises with other Organization 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 Organization Name {Repository}

### Information Spillage

Organization Name has documented specific database fields that contain PHI and 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 Organization Name communications regarding the spill will occur through {Tool}

If an information spillage event occurs, the IRT will block all communication to the impacted database tenant through {define how isolation of affected data will occur} Eradication of the spillage can consist of:

* Deleting data outside of the database such as attachments associated with the spillage event
* Rollback of the information system database to the last known good state

The IRT will conduct reviews within the database transaction logs and within the SIEM, {Tool}, to identify contaminated components. Organization Name contacts potentially affected customers via e-mail in the event of an information spillage.

## INCIDENT HANDLING

### PHASES

Automated mechanisms must be implemented to assist in the incident response capability. Organization Name uses the {Tools}. The solution must be configured to address the following phases:

* **Preparation:** The {Role} is responsible for the oversight and how the solution prepares for incident handling.
* **Detection and Analysis:** Alerting will be configured to detect anomalies outside the standard baseline, as well as a weekly audit review.
* **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.
* **Recovery:** Once the incident has been resolved and the affected component(s) cleared, normal operation for the component will resume.

## PLANNING

The Organization Name {Role} and {Role} will coordinate incident handling activities with contingency planning activities using the Organization Name {Tools} via pre-configured IRTs. Any collaborative documentation is recorded and will be reviewed for lessons learned and documentation process updates.

Organization 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

All testing or training of the incident response handling capabilities, including actual incident response events, will include a lesson learned. {Role} shall document 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 sign off on the updated IRP inside of {Tool}.

## INCIDENT MONITORING

In the event a system security incident occurs, Organization Name {Role} will use the Organization Name {Tool} to track and document all system security incidents.

## REPORTING SECURITY INCIDENTS

In the event of a security incident notification, Organization Name {Role} must document a description of the security incident within an {Tool} 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).

When reporting security incidents, the following reporting timeline consistent with NIST SP 800-61 will be employed:

* 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

If Organization Name users are aware of a security incident, users will contact the Organization Name {Role} via email {Insert email} or {Other communication/Chat}. The {Role} will then decide if this is a legitimate security incident and will open an {Tool} security incident record if necessary. The Organization Name {Role} will decide on urgency of the incident based on the type of incident that occurred. Upon the resolution of a security incident, the {Role} will verify that all follow-up or remedial actions have been completed.

## INCIDENT RESPONSE ASSISTANCE

### INCIDENT RESPONSE ASSISTANCE PERSONNEL

* Organization Name provides an incident response support resource through {Company/Partnership} to strengthen Organization Name incident response capability. This resource offers advice and assistance to users of the information system for the handling and reporting of security incidents.
* To support automated mechanisms, Organization Name will have incident response plans (IRPs) and procedures made readily available to personnel via Organization Name {Repository} and this will be available via {Tool} for review and sign-off for the IRT members.
* Organization Name will coordinate their incident response support resource with other external providers of information system protection capability. In the event that external resources are needed, the planned company to provide this service is {Company Name}. The {Role} retains needed contact information for engaging {Company Name} support with security incidents.

## INCIDENT RESPONSE PLAN

### INCIDENT RESPONSE PLAN OVERVIEW

The following statements and references provide an overview of the incident response plan. For complete details, see the *{SSP\_A\_IRP\_V1.0\_20210406}*

* **Implementation Roadmap:** Contained in *{SSP\_A\_IRP\_V1.0\_20210406}*
* **Structure and Organization:** Contained in *{SSP\_A\_IRP\_V1.0\_20210406}*
* **Incident Response Team Lead:** {Name} {Role}
  + {Email}
  + {Phone Number}
* **Incident Responder:** {Name} {Role}
  + {Email}
  + {Phone Number}
* **Requirements:** Organization Name {Team/Role} will receive the first reports of an incident within the information system, if deemed a security event, the {Team/Role} will contact the {Team/Role} to report the security incident.
* **Security related reportable incidents:**
  + Unauthorized access
  + Data breach
  + Data spillage
  + Malicious code
  + Access/security breach (remote or onsite)
  + Improper (malicious) usage
  + File changes (may be security related)
  + Domain Name System (DNS) Server Denial of Service (DOS)
  + Worm and Distributed Denial of Service (DDOS) Attack
  + Network (Port Scans/Network Probes)
* **Non-security related reportable incidents:**
  + Authorized user cannot access
  + A system component is not operational
  + Performance degradation
  + Meeting unexpected disconnected
  + Not able to upload or use content
* **Metrics:** Defined in IRP
* **Resources and/or management:** The {Team/Role} and Organization Name leadership will be involved in all incident resolutions. The involvement of said groups is mentioned in the IRP and is part of the run books. Each incident may vary the needed involvement.
* **Review and/or approval:** The IRP is reviewed on an annual basis. The IRP is updated if needed improvements are found during the annual review, if improvements are found from lessons learned following the use of the IRP, or if improvements are found during the testing or training phases of the IRP.

### REVIEW AND DISTRIBUTION

It is the responsibility of the {Team/Role} to distribute the incident response plan via {Tool}, to the following list of individuals, including any changes to the plan:

* The Incident Response Team
* Any Organization Name personnel who are involved in an incident and its response

Organization Name will ensure and maintain the protection of the IRP from unauthorized disclosure and modification by sharing a read-only, secured copy of the plan with only those who need access to the IRP.

## INFORMATION SPILLAGE RESPONSE

### INFORMATION SPILLAGE RESPONSE OVERVIEW

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

* All specific information involved will be identified using categorized fields within the information system
* IRT members are notified of the initiation of the incident response plan via {Tools} using a dedicated channel for incident spillage within {Tool}.
* 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
* The information is eradicated from the contaminated system or components.
  + If the event is a spillage within the 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), Organization Name will delete the spilled information from the information system.
* The IRT will investigate the rest of the system to determine if any other components or systems were affected by the spill and take the necessary actions to contain and eradicate the spill

The IRT and specific members of the {Team/Role} such as Database Administrators and Systems Administrators, have been assigned the responsibility of responding to information spills

All Organization Name personnel have signed non-disclosure agreements in the event they are exposed to information not within their assigned access authorization. All users have been provided basic security awareness training requiring the reporting of an incident.