**Name of Organization**

**Incident Response Plan**

December 2021

**Revision History**

|  |  |  |  |
| --- | --- | --- | --- |
| Revision Number | Revision Date | Summary of Changes Made | Changed By |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Instructions

The (Name of Organization) Incident Response Plan is designated For Official Use Only (FOUO) and is the property of (Name of Organization). Only (Name of Organization) representatives may distribute the handbook to individuals on a need-to-know basis. Distribution by other individuals without prior authorization is prohibited. This document is unclassified but contains sensitive information.

**Table of Contents**

[I. Purpose 6](#_Toc89329870)

[II. Mission 6](#_Toc89329871)

[III. Scope 7](#_Toc89329872)

[IV. Incident Response High Level Process 8](#_Toc89329873)

[V. Confidentiality 9](#_Toc89329874)

[VI. Report Management 9](#_Toc89329875)

[Cyber Security Incident Log 9](#_Toc89329876)

[Incident Summary Report (ISR) 9](#_Toc89329877)

[Process Improvement Plan (PIP) 10](#_Toc89329878)

[VII. Resource Planning 10](#_Toc89329879)

[VIII. Roles and Responsibilities 10](#_Toc89329880)

[Incident Commander 11](#_Toc89329881)

[Chief Security Information/Technology Officer (CISO/CIO/CTO) 11](#_Toc89329882)

[Incident Handling Team (IHT) 12](#_Toc89329883)

[Cybersecurity Incident Response Team (CIRT) 12](#_Toc89329884)

[Incident Response Team Members 12](#_Toc89329885)

[Cost Unit Leader 13](#_Toc89329886)

[Documentation Unit Leader 13](#_Toc89329887)

[Support Teams 14](#_Toc89329888)

[IX. Incident Response Life Cycle 17](#_Toc89329889)

[Preparation 17](#_Toc89329890)

[Preventing Incidents 17](#_Toc89329891)

[Detection and Analysis 18](#_Toc89329892)

[Signs of an Incident 18](#_Toc89329893)

[Sources of Precursors and Indications 18](#_Toc89329894)

[Incident Analysis 18](#_Toc89329895)

[Incident Documentation 19](#_Toc89329896)

[Incident Prioritization 19](#_Toc89329897)

[Containment, Eradication, and Recovery 20](#_Toc89329898)

[Choosing a Containment Strategy 20](#_Toc89329899)

[Evidence Gathering and Handling 20](#_Toc89329900)

[Forensics for standard computers 20](#_Toc89329901)

[Forensics for mobile devices 20](#_Toc89329902)

[Identifying the Attacker 20](#_Toc89329903)

[Eradication and Recovery 21](#_Toc89329904)

[Post-Incident Activity 21](#_Toc89329905)

[Lessons Learned 21](#_Toc89329906)

[Using Collected Incident Data 21](#_Toc89329907)

[Evidence Retention 22](#_Toc89329908)

[Incident Handling Forms, Documents and Standard Operating Procedures 23](#_Toc89329909)

[X. Notification and Communication 23](#_Toc89329910)

[XI. Regional and national Incidents 24](#_Toc89329911)

[XII. Plan Testing and Review 24](#_Toc89329912)

[XIII. Incident Response Contact List 25](#_Toc89329913)

[XIV. Appendix 1 - Reference Resources 28](#_Toc89329914)

[NIMS Guideline for Resource Management Preparedness 28](#_Toc89329915)

[NIMS Communications and Information Management Standards 29](#_Toc89329916)

# Purpose

The (Name of Organization) Incident Response Plan (“the Plan”) has been developed and is owned by the Organization Executive Team to provide direction and focus to the handling of information security incidents that adversely affect (Name of Organization) Information Resources.

Processes and nomenclature of this Plan and all supporting documents are aligned with NIST Incident Response documentation and National Incident Management System (NIMS). Although most Cybersecurity incidents will be internal or local with limited scope (e.g., organizations’ clients, vendors, and Internet Service Providers (ISPs)), organizational management staff and Incident Commanders will need to know when and how to engage with NIMS.

To implement this Plan successfully and be able to respond to incidents that will be regional or national and require collaboration and coordination with multiple agencies, it is strongly recommended that the (Name of Organization) management teams maintain staff trained within the key areas of NIMS:

* Resource Management
* Command and Coordination
* Communications and Information Management
* Incident Command System

Further, it is key that the organization adheres to the [**National Preparedness Goal**](https://www.fema.gov/emergency-managers/national-preparedness/goal) focusing on - prevention, protection, mitigation, response and recovery.

# Mission

The (Name of Organization) Incident Response Plan applies to any person or entity charged by the (Name of Organization) Incident Commander with actions in relation to a response to information security related incidents at the organization, and specifically those incidents that affect (Name of Organization) Information Resources. The purpose of this Plan is to facilitate a well-understood, consistent, appropriate, and rapid response capability to information security incidents. The Organization will satisfy handling of Security Incidents through a formal Cybersecurity Incident Response Team (CIRT).

This plan should:

* Integrate into existing processes and organizational structures so that it enables rather than hinders critical business functions
* Be part of an overall strategy to protect and secure critical business functions and assets
* Strengthen and improve the capability of the organization, where required, to effectively manage security events and thereby keep intact the availability, integrity, and confidentiality of an organization’s systems and critical assets
* Align with incident command structures, reporting lines and collaboration with National Management Incident System (NIMS) where applicable, for regional or national emergencies where cybersecurity is part of the incident or emergency.
* Support, complement, and link to any existing Business Continuity or Disaster Recovery plans where and when appropriate
* Support, complement, and provide input into existing business and IT policies that impact the security of an organization’s infrastructure
* Implement a command-and-control structure, clearly defining roles and responsibilities, as well as accountability for decisions and actions
* Be consistent with existing organization and Agencies terminology, processes, and expectations, to support collaborative and efficient communications
* Take advantage of existing resources, knowhow, processes, and systems at the national, state, and regional levels

**Incident Definition**

A violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices that jeopardizes the confidentiality, integrity, or availability of information resources or operations. A security incident may have one or more of the following characteristics:

* Violation of an explicit or implied (Name of Organization) security policy
* Attempts to gain unauthorized access to a (Name of Organization) Information Resource
* Denial of service to a (Name of Organization) Information Resource
* Unauthorized use of (Name of Organization) Information Resource
* Unauthorized modification of (Name of Organization) information
* Loss of (Name of Organization) Confidential or Protected information
* Loss of business operational capability

This document only applies to adverse events that are computer systems security related, be they through malicious intent or human error, not necessarily those caused by natural disasters, power failures, etc.

For Incident Classification, please see document *“Incident Response Categorization”*

# Scope

(Name of Organization) establishes and maintain capabilities to respond effectively to electronic intrusions into the Organization network infrastructure. The assigned Incident Commander will be in charge to manage and coordinate CIRT analysis and planning activities which will support proactive development of authorized, coordinated responses to incidents. The CIRT also will contribute to incident recovery activities after intrusions are contained. All CIRT members, as well as their management, are covered by the Incident Response Plan and must comply with its associated procedures and guidelines.

While the primary purpose is to deploy and test an organizational Incident Response plan, it must also be able to manage and coordinate other organizations and agencies in case of a major, regional, or national Incident. The Organization needs to be able to adopt and align with National Incident Management System (NIMS) – specially to receive Federal [Preparedness Grants](https://www.fema.gov/grants/preparedness).

# Incident Response High Level Process

The High-Level process below identifies Incident Response escalation related to internal, regional, or national incidents, and shows when or where NIMS ICS may apply.



# Confidentiality

During a Cyber Security Incident investigation, the Incident Commander, or members of the Cybersecurity Incident Response Team (CIRT) will be gathering information from multiple computer systems and/or conducting interviews with key personnel based on the scope of the incident in question. All information gathered or discovered during a Cyber Security Incident will be treated as strictly confidential throughout the investigative process. All members of the CIRT are trained in information security and data privacy best practices. At the conclusion of the investigative process, the Incident Commander will brief the executive team on the relevant details of the incident and the investigation. During the investigation phase, no confidential information will be shared unless it is strictly relevant to the investigation and/or the incident itself or needs to be shared with authorized parties due to legal or regulatory requirements. Details on communication and information sharing is outlined in documents “Regulatory Notification Requirements” and “IR Customer and Media Communication”.

# Report Management

All reports generated during an investigation along with any evidence gathered will be stored and managed by the Incident Commander. Any physical records will be stored at the Incident Commanders office in a locked file. Any digital records will be stored on the Organization network share only accessible by the Incident Commander and approved CIRT staff. That share will be backed up and stored in accordance with Organization’s regular backup procedures. In the event past records of incidents need to be reviewed, a written request must be made to the Incident Commander that includes the requestor, the information requested and the reason for the request. The Incident Commander will review the request and has the discretion to approve or deny any request. Incident summary information will always be made available by the Incident Commander.

## Cyber Security Incident Log

The Cyber Security Incident Log is the central repository for captured critical information about a Cyber Security Incident and the organizations response to that incident and should be maintained while the incident is in progress. See Document “*Incident Response Log”.*

## Incident Summary Report (ISR)

The ISR is a document prepared by the Incident Commander at the conclusion of a Cyber Security Incident and provides a detail of the incident, including how and why it may have occurred, estimated data loss, affected parties, and impacted services. Finally, it will examine the procedures of the Cyber Security Incident Response Plan, including how the CIRT followed the procedures and whether updates through lessons learned are required. The template for the ISR is the document *“IR Summary Report”*

## Process Improvement Plan (PIP)

The PIP is a document prepared by the Incident Commander as part of the Lesson learned Process at the conclusion of a Cyber Security Incident and provides recommendations for avoiding or minimizing the impact of future Cyber Security Incidents based upon the “lessons learned” from the recently completed incident. This plan should be kept confidential.

# Resource Planning

To be successful in responding to incidents the organization should implement and maintain a comprehensive resource management process. This will help align resource capabilities not only for their organization, but also if needed to align resource management and terminology, to streamline resource coordination and ensure interoperability nationwide. Each organization that owns, maintains, and operates these resources is responsible for managing details of the minimum capabilities, interoperability, and mechanisms for sharing of these resources during an incident.

# Roles and Responsibilities

During a security incident multiple organizations and team members need to be ‘activated’ to respond to the incident at hand. Depending on the categorization of the incident and its size, collaboration with regional agencies using The National Incident Management System (NIMS) may be required. It is highly recommended that all supporting staff (technical, non-technical and management/leadership) familiarize themselves not only with their organizational processes and plans, but also complete at least the basic training of The National Incident Management System (NIMS) Training Program including:

* IS-100: Introduction to the Incident Command System, ICS-100
* IS-200: Basic Incident Command System for Initial Response, ICS-200
* ICS-300: Intermediate Incident Command System for Expanding Incidents
* IS-700: National Incident Management System, An Introduction
* IS-800: National Response Framework, An Introduction
* E/G/L 0191: Emergency Operations Center/Incident Command System Interface

Below are the key roles for Cybersecurity Incidents (based on NIST and NIMS as applicable). All other FEMA NIMS Job Titles/Position Qualifications as they pertain to all other incidents/emergencies and supporting functions can be found [**here.**](https://www.fema.gov/emergency-managers/nims/components/positions)https://www.fema.gov/emergency-managers/nims/components/positions

## Incident Commander

The Incident Commander (IC) owns the Plan. The responsibilities of the IC may be a component of the CISO roles and responsibilities or be a distinct full-time role within the organization. The Incident Commander:

* Acts as the primary person responsible for formally declaring a cyber security incident and managing team response activities.
* Acts as focal point and liaison for all communications to and from the CIO/CTO, DPO, and executive leadership.
* Oversees and prioritizes actions during the detection, analysis, and containment of an incident. They are also responsible for conveying the special requirements of high severity incidents to the rest of the organization as well as communicating potential impact to the CIO/CTO
* Responsible for understanding the SLAs in place with third parties, and the role third parties may play in specific response scenarios
* Aligns and collaborates with other agencies and/or Emergency Operation Centers
* Ensure team activities comply with legal and industry requirements for incident response procedures.
* Ensures after-action reports are completed.
* Authorizes information release to the media.
* Orders demobilization as needed.

## Chief Security Information/Technology Officer (CISO/CIO/CTO)

* Seek approval from Executive Management for the administration of the Plan.
* Coordinate response activities with auxiliary departments and external resources as needed to minimize damage to information resources.
* Provide updates on response activities to Incident Handling Team (IHT) and other stakeholders during an incident.
* Ensure service level agreements (SLAs) with service providers clearly define expectations of the organization and deliverables of the service provider in relation to incident response.
* Ensure policies related to incident management accurately represent the goals of the organization, and are regularly reviewed for such.
* Review the Plan to ensure that it meets policy objectives and accurately reflects the goals of the organization. Seek Plan approval from IHT.
* Work with the Incident Commander (IC) to periodically evaluate the effectiveness of the Plan and CIRT.
* Ensure CIRT managers are given the necessary authority to seize assets and stop services quickly to contain an incident.
* Approve close of moderate or critical-severity incidents.
* Ensure Cyber Insurance is maintained as necessary and appropriate stakeholders are informed.

## Incident Handling Team (IHT)

Consists of legal experts, risk managers, data privacy officer (DPO), Public Information Officer (PIO) and other department managers that may be consulted or notified during incident response.

* These experts advise on incident response activities relevant to their area of expertise.
* Maintain a general understanding of the Plan and policies of the organization.
* Ensure incident response activities are in accordance with legal, contractual, and regulatory requirements.
* Participate in tests of the Plan and procedures.
* Team is responsible for internal and external communications pertaining to cyber security incidents.

## Cybersecurity Incident Response Team (CIRT)

The CIRT is comprised of IT management and experienced IT and Security personnel. The role of the CIRT is to promptly handle an incident so that containment, investigation, and recovery can occur quickly. Where third-party services are leveraged, ensure they are engaged as necessary.

## Incident Response Team Members

The Incident Commander is supported by a team of technical staff that work directly with the affected information systems to research the time, location, and details of an incident. Team members are typically comprised of subject matter experts (SMEs), senior level IT staff, third parties, and outsourced security or forensic investigation partners.

Further responsibilities:

* Assist in incident response as requested. CIRT responsibilities should take priority over normal duties.
* Understand incident response plan and procedures to appropriately respond to an incident.
* Continue to develop skills for incident response management.
* Ensure tools are properly configured and managed to alert on security incidents/events.
* Analyze network traffic for signs of denial of service, distributed denial of service, or other external attacks.
* Review log files of critical systems for unusual activity.
* Monitor business applications and services for signs of attack.
* Collect pertinent information regarding incidents at the request of the Incident Commander.
* Consult with qualified information security staff for advice when needed.
* Ensure evidence gathering, chain of custody and preservation is appropriate.
* Participate in tests of the incident response plan and procedures.
* Be knowledgeable of service level agreements with service providers in relation to incident response.

## Cost Unit Leader

The Incident Commander may assign a team member to begin formal cost and financial documentation of the incident. This function should include:

* Collecting and recording incident cost data
* Maintaining cumulative incident cost documentation at the direction of the Finance/Administration Section Chief to meet Authority Having Jurisdiction (AHJ) needs
* Performing cost-effectiveness analyses
* Providing incident-related cost estimates and cost-saving recommendations

## Documentation Unit Leader

The Incident Commander may assign a Documentation Unit leader that manages staff who maintain incident files and data for legal, analytical, and historical purposes, including a complete record of the major steps taken to resolve the incident. This function includes:

* Overseeing the maintenance of accurate, complete, up-to-date incident files
* Ensuring that each section maintains and submits appropriate files for post- incident documentation purposes
* Providing duplication services to support incident operations
* Assisting with compiling, reproducing and distributing the Incident Action Plan (IAP)
* Ensuring that all personnel who handle data or intelligence are aware
* Maintain a document security plan to manage the confidentiality and security of any classified, confidential, sensitive and For Official Use Only (FOUO) documentation, intelligence, data or incident information

## Support Teams

|  |
| --- |
| **OPERATIONS** |
| **Role** | **Responsibilities** | **Prevention** | **Incident Response** |
| InfoSec Technical Assessment Team | * Conduct incident investigation and evidence collection
 |   | ✔ |
| * Assure evidence preservation, including data handling and chain of custody
 |   | ✔ |
| * Maintain investigative history
 |   | ✔ |
| Windows  | * Maintain Windows environment to Organization standards
 | ✔ |   |
| * Confirm Windows installation of anti-virus to Organization standards
 | ✔ |   |
| * Preserve evidence in the Windows environment
 |   | ✔ |
| * Provide resource assistance in the event of an incident
 |   | ✔ |
| UNIX | * Ensure applications are patched to Organization standards
 | ✔ |   |
| * Preserve application evidence in the UNIX environment
 |   | ✔ |
| * Provide resource assistance in the event of an incident
 |   | ✔ |
| Desktop | * Maintains Windows machines to Organization standards
 | ✔ |   |
| * Preserves evidence related to desktop investigation
 |   | ✔ |
| * Provide resource assistance in the event of an incident
 |   | ✔ |
| Network | * Support segregation and isolation activities, as directed
 |   | ✔ |
| * Preserve network-related evidence
 |   | ✔ |
| * Communicate network partner security alerts or incidents to Organization Security when received
 | ✔ | ✔ |
| Solution Center | * Capture and escalation of potential Information Security incidents
 |   | ✔ |
| * Support communication to users and the user community, as appropriate
 |   | ✔ |
| * Support remediation activities when required
 |   | ✔ |

|  |
| --- |
| **PLANNING** |
| **Role** | **Responsibilities** | **Prevention** | **Incident Response** |
| Business Alignment Leaders (BALs) | * Organization security practices applied when business owners engage a new partner or expand partner roles
 | ✔ |   |
| * Capture incident information from Organization business owners and partners
 | ✔ | ✔ |
| * Provide access to application support resources when needed
 |   | ✔ |
| * Communicate incident-related information including status and instructions to business owners and DPO
 |   | ✔ |
| Application Development | * Assure secure coding practices in place and enforced
 | ✔ |   |
| * Aid in remediation efforts that apply to custom code
 |   | ✔ |
| * Support evidence collection as appropriate
 |   | ✔ |
| Information Security & Compliance | * Provide computer security guidance, assistance, and feedback to management in the form of “lessons learned” reports, technical recommendations, and risk assessments
 | ✔ |   |
| * Prevent the use of Organization systems in attacks against other systems which could cause Organization to incur legal liability
 | ✔ |   |
| * Minimize negative exposure potential
 | ✔ |   |
| Legal | * Provide guidance on ramification and regulatory impacts
 | ✔ | ✔ |
| * Assure protection of attorney-client privilege
 |   | ✔ |
| * Support interaction with engaged third parties
 |   | ✔ |
| Engaged Third Parties | * Law Enforcement
* Assist with internal and external investigations
* Correlate incidents with other similar events
 |   | ✔✔✔ |
| * IT Forensic Investigators
* Assist with detailed IT investigation
* Identify IT security gaps and remediation strategy
 |   | ✔✔✔ |

|  |
| --- |
| **LIAISON** |
| **Role** | **Responsibilities** | **Prevention** | **Incident Response** |
| Business Continuity | * Manage enterprise Business Continuity
 | ✔ |   |
| * Manage enterprise Incident Response Plan development and maintenance
 | ✔ |   |
| * Support cross-functional partner activation and coordination
 | ✔  | ✔ |
| * Help manage communication across the business
 |   | ✔ |
| Communications Team | * Support internal communications regarding an incident
 |   | ✔ |
| * Support external communication as warranted
 |   | ✔  |

# Incident Response Life Cycle

The Organization has implemented a standard/best practice incident response Lifecycle which is comprised of six phases that ensure a consistent and systematic approach.



Figure 3-0. Incident Response Life Cycle (Detection and Analysis)

## Preparation

Most incident response methodologies place a premium on preparation—not only establishing an incident response capability to ensure that the organization is prepared to respond to incidents, but also on preventing incidents by ensuring that systems, networks, and applications are sufficiently secured.

### Preventing Incidents

Keeping the number of incidents to a minimum is critical for protecting the organization's business processes and operations. Without adequate security controls, large volumes of incidents may occur, overwhelming the incident response team and potentially putting the business out of action.

* Patch Management: Many information security experts agree that a significant proportion of incidents involve the exploitation of a small number of system and application vulnerabilities. All application and operating system vendors regularly release patches to protect against vulnerabilities. They typically give an indication as to severity, meaning you can make risk-based decisions on when to test and schedule your patching activities. Critical vulnerabilities patched as soon as possible, low risk patched can be batched and installed quarterly for example.
* Host Security: All hosts should be adequately hardened. Apart from keeping each host patched, hosts should be configured to provide only the bare minimum services to the appropriate users and hosts—the least privilege principle. Insecure default settings should be changed (e.g., default passwords, unsecured shares).
* Network Security: The network perimeter should be configured to deny any activity not explicitly permitted. Only activities necessary for the organization's proper functioning should be permitted. This includes securing all points of connection, including modems, virtual private networks (VPNs), and dedicated connections to other organizations.
* Malicious Code Prevention: Throughout the organization, software to detect and prevent malicious code, such as viruses, worms, Trojan horses, and malicious mobile code, should be deployed.
* User Awareness and Training: Users should be made aware of network, system, and application policies and procedures governing appropriate network, system, and application use. Lessons learned from previous incidents should also be shared with users so they are aware of the potential consequences of their actions.
* 3rd party (vendor) risk management – all remote third-party vendor connections should be assessed and configured for least privilege, firewalled, and there should be a process in place where access has to be requested, approved, and connectivity is auto-terminated.

## Detection and Analysis

### Signs of an Incident

For many organizations, the most difficult part of the incident response process is accurately detecting and assessing potential incidents—determining whether an incident occurred and, if so, determining the nature, scope, and magnitude of the problem.

Incidents can occur in countless ways, so it is impractical to develop exhaustive procedures with step-by-step instructions for dealing with each one. The organization's best course of action is to prepare broadly for any type of incident and more specifically for common incident types.

### Sources of Precursors and Indications

Precursors and indicators are discovered through a variety of sources, the most common of which are computer security software alerts, logs, publicly available information, and people.

### Incident Analysis

* Profile Networks and Systems: Profiling is the process of determining the characteristics of expected activity to identify changes more easily.
* Understand Normal Behaviors: Members of the incident response team should study networks, systems, and applications in depth to gain a firm grasp on their normal behavior so that abnormal behavior can be identified more easily.
* Use Centralized Logging and Create a Log Retention Policy: Information about an incident can be stored in a variety of locations, including firewall, router, IDPS, and application logs.
* Perform Event Correlation: Numerous logs may contain evidence of an incident. Each log file may contain a variety of different types of information about the incident—for example, a firewall log may contain the source IP address that was used, whereas an application log may contain a username.
* Maintain Synchronization of All Host Clocks: Protocols such as the Network Time Protocol (NTP) are used to synchronize host clocks. This is critical for incident response because it complicates event correlation if the devices reporting events have inconsistent clock settings.
* Create and maintain an information knowledge base: The knowledge base should contain information that incident handlers require for quick reference during incident analysis.
* Conduct research using Internet search engines. Analysts can use comprehensive Internet search engines such as Google and Yahoo to uncover information about unusual activity, particularly scanning. For more information and instructions, please review *“Incident Response Tool Kit”* document.
* Collect Additional Data by Using Packet Sniffers: Occasionally, the indications lack sufficient detail to enable the handler to comprehend what is occurring.
* Consider Data Filtering: Many organizations simply lack the time necessary to review and analyze all indications. When confronted with large amounts of data, it is natural for humans to become overwhelmed and, in many cases, simply ignore the information.
* Develop a Diagnosis Matrix for Staff with Less Experience: A matrix of this type may be especially beneficial for help desk staff, system administrators, and others who conduct their own analysis of precursors and indications. Additionally, it may prove beneficial for newly hired intrusion detection analysts and incident response team members.
* Enlist the Assistance of Others: At times, the team may be unable to ascertain the full cause and nature of an incident. If the team is unable to contain and eradicate the incident due to a lack of information, it should consult with internal (e.g., information security staff) and external (e.g., US-CERT, other CIRTs, contractors with incident response expertise) resources for assistance with analysis, containment, and eradication. Organizations with Cyber Security Insurance may have the advantage to access Third Party Incident Response Teams provided and covered under their Cyber Security Insurance Policy.

### Incident Documentation

As soon as an incident response team suspects that an incident is about to occur or has already occurred, it is critical to immediately begin documenting all pertinent facts about the incident. While a Ticket System or logbook is an effective and simple medium for this, it is critical that information about the incident is recorded in a secure/encrypted system. Communication of incident information should also be encrypted.

### Incident Prioritization

Perhaps the most critical decision point in the incident handling process is prioritizing the incident's handling. Due to resource constraints, incidents should not be handled on a first-come, first-served basis. Rather than that, handling should be prioritized according to two criteria:

* Current and Potential Technical Effect of the Incident: Incident handlers should consider not only the incident's immediate negative technical impact (e.g., unauthorized user-level access to data), but also the incident's likely future negative technical impact if it is not contained immediately (e.g., root compromise).
* Criticality of the Affected Resources: Affected resources (e.g., firewalls, Web servers, Internet connectivity, user workstations, and applications) have varying degrees of importance to the organization.

## Containment, Eradication, and Recovery

### Choosing a Containment Strategy

Once an incident has been identified and analyzed, it is critical to contain it before it overwhelms resources or causes additional damage. Because most incidents require containment, it is critical to consider it early in the incident's handling process.

Another potential issue with containment is that certain attacks may inflict additional damage while being contained. For instance, a compromised host may run a malicious process that periodically pings another host. At that time there needs to be a conversation about whether to disable or quarantine the host immediately, or even keep it running to be able to collect more data.

### Evidence Gathering and Handling

While gathering evidence during an incident is primarily for the purpose of resolving the incident, it may also be required for legal proceedings. It is critical to clearly document how all evidence, including compromised systems, was preserved in such cases.

### Forensics for standard computers

Prior to copying files from the affected host, it is frequently desirable to capture volatile information that is not stored in a file system or image backup, such as active network connections, processes, login sessions, open files, network interface configurations, and the contents of memory.

### Forensics for mobile devices

Mobile devices, such as smart phones and PDAs, are increasingly being used for computing tasks such as email access, Web browsing, and document viewing. As a result, organizations now require the ability to perform forensics on mobile devices involved in incidents.

### Identifying the Attacker

Typically, system administrators and others involved in incident response want to identify the attacker. While this information is valuable, especially if the organization wishes to prosecute the attacker, incident handlers should remain focused on containment, eradication, and recovery.

* Validating the Attacker’s IP Address: Inexperienced incident handlers frequently focus exclusively on the attacker's IP address. The handler may attempt to verify that the address was not spoofed by performing pings, traceroutes, or other methods of connectivity verification.
* Scanning the Attacker’s System: Certain incident handlers go beyond pinging and tracing an attacking IP address; they may run port scanners, vulnerability scanners, and other tools to gather additional information about the attacker.
* Researching the Attacker Through Search Engines: In most attacks, incident handlers will have at least a few pieces of information about the attacker's possible identity, such as a source IP address, an email address, or an IRC nickname.
* Using Incident Databases: Numerous organizations aggregate and consolidate intrusion detection and firewall log data from multiple sources into incident databases. Numerous these databases allow users to conduct searches for records associated with a particular IP address. Incident handlers could use the databases to determine whether other organizations are reporting suspicious activity from the same source.
* Monitoring Possible Attacker Communication Channels: Another technique that some incident handlers use to identify an attacker is to monitor possible attacker communication channels.

### Eradication and Recovery

After an incident has been contained, eradication may be required to remove incident components, such as malicious code and compromised user accounts. Eradication is not necessary (e.g., ransomware encryption where a restore from backup would be more suitable) or performed during the recovery process for some incidents. Administrators perform recovery by restoring systems to normal operation and, if necessary, hardening them to prevent future incidents.

## Post-Incident Activity

### Lessons Learned

One of the most critical components of incident response is also one of the most frequently overlooked: learning and improvement. Each incident response team should evolve in response to evolving threats, advancements in technology, and lessons learned. Numerous organizations have discovered that convening a “lessons learned” meeting with all involved parties following a significant incident, and on a more frequent basis following minor incidents, is extremely beneficial in terms of improving security measures and the incident handling process itself.

### Using Collected Incident Data

Lessons learned activities should result in a collection of objective and subjective data for each incident. Over time, the incident data collected should prove useful in a variety of ways. The data, particularly the total number of hours spent and the associated cost, may be used to justify increased funding for the incident response team. An examination of incident characteristics may reveal systemic security vulnerabilities and threats, as well as shifts in incident trends.

* Number of Incidents Handled: Managing more incidents is not always preferable—for example, the number of incidents handled may decrease because of improved network and host security controls, not because of incident response team performance.
* Time Per Incident. For each incident, time can be measured in several ways:
	+ Total labor hours spent on the incident elapsed time from the start of the incident to its resolution
	+ Elapsed time for each stage of the incident handling process (e.g., containment, recovery)
	+ How long it took to notify management and, if necessary, appropriate external entities of the incident (e.g., vendors, third-party responders etc.).
* Objective Assessment of Each Incident: The response to a resolved incident can be analyzed to determine its effectiveness. The following are some examples of how to conduct an objective evaluation of an incident:
* Examining logs, forms, reports, and other incident documentation to ensure that established incident response policies and procedures are followed.
* Identifying which incident precursors and indicators were recorded to determine the effectiveness with which the incident was logged
* Determining whether the incident caused damage prior to its detection
* Determining whether the incident's actual cause was identified
* Calculating the incident's estimated monetary damage
* Identifying which preventative measures, if any, could have been taken to avoid the incident.
* Subjective Assessment of Each Incident: Members of the incident response team may be asked to evaluate their own performance, as well as that of their coworkers and the entire team. Another valuable source of information is the owner of an attacked resource—to ascertain whether the owner believes the incident was handled efficiently and with a satisfactory outcome.

### Evidence Retention

Organizations should establish a policy regarding the retention of evidence from an incident. Most organizations retain all evidence for months or even years after an incident occurs. The following factors should be considered when developing such a policy:

* Prosecution: If the attacker is likely to be prosecuted, evidence may need to be retained until all legal proceedings are concluded. This may take several years in some cases. Additionally, evidence that appears insignificant in the moment may become more significant in the future.
* Data Retention: Most organizations have data retention policies that specify the length of time that certain types of data may be retained. For instance, an organization may specify a maximum retention period of 180 days for email messages. In such cases, an exception or hold policy for IR data should be established.
* Cost: Original hardware (e.g., hard drives, compromised systems) that is retained as evidence, as well as hard drives and other devices used to store disk images, are inexpensive for most organizations.

## Incident Handling Forms, Documents and Standard Operating Procedures

The Incident Response Forms, Documents and Standard Operating Procedures detail the major steps that must be taken during the life cycle of an incident. The items address the detection and analysis of an incident and specific type of incident and include the collection of evidence and chain of custody.

The actual steps taken will vary depending on the type of incident and the nature of the individual incidents, the technology and software impacted, as well as size and priority. For instance, if the handler is certain what occurred based on an analysis of indications (e.g., a virus infection on only one asset) the entire incident may require only a couple steps for the entire life cycle vs. a regional incident impacting multiple organizations with ransomware and Denial of Service attack.

The Standard Operating Procedures and Incident Handling Checklists are to be reviewed and updated periodically – especially when processes or technologies change within the Organization.

# Notification and Communication

Required notification and communication both internally and with third parties (customers, vendors, law enforcement, etc.) based on legal, regulatory, and contractual requirements must take place in a timely manner.

* The Incident Commander must report the incident to senior leadership.
* The senior leadership must report any potential breaches and/or incidents involving customer data to the Incident Handling Team (IHT) promptly.
* The IHT is responsible for appropriate notification to:
	+ Personnel.
	+ Affected customers and/or partners (within 48 hours, based on SLA, based on legal or regularity compliance, whichever is shorter).
	+ Local, state, or federal law officials as required by applicable statutes and/or regulations.

Depending on the type and scope of breach, the following entities may need to be informed and incident details reported to:

Law Enforcement

* Law Enforcement’s priorities are eventual prosecution of offenders and not necessarily returning the Company to a functional state. Ensure Legal is consulted and provides direction before and while communicating with Law Enforcement.

Regulatory Authorities

* Organization is subject to various regulatory oversight, depending on the data impacted. If there is the potential that regulated data were breached, it may be necessary to notify governmental regulators.
* The IHT should contact regulators as soon as practical.

Customers

* All customers who are affected by the incident must be notified according to applicable contract language, service level agreements (SLAs), applicable statutes and/or regulations.
* Customer service and/or customer account managers will communicate with customers according to the message developed by the Incident Handling Team.

Public Media Handling

* All Information concerning an incident is to be considered confidential, and at no time should any information be discussed with anyone outside of the organization without approval of executive management and legal counsel.

The following documents with detailed instructions should be consulted to adhere to approved communication standard including lists of who to contact:

* *IR Customer & Media Communications*
* *Regulatory Notification Requirements*

# Regional and national Incidents

The majority of cybersecurity incidents will be internal and local – impacting the organization directly, the services they deliver, their clients, and possibly their Internet Service Providers (ISPs). Some incidents may – especially if not contained well or fast enough – become a regional or national event. In those cases, the organization will need to escalate and collaborate with regional and national agencies. Training and understanding in NIMS, Incident Complexity Guide and Incident Command Systems is key. For details, please see Appendix 1.

# Plan Testing and Review

The Organization Incident Response Plan and procedures must be tested at least annually. The Incident Commander will conduct training using a scheduled simulated incident to guide and test procedures. (Refer to document “IR Tabletop Exercise Examples” and NIST SP 800-61r2, Appendix A—Incident Handling Scenarios for test scenarios). The plan and procedures will be updated to reflect lessons learned and to incorporate any new industry developments.

CIRT members, the CIO/CTO, and members of the IHT must participate in test exercises at least annually.

Plan review should include:

* Review supporting documents and forms listed in Supporting Document List to ensure they are accurate and effective.
* Review Appendices and supporting documentation and forms to ensure they are accurate and effective.
* Review completed Incident Reporting Forms and corrective action plans for recommended plan and procedure updates.
* Compare recent changes to the organization’s infrastructure and management structure to documented plan and procedures.

# Incident Response Contact List

##

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Name** | **Role** | **E-mail** | **Work** | **Mobile** | **Alternate** |

|  |
| --- |
| **Incident Commander** |
| First & Last | Primary | name@Organization.com  | ###-###-#### x## | ###-###-#### | ###-###-#### x## |
| First & Last | Secondary | name@Organization.com  | ###-###-#### x## | ###-###-#### | ###-###-#### x## |
| First & Last | Tertiary | name@Organization.com  | ###-###-#### x## | ###-###-#### | ###-###-#### x## |

|  |
| --- |
| **Cybersecurity Incident Response Team (CIRT)** |
| First & Last | Primary | name@Organization.com  | ###-###-#### x## | ###-###-#### | ###-###-#### x## |
| First & Last | Secondary | name@Organization.com  | ###-###-#### x## | ###-###-#### | ###-###-#### x## |

|  |
| --- |
| **Incident Handling Team (IHT)** |
| First & Last | Primary | name@Organization.com  | ###-###-#### x## | ###-###-#### | ###-###-#### x## |
| First & Last | Secondary | name@Organization.com  | ###-###-#### x## | ###-###-#### | ###-###-#### x## |
| **Technical Assessment Team** |
| First & Last | Primary | name@Organization.com  | ###-###-#### x## | ###-###-#### | ###-###-#### x## |
| First & Last | Secondary | name@Organization.com  | ###-###-#### x## | ###-###-#### | ###-###-#### x## |

|  |
| --- |
| **Extended Team** |
| First & Last | Legal | name@Organization.com  | ###-###-#### x## | ###-###-#### | ###-###-#### x## |
| First & Last | Insurance | name@Organization.com  | ###-###-#### x## | ###-###-#### | ###-###-#### x## |

|  |
| --- |
| **Business Continuity** |
| First & Last | Primary | name@Organization.com  | ###-###-#### x## | ###-###-#### | ###-###-#### x## |
| First & Last | Secondary | name@Organization.com  | ###-###-#### x## | ###-###-#### | ###-###-#### x## |

|  |  |  |
| --- | --- | --- |
| **External Contacts** | **Main** | **Additional** |
| Organization | Name/Address  | ###-###-#### | ###-###-#### |
| FBI | Name/Address | ###-###-#### | ###-###-#### |
| Secret Service | Name/Address | ###-###-#### | ###-###-#### |
| Physical Security | Name/Address | ###-###-#### | ###-###-#### |
| NIMS | Name/Address | ###-###-#### | ###-###-#### |
| CERT | Name/Address | ###-###-#### | ###-###-#### |
| FEMA | Name/Address | ###-###-#### | ###-###-#### |
| Texas Department of Information Resources | https://dir.texas.gov/information-security/cybersecurity-incident-management-and-reporting | 877-DIR-CISO | [SPECTRIM](https://dir.archer.rsa.com/Default.aspx) |
| Vendor 2 | Name/Address | ###-###-#### | ###-###-#### |
| Cyber Insurance | Name/Address | ###-###-#### | ###-###-#### |
| ISP | Name/Address | ###-###-#### | ###-###-#### |
| Media | Name/Address | ###-###-#### | ###-###-#### |
|  | Name/Address | ###-###-#### | ###-###-#### |
|  | Name/Address | ###-###-#### | ###-###-#### |

# Appendix 1 - Reference Resources

**Texas Department of Information Resources**

Texas DIR provides a list of available Resources, Incident Reporting capabilities, Incident Response Guidance and Incident Reporting for State Agencies and Higher Education Incident Reporting

<https://dir.texas.gov/information-security/cybersecurity-incident-management-and-reporting>

**National Incident** **Management System (NIMS)**

On the NIMS website, users can find links to NIMS documents, guidelines, and operational tools, as well as training information, implementation guidance, updates, and contact information for the FEMA Regional NIMS Coordinators. https://www.fema.gov/emergency-managers/nims

**National Qualification System (NQS)**

The NIMS Guideline for the NQS describes the components of a qualification and certification system, defines a process for certifying the qualifications of incident personnel, describes how to establish and implement a peer review process, and introduces the process of credentialing personnel. NQS also provides Job Titles/Position Qualifications and Position Task Books (PTB) for a range of incident management, incident support, and emergency management positions. https://www.fema.gov/emergency-managers/nims/components#nqs

**Incident Command System (ICS) Resource Center**

The Emergency Management Institute’s ICS Resource Center provides information about and links to an extensive array of ICS training materials, job aids, position checklists, and forms. https://training.fema.gov/emiweb/is/icsresource/index.htm

**NIMS Incident Complexity Guide**

The Incident Complexity Guide promotes a common language and shared understanding of incident complexity across the whole community to determine the complexity or difficulty of managing a disaster, incident, event or exercise. https://www.fema.gov/sites/default/files/documents/nims-incident-complexity-guide.pdf

**NIMS Training Program**

The NIMS Training Program specifies National Integration Center (NIC) and stakeholder responsibilities and activities for developing, maintaining, and sustaining NIMS training. https://www.fema.gov/emergency-managers/nims/implementation-training#training

### NIMS Guideline for Resource Management Preparedness

This guideline supplements the Resource Management component of NIMS by providing additional details on resource management preparedness processes, best practices, authorities, and tools. <https://www.fema.gov/sites/default/files/documents/nims-guideline-resource-management-preparedness.pdf>

### NIMS Communications and Information Management Standards

This NIMS Guide provides a brief overview of five recommended standards that support NIMS implementation. https://www.fema.gov/sites/default/files/documents/fema\_nims-communications-information-standards\_2009.pdf

**NIMS Preparedness and Incident Management Standards**

This NIMS Guide provides a brief overview of two recommended standards that support NIMS implementation. https://www.fema.gov/sites/default/files/documents/fema\_nims-preparedness-incident-management-standards\_2008.pdf

**NIMS Guideline for Mutual Aid**

The NIMS Guideline for Mutual Aid outlines common practices for mutual aid agreements, compacts, and plans for use before and after an incident or planned event. Private and nonprofit sectors, faith-based organizations, and governments can use this guidance as a resource in developing or refining mutual aid agreements or plans. <https://www.fema.gov/emergency-managers/nims/components#mutual-aid>

**NIMS Training Courses**

The Emergency Management Institute (EMI), located at the National Emergency Training Center in Emmitsburg, MD, offers a broad range of NIMS-related training. <https://training.fema.gov/>

**ICS Forms Booklet**

The NIMS ICS Forms Booklet, FEMA 502-2, assists emergency response personnel in the use of ICS and corresponding documentation during incident operations.

https://www.fema.gov/incident-command-system-resources