**Incident Response Plan**

**COMPANY NAME**

**Version #**

**Last Revision Date:**

Document Classification

**Table of Contents**

[Policy Requirement Reference 3](#_Toc50534065)

[Executive Summary 3](#_Toc50534066)

[Preparation planning 4](#_Toc50534067)

[Staff Support 4](#_Toc50534068)

[Detection and Analysis 6](#_Toc50534069)

[Incident Detection 6](#_Toc50534070)

[Incident Identification 6](#_Toc50534071)

[Incident Classifications 6](#_Toc50534072)

[Incident Severity 6](#_Toc50534073)

[Containment, Eradication and Recovery 8](#_Toc50534074)

[Form Response Team 8](#_Toc50534075)

[Incident Response Support and Coordination 8](#_Toc50534076)

[Create Communication Plan 8](#_Toc50534077)

[Containment 8](#_Toc50534078)

[Eradication and Recovery 9](#_Toc50534079)

[Resume Operation 9](#_Toc50534080)

[Post Incident Review 10](#_Toc50534081)

[Follow Up 10](#_Toc50534082)

**Plan Information**

|  |  |
| --- | --- |
| **Prepared By / SSP Point-of-Contact** | |
| **Name:** |  |
| **Department / Title:** |  |
| **Email Address:** |  |
| **Phone #:** |  |

**Revision History**

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Revision Date** | **Description** | **Pages Affected** |
| 1.0 | [DATE] | Initial version of Information Response Plan | All |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Policy Requirement Reference

|  |  |  |
| --- | --- | --- |
| **Control #** | **Control Description / Requirement** | **NIST 800-53** |
| **3.3.3** | Review and update audited events. | AU-2(3) |
| **3.3.5** | Correlate audit review, analysis, and reporting processes for investigation and response to indications of inappropriate, suspicious, or unusual activity. | AU-6(3) |
| **3.3.6** | Provide audit reduction and report generation to support on-demand analysis and reporting. | AU-7 |
| **3.6.1** | Establish an operational incident-handling capability for organizational information systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities. | IR-2 IR-4 IR-5 IR-6 IR-7 |
| **3.6.2** | Track, document, and report incidents to appropriate officials and/or authorities both internal and external to the organization. | IR-4 IR-6 IR-7 |
| **3.6.3** | Test the organizational incident response capability. | IR-3 IR-3(2) |
| **3.14.1** | Identify, report, and correct information and information system flaws in a timely manner. | SI-2 |
| **3.14.3** | Monitor information system security alerts and advisories and take appropriate actions in response. | SI-5 |

Executive Summary

This plan defines a National Institute of Standards and Technology (NIST) compliant incident response plan for use by *[COMPANY NAME]*. The purpose of this plan is to make incident response more simplistic and consistent for all potential types of incidents. NIST compliance enhances the scalability of the plan, allowing interaction with customer, local, state, and federal resources using common methods and terminology.

Incidents response occurs in four phases.   
**1. Preparation:** Preparation must be completed before effective response to an incident can occur. Different incident types require different preparation. For each incident response, several things need to be in place prior to the occurrence of an incident such as: contact information and methodologies for team members; facilities for meetings, work, storage, and other activities related to the incident response; hardware and software tools needed for the recognition and handling of the incident; as well as documentation and other knowledge bases needed for effective response to the incident.

**2. Detection and Analysis** – First reports of an incident may come from a customer report, monitoring tools or other methods. At this step, the incident is vetted for validity and categorized for type and severity. Preliminary notifications and communications are established. Appropriated response procedures, personnel, and tools are assembled.

**3. Containment, Eradication, and Recovery** – Based on the results of detection and analysis, the proper response procedure is implemented. Immediate steps are taken as appropriate to limit loss from the incident. Evidence is preserved. Impact of this containment to customers and the enterprise is communicated to those affected. A long-term resolution of the incident is developed and implemented. This step may include policy alteration or development, system redesign, introduction of new systems or technologies, training, or other actions deemed necessary to permanently resolve an incident. As necessary, systems are restored and brought back online, data is restored, and appropriate parties are notified.

**4. Post Incident Activity** – Report of the incident from start to conclusion is finalized. Updated incident response procedures, lessons learned, and documentation of any permanent changes to systems because of the incident are generated. Incident data collected is analyzed to determine such things as the cost of the incident in money, time, etc. Evidence retention policies and procedures are implemented.

General points regarding this plan:

1. Communication to appropriate parties will be maintained throughout the incident. Critical communication paths are between response team members, between the response team and senior leadership, and between senior leadership and customers. Some of these communication paths may need to be secure. Communication procedures should be developed to be consistent across incident response procedures.
2. All procedures should be available and accessible. This means that all procedures should be maintained through several different methods in case an incident renders one or more methods unavailable. All updates must be communicated to all those who may be involved in a response.

Preparation planning

Staff Support

**Background:** It is important to pre-identify the necessary roles for the purpose of incident response. Required knowledge and skill sets should be in place prior to the need for an incident response. Individuals with the required knowledge and skill sets should always be available to respond to an incident. A single individual may perform several roles concurrently. Members of an incident response group may or may not participate in a similarly labeled group in their day to day work. Specific incident response will dictate which roles are necessary and activated.

**Roles:**

1. Response Team
   1. Incident Commander - Management level person(s) with the authority to make high level decisions and approve actions to be taken by the incident response team.
   2. Information Officer – Person who disseminates public and non-sensitive information to interested parties.
   3. Liaisons – Persons who are the point of contact for customers, governmental and/or non-governmental agencies and organizations.
   4. Safety Officer – Person who monitors incident operations and advises on matters related to operational safety.
   5. Legal - Advises incident command on legal matters
   6. Documentation Lead - responsible for maintaining accurate and complete incident records including major steps taken to resolve an incident. Also maintains and stores incident information for legal, analytical, and historical purposes
   7. Communication Specialist - Responsible for developing, implementing, and maintaining a communication plan for the incident.
   8. Human Resource Specialist – Responsible for advising the response team about HR matters including privacy
2. General Response Staff
   1. Operations staff – responsible for the functional aspects of the incident command structure
      1. Operations Chief and deputies
         1. Directly manages all incident tactical activities
      2. Security SME/Analysts:
         1. Intrusion and Monitoring SME and Analysts – Person(s) with firewall, IPS, and monitoring tool experience.
         2. Forensic SME - Person(s) with systems analysis and forensic ability and experience
      3. Network SMEs – Network SMEs (local area networks, area specialists) – Persons with experience and authorization necessary to manage affected local area networks.
      4. Database SMEs – person(s) with experience and authorization necessary to manage affected database systems.
      5. Server Platform SMEs - person(s) with experience and authorization necessary to manage affected server platforms
      6. Web Application SMEs - person(s) with experience and authorization necessary to manage affected web server applications
      7. Management Application SMEs - person(s) with experience and authorization necessary to manage affected management information systems
      8. Desktop Application SMEs - person(s) with experience and authorization necessary to manage affected workstation-based applications.
   2. Finance / Administration staff
      * 1. Finance Leadership – Management level person responsible for determining current and anticipated requirements and potential impact

Detection and Analysis

Incident Detection

Once a security incident is identified it is classified and prioritized. Depending on the priority of the incident, the Response Team will determine if the company needs support in its incident response. All incidents should be entered into the incident log at the time of classification and prioritization.

Incident Identification

Incidents may be detected by the company, third-party support organizations or customers. Incident detection will in general occur as a report to the help desk or through ongoing system monitoring by the Security SME.

Incident Classifications

All incidents are classified according to the following criteria. An incident may fit into more than one defined type. A 'security incident' can be defined as any security related event that has an actual or potential adverse effect on company data or systems, or the violation of an explicit or implied security policy. Although references to many other incident types can be found in documentation, they seem to all fall in one of the three categories. For example, malicious code such as a virus or trojan will be first recognized as a denial of service, unauthorized access, or inappropriate usage, depending on the payload of the malicious code. Using these three incident types tailored responses can be developed to cover any incident.

**Incident Types:**

**Denial of Service:** An incident by which authorized access to systems or data is prevented or impaired. Usually a denial of service (DoS) incident is a security event if the DoS is due to malicious intent. Not all events that prevent or hinder authorized access to systems or data are security incidents. The mechanical, electrical, or administrative failure of a system or access mechanism may not be a security incident.

**Unauthorized Access:** An incident where unauthorized access is attempted or gained to systems or data. This access can be logical or physical in nature. Unauthorized access is any access for which permission has not been granted. Such permissions would include connect, authenticate, read, write, create, delete, modify, etc. This unauthorized access can be by an individual or another system.

**Inappropriate Usage:** An incident by which acceptable use policies are violated. Acceptable use policies may include what types of data may be accessed or transmitted, how information may be accessed or transmitted, and where information may be received from or transmitted to.

Incident Severity

Once the incident is categorized it is prioritized according to its severity level. The appropriate response to an incident is dependent on the severity rating of the incident.

**Method for Determining Severity:**

By adding the scores from the following evaluation criteria, a severity rating is established:

1. Potential number of affected parties: How much productivity is impacted by this incident?
   1. Less than 1% of systems; less than 1% of workforce = 1
   2. More than 1%, but less than 10% of systems; more than 1% but less than 10% of workforce = 2
   3. More than 10% of systems; more than 10% of workforce = 3
2. Probability of widespread escalation. Does this incident have the potential to spread to unaffected systems?
   1. Minimal = 1
   2. Moderate = 2
   3. High = 3
3. Commonality. Has this occurred in the past; is there experience in mitigating this incident?
   1. Commonly Seen = 1
   2. Occasionally happens = 2
   3. Rare = 3
4. Potential for damage or loss. How expensive is the incident expected to be, both in lost production and in mitigation costs?
   1. Minimal = 1
   2. Moderate = 2
   3. High = 3
5. Business impact. What is the expected negative impact on the overall health of the enterprise both in short- and long-term contexts?
   1. Minimal = 1
   2. Moderate = 2
   3. High = 3, Certain types of data, due to regulatory and/or legal definitions are always classified as ‘High’. One example would be HIPAA covered Electronic Protected Health Information

This score can be used to determine the severity as follows:

|  |  |  |  |
| --- | --- | --- | --- |
| **Priority Guideline** | **Score** | **Initial Action** | **Containment Goal** |
| Severe | 13-15 | Immediately | ASAP |
| High | 11-12 | Immediately | <24 Hours |
| Medium | 8-10 | Within 4 hours | <72 Hours |
| Low | 5-7 | Within 24 hours | <7 Days |

(Reference: SANS Incident Handling and Intrusion detection)

Containment, Eradication and Recovery

Form Response Team

Once the incident has been categorized and an appropriate severity level has been identified, the process enters the phase of Containment, Eradication and Recovery.

The first step in creating and executing the incident response plan is activation of the IMT and response teams when necessary. Team members are assigned based upon the required rolls as listed in the preparation phase of incident response.

Incident Response Support and Coordination

Response Team members provide incident information to senior leadership. General support staff develop and document mitigation and recovery strategies to address the immediate threat for distribution to the rest of the company, as necessary. This notification can be achieved through secure mailing list aliases, secure web intranet or extranet servers, or even via phone or fax. Timely information that is important for all organizational staff to receive can be distributed via internal employee mailing lists if necessary.

Response coordination is provided primarily by the Response team. The team members confirm that local administrators have implemented the appropriate actions and relay this information back to the senior leadership.

Create Communication Plan

A communication plan is created for each phase of containment, eradication and recovery identifying who within the company will be contacted once each phase is complete.

Containment

Containment processes can include:

* Disconnect suspected subnet
* Terminate operation
* Observation and assessment
* Run full system backup
* Determine duration of termination
* Notify help desk
* Change the passwords on the compromised systems
* Vulnerability analysis to identify the root cause
* Encapsulation of incident
* Any action deemed necessary to mitigate the incident

Containment times vary according to the level of severity of the incident. Containment steps will be carried out in different order and concurrency depending on the nature of the incident.

Eradication and Recovery

Eradication and recovery occur concurrently and involves the following activities:

* Eradication actions for specific incident type
* Follow change management procedures
* Perform recovery procedures
* System verification
* Remove malicious code/virus
* Assess the impact on operating systems
* Harden the operating systems
* Remove dormant user ID’s
* Tighten access rights
* Shut down and restart systems/services for DoS
* Software/Hardware configuration changes
* Restoration from previous backup
* Re-installation.

Resume Operation

Once eradication and recovery have been completed successfully, normal operations can resume. Appropriate communication will occur at this time.

Post Incident Review

Post Incident Activity – The Response Team and General Response Staff will attend a debriefing meeting and an After-Action Report (AAR) of the incident from start to conclusion is developed which will include an improvement plan. Documentation of any permanent changes to systems because of the incident are generated. Incident data collected is analyzed to determine such things as the cost of the incident in money, time, etc. Evidence retention policies and procedures are implemented.

Follow Up

Specific follow up activities include

* Monitor affected systems
* Update incident log
* Perform post-mortem
* Incident documentation
* Media-Handling
* Update incident response procedures