**Name of Organization**

**Incident Response Framework**

December 2021

**Revision History**

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

Instructions

The (Name of Organization) Incident Response Framework is designated For Official Use Only (FOUO) and is the property of (Name of Organization). Only (Name of Organization) representatives may distribute this document 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. Introduction 5](#_Toc88583251)

[1.Importance of Cybersecurity 5](#_Toc88583252)

[II. Importance of Incident Response 6](#_Toc88583253)

[2.1 Development of an Incident Response Policy, Plan, and Procedure 6](#_Toc88583254)

[2.1.1 Incident Response Policy Components 6](#_Toc88583255)

[2.1.2 Incident Response Elements of the Plan 6](#_Toc88583256)

[2.1.3 Incident Response Elements of the Procedure 7](#_Toc88583257)

[2.1.4 Information Sharing with Third Parties 7](#_Toc88583258)

[2.2 Organization of the Incident Response Team 9](#_Toc88583259)

[2.2.1 Models Based on Collaboration 9](#_Toc88583260)

[2.3 Dependencies Within Organizations 9](#_Toc88583261)

[III. Incident Response Framework 11](#_Toc88583262)

[Phase I – Preparation 11](#_Toc88583263)

[Phase II – Detection and Analysis 11](#_Toc88583264)

[Phase III – Containment, Eradication and Recovery 11](#_Toc88583265)

[Phase VI – Post-Incident Activity 11](#_Toc88583266)

[IV. Coordination and Information Sharing 12](#_Toc88583267)

[4 Incident Coordination 12](#_Toc88583268)

[4.1 Sharing Agreements and Reporting Requirements 12](#_Toc88583269)

[4.2 Information Sharing Techniques 13](#_Toc88583270)

[4.2.1 Ad Hoc 13](#_Toc88583271)

[4.2.2 Partially Automated 13](#_Toc88583272)

[4.2.3 Security Considerations 14](#_Toc88583273)

[4.2.4 Technical Information 14](#_Toc88583274)

[V. References and Supporting Documentation 15](#_Toc88583275)

# Introduction

The Incident Response process has evolved into a critical component of Information Technology (IT) programs. Not only have security threats increased in number and diversity, but they have also become more disruptive. New types of security-related incidents (zero-day incidents) occur on a regular basis, as is evidenced through the frequent need to update applications and operating systems, be they Windows, MAC, or Linux. While preventative actions based on risk assessments can help reduce the number of incidents, not all incidents can be avoided.

This Framework is intended to assist both newly formed and already established Cybersecurity Incident Response Teams (CIRTs) in developing and improving Incident Response capabilities, and effectively managing incidents.

### 1.Importance of Cybersecurity

To minimize the risk and impact of security incidents, as a baseline, organizations should:

* Strive to reduce the frequency and risk of incidents by effectively securing their networks, systems, and applications through preventative activities - preventative measures are typically much less expensive and more effective than reactive measures. Thus, incident prevention is a critical component of an incident response capability.
* Document their policies on how they will interact with other organizations in the event of an incident.
* During the incident response process, the organization may be required to communicate with external parties, such as other incident response teams, law enforcement, the media, vendors, and external victims. The structure of these communications should be clearly laid out in advance so that roles and responsibilities, and appropriate messaging, are clear.
* Establish communication guidelines in advance to ensure that only the necessary information is shared with the appropriate parties.
* Plan for incident evidence gathering to happen in such a way that all evidence is admissible in a court of law.
* Familiarize themselves with National Incident Management Systems (NIMS) and plan their Incident Response plans to align with NIMS for easier communication, incident management, reporting and collaboration as needed.

It is further recommended that each organization strives to continuously improve their overall cybersecurity posture, with focus on maturity within security and incident response. For this purpose, a Nationwide Cybersecurity Review (NCSR) annual self-assessment was established to measure gaps and capabilities of state, local, tribal and territorial governments’ cybersecurity programs. It evaluates cybersecurity maturity across the nation while providing actionable feedback and metrics directly to individual respondents in State, Local, Tribal & Territorial (SLTT) governments.

The free and annual self-assessment is designed to identify gaps within an organization and develops a benchmark to gauge year-to-year progress, as well as anonymously measure results against peers. Additional resources and services are available for gap remediation and cybersecurity improvements. More information can be obtained here https://www.cisecurity.org/ms-isac/services/ncsr/

# Importance of Incident Response

Incident response has become necessary because of the frequent compromise of personal and business data by attacks, not just from external hackers but also internal bad actors. Virus, worm, Trojan horse, spyware, and other malicious code-related incidents have disrupted or damaged millions of systems and networks worldwide. Concerns about national security and the potential exposure of personally identifiable information (PII) are also increasing awareness of the potential consequences of computer-based attacks.

### 2.1 Development of an Incident Response Policy, Plan, and Procedure

This section discusses incident response policies, plans, and procedures, with a particular emphasis on interactions with external parties such as the media, law enforcement, and incident reporting and management organizations.

### 2.1.1 Incident Response Policy Components

The policy that governs incident response should be customized for each organization, as each organization is different. Regardless of whether an organization's incident response capability is in-house or outsourced, most policies contain the same major elements such as mission, scope, responsibilities, reviews and organization.

### 2.1.2 Incident Response Elements of the Plan

It is critical for organizations to have a structured, focused, and coordinated response capability to incidents. To implement such a capability effectively, an organization should have an incident response plan in place. The plan serves as a roadmap for the organization's implementation of its incident response capability. Once an organization develops a plan and obtains management approval for it, the plan should be implemented and then reviewed at least annually and/or after major organizational change to ensure any new gaps are recognized and dealt with, and the organization is adhering to the roadmap for capability maturation and meeting incident response goals.

### 2.1.3 Incident Response Elements of the Procedure

Procedures should be based on the policy and plan for incident response. Standard Operating Procedures (SOPs) are a description of the incident response team's specific technical processes, techniques, checklists, and forms. SOPs should be comprehensive and detailed to ensure that response operations reflect the organization's priorities.

### 2.1.4 Information Sharing with Third Parties

The organization may be required to communicate with external parties in the aftermath of an incident. Federal agencies are required to report incidents to the United States Computer Emergency Readiness Team at a minimum (US-CERT). Organizations may communicate with additional parties in a variety of ways, including reporting incidents to the CERT® Coordination Center (CERT®/CC), contacting law enforcement, and fielding inquiries.



Figure 2-1. Incident-Related Communications with Outside Parties

#### 2.1.4.1 The Media

Communicating with the media is a critical component of incident response. The incident response team should establish media communications procedures that are consistent with the organization's policies regarding appropriate media interaction and information disclosure. For discussing incidents with the media and other key stakeholders, organizations frequently find it beneficial to designate a single media Point of Contact (POC), typically the Incident Commander, and at least one backup contact.

#### 2.1.4.2 Law Enforcement

One reason for the failure of many security-related incidents to result in convictions is that organizations do not contact law enforcement in a timely manner. Numerous levels of law enforcement are available to investigate incidents, including federal investigatory agencies (e.g., the Federal Bureau of Investigation [FBI] and the United States Secret Service), district attorney offices, state law enforcement, and local law enforcement (e.g., county).

#### 2.1.4.3 Incident Reporting Organizations

Commercial and non-commercial organizations, institutions and agencies are in some cases required by their prevailing governance mandates, e.g., State Data Breach Laws or based on criticality and size of the incident, to report these to different organizations and/or notify customers/end users of the breach. This applies in particular to breaches that include credit card data and Personally Identifiable Information (PII). Texas also has their own requirements which are continuously changing and it is critical that each organization reviews these periodically.

In Texas, a breach is defined as “Breach of System Security, applicable to electronic Sensitive Personal Information (SPI) as defined by the Texas Identity Theft Enforcement and Protection Act, Business and Commerce Code Ch. 521, that compromises the security, confidentiality, or integrity of Sensitive Personal Information”. The Texas Department of Information Resources (DIR) (website <https://dir.texas.gov/information-security/cybersecurity-incident-management-and-reporting>) may provide organizations with incident support, and host a hotline for reporting incidents at (877) DIR-CISO.

Federal agencies and organization working in the critical infrastructure industry are required by Federal Information Security Modernization Act (FISMA) to report incidents to US-CERT, a government-wide incident response organization that assists Federal civilian agencies with incident response efforts. US-CERT does not intend to replace existing agency response teams; rather, it intends to supplement the efforts of Federal civilian agencies by serving as a focal point for incident response.

Additional details around regulatory requirements can be found in documents *“Regulatory Notification Requirements”* and *“IR Customer & Media Communications”.*

#### 2.1.4.4 Additional Third Parties

An organization may wish to consult with or engage several other groups regarding an incident for investigation, remediation and reporting purposes:

* The organization's Internet Service Provider (ISP): An organization may require assistance from its ISP in blocking or tracing the origin of a network-based DoS attack.
* Owners of Vulnerable IP Addresses: If attacks originate from an external organization's IP address space, incident handlers may wish to contact the organization's designated security contacts to alert them to the activity or to request evidence collection.
* Vendors of software: In some instances, incident handlers may wish to communicate suspicious activity to a software vendor.
* Additional Cybersecurity Incident Response Teams (CIRTs): Several organizations, including the Forum of Incident Response and Security Teams (FIRST) and the Government Forum of Incident Response and Security Teams (GFIRST), promote information sharing among incident response teams.
* Affected External Parties: External parties may be directly impacted by an incident; for instance, an external party may contact the organization and claim that one of the organization’s users is attacking it.

## 2.2 Organization of the Incident Response Team

Anyone who discovers or suspects that an organization-related incident has occurred should have access to report this to an incident response team. After that, depending on the priority and severity/size of the incident and available personnel, the incident will be handled by one or more team members of the Cybersecurity Incident Response Team (CIRT) and or Incident Handling Team (IHT) in accordance with the Standard Operating Procedures.

### 2.2.1 Models Based on Collaboration

Possible structures for an incident response team include the following:

* Central Incident Response Team: A single incident response team is accountable for incidents occurring throughout the organization. This model is effective for organizations of all sizes that have a limited geographic diversity of computing resources.
* Distributed Incident Response Teams: The organization is divided into multiple incident response teams, with each team responsible for incidents affecting a particular logical or physical segment of the organization. This model is effective in large organizations (one team per division, for example) and in organizations with significant computing resources located in remote locations (e.g., one team per geographic region, one team per major facility).
* Coordination Committee: A response team advises other teams without exercising authority over them; for example, a department-wide team may assist the response teams of individual organizations.
* Employees: The organization manages all incident response activities independently, with the assistance of contractors for limited technical and administrative support.
* Partially or fully outsourced: Outsourcing a portion or all of the organization's incident response work is a valid option as maintaining an in-house CIRT can be expensive. Buying IR services on a retainer basis gets you the specialists you need, prioritized above those organizations not on a retainer, on demand.

## 2.3 Dependencies Within Organizations

It is critical to identify other groups within the organization (see “*Incident Response Plan”)* that may be required to assist with incident handling to solicit their cooperation prior to their involvement being required. Each incident response team is dependent on the expertise, judgment, and capabilities of others, including the following:

* Management: Management is invariably central to incident response. Management establishes incident response policy, budget, and staffing in the most fundamental sense. Management also decides on actions to be taken that may impact business operations, have significant financial impact etc.
* The organization will need to decide who the Incident Commander will be, as that person may hail from Information Security, the Risk team, the IT team, or be in a senior officer of the organization in a business-related role.
* Information Security: Members of the information security team are frequently the first to recognize when an incident has occurred or is about to occur and may conduct the initial incident analysis. Additionally, information security personnel may be required during other stages of incident management, such as modifying network security controls (e.g., firewall rulesets) to contain an incident. This team may include the Data Privacy Officer.
* Telecommunications: Unauthorized access to telephone lines, such as dialing into unsecured modems – especially in legacy systems, is a cause of some incidents. The telecommunications staff is aware of the organization's current capabilities, as well as the points of contact and procedures for collaborating with telecommunications carriers.
* IT Operations: Not only do IT technical experts (e.g., system administrators, network administrators, and software developers) possess the necessary technical skills to assist during an incident, but they also typically possess the most in-depth understanding of the technology with which they interact daily.
* Legal Department: Legal counsel should review incident response plans, policies, and procedures to ensure they comply with applicable law and Federal guidance, including the right to privacy.
* Public Affairs and Media Relations: Depending on the nature and priority of an incident, the need to inform the media and, by extension, the public may exist (within the constraints imposed by security and law enforcement interests).
* Human Resources: When an employee appears to be the target of an incident or is suspected of causing one, the human resources department is frequently called upon to assist with disciplinary proceedings or employee counseling.
* Business Continuity Planning: Computer security incidents erode an organization's business resilience and serve as a barometer of its level of vulnerability and inherent risks.
* Physical Security and Facilities Management: Certain computer security incidents are the result of physical security breaches, are the result of coordinated logical and physical attacks or a local, regional, or national emergency.

# Incident Response Framework

(Name of Organization) recognizes that, despite reasonable and competent efforts to protect Information Resources, a breach or other loss of information is possible. The organization must make reasonable efforts and act competently to respond to a potential incident in a way that reduces the loss of information and potential harm to customers, partners, and the operation of organization itself.

Developing a well-defined incident response framework is critical to an effective incident response plan. The (Name of Organization) incident response framework is comprised of six phases that ensure a consistent and systematic approach.

### Phase I – Preparation

It is essential to establish a Cybersecurity Incident Response Team (CIRT), define appropriate lines of communication, articulate services necessary to support response activities, and procure the necessary tools.

### Phase II – Detection and Analysis

Identifying an event and conducting an assessment should be performed to confirm the existence of an incident. The assessment should include determining the scope, impact, and extent of the damage caused by the incident. In the event of possible legal action, digital evidence must be preserved, and forensic analysis must be conducted consistent with legislative and legal requirements.

### Phase III – Containment, Eradication and Recovery

Containment of the incident is necessary to minimize and isolate the damage caused. Steps must be taken to ensure that the scope of the incident does not spread to include other systems and Information Resources. Root cause analysis is required prior to moving beyond the Containment phase and may require expertise from outside parties.

Eradication requires removal of or addressing all components and symptoms of the incident. Further, validation must be performed to ensure the incident does not reoccur.

Recovery involves the steps required to restore data and systems to a healthy working state allowing business operations to be returned.

### Phase VI – Post-Incident Activity

The post-incident analysis phase includes Lessons Learned the on system(s) that were impacted by the incident and other potentially vulnerable systems. Lessons learned from the incident are communicated to executive management and action plans developed to improve future incident management practices and reduce risk exposure.

# Coordination and Information Sharing

The nature of contemporary threats and attacks makes it more important than ever for organizations to work together during incident response. Organizations should ensure that they effectively coordinate portions of their incident response activities with appropriate partners. The most important aspect of incident response coordination is information sharing, where different organizations share threat, attack, and vulnerability information with each other so that each organization’s knowledge benefits the other. Incident information sharing is frequently mutually beneficial because the same threats and attacks often affect multiple organizations simultaneously.

Coordinating and sharing information with partner organizations can strengthen the organization’s ability to effectively respond to IT incidents and collaboration with the trusted partner can enable an organization to respond to the incident more quickly and efficiently than an organization operating in isolation.

### 4 Incident Coordination

An organization may need to interact with several types of external organizations while conducting incident response activities. The incident response team should plan its coordination with those parties before incidents occur to ensure that all parties know their roles and that effective lines of communication are established. This coordination should be tested at least twice a year or when major changes in the organization occur, to make sure communication and coordination channels are functioning and all involved parties know their responsibilities and functions.

Organizations may find it challenging to build the relationships needed for coordination. Good places to start building a community include the industry sector that the organization belongs to and the geographic region where the organization operates. An organization’s incident response team can try to form relationships with other teams (at the team-to-team level) within its own industry sector and region, or join established bodies within the industry sector that already facilitate information sharing.

### 4.1 Sharing Agreements and Reporting Requirements

Organizations trying to share information with external organizations should consult with their legal department before initiating any coordination efforts. There may be contracts or other agreements that need to be put into place before discussions occur. An example is a nondisclosure agreement (NDA) to protect the confidentiality of the organization’s most sensitive information. Organizations should also consider any existing requirements for reporting incidents to a higher-level CIRT.

### 4.2 Information Sharing Techniques

Information sharing is a key element of enabling coordination across organizations. Even the smallest organizations need to be able to share incident information with peers and partners to deal with many incidents effectively. Organizations should perform such information sharing throughout the incident response life cycle and not wait until an incident has been fully resolved before sharing details of it with others. There are different types of incident information that organizations may or may not want to share with others. The means on how information is being shared is as important as the types.

### 4.2.1 Ad Hoc

Most incident information sharing has traditionally occurred through ad hoc methods, such as email, instant messaging clients, and phone. Ad hoc information sharing mechanisms normally rely on an individual employee’s connections with employees in incident response teams of partner organizations. These ad hoc techniques may be the most cost-effective way of sharing information with partner organizations, however, due to the informal nature of ad hoc information sharing, it is not possible to guarantee that the information sharing processes will always operate. For example, if a particularly well-connected employee resigns from an incident response team, that team may temporarily lose most of the information sharing channels it relies on to effectively coordinate with outside organizations. A more formalized method is recommended.

This information sharing method is also largely unstandardized in terms of what information is communicated, how that communication occurs and what information is being shared. Because of this, they tend to be more resource-intensive to process than the alternative, partially automated methods.

### 4.2.2 Partially Automated

Organizations should attempt to automate as much of the information sharing process as possible to make cross-organizational coordination efficient and cost effective. A fully automated information sharing process will not be possible, nor will it be desirable due to security and trust considerations.

When engineering automated information sharing solutions, organizations should first consider what types of information they will communicate with partners. The organization may want to construct a formal data dictionary enumerating all entities and relationships between entities that they will wish to share. Wherever possible, an organization should use existing data exchange standards for representing the information they need to share.

In addition to selecting the data exchange models for sharing incident information, an organization must also work with its partner organizations to agree on the technical transport mechanisms for enabling the information exchange to occur in an automated fashion. These transport mechanisms include, at a minimum, the transport protocol for exchanging the information. For example, encrypted information sharing over HTTPS or encrypted email.

### 4.2.3 Security Considerations

There are several security considerations that incident response teams should consider when planning their information sharing. One is being able to designate who can see which pieces of incident information (e.g., protection of sensitive information). It may also be necessary to perform data sanitization or scrubbing to remove sensitive pieces of data from the incident information without disturbing the information on precursors, indicators, and other technical information. The incident response team should also ensure that the necessary measures are taken to protect information shared with the team by other organizations.

There are also many legal issues to consider regarding data sharing that need to be considered – especially if data will be sent out of state or out of country.

### 4.2.4 Technical Information

There are many different types of technical indicators signifying the occurrence of an incident within an organization. These indicators originate from the variety of technical information associated with incidents, such as the hostnames and IP addresses of attacking hosts, samples of malware, precursors and indicators of similar incidents, and types of vulnerabilities exploited in an incident.

While organizations gain value from collecting their own internal indicators, they may gain additional value from analyzing indicators received from partner organizations and sharing internal indicators for external analysis and use. If the organization receives external indicator data pertaining to an incident they have not seen, they can use that indicator data to identify the incident as it begins to occur.

Organizations should share as much of this information as possible; however, there may be both security and liability reasons why an organization would not want to reveal the details of an exploited vulnerability. External indicators, such as the general characteristics of attacks and the identity of attacking hosts, are usually safe to share with others.

Organizations participating in incident information sharing should have staff skilled in taking technical indicator information from sharing communities and disseminating that information throughout the enterprise, preferably in an automated way. Organizations should also attempt to ensure that they only share an indicator for which they have a relatively high level of confidence that it signifies an actual incident.

Several government organizations such as FBI NDCA (National Defense Cyber Alliance) and Infragard are sharing information and threat data with their members. Organizations and their Security teams should become part of the information sharing groups.

# References and Supporting Documentation

Nationwide Cybersecurity Review (NCSR) - <https://www.cisecurity.org/ms-isac/services/ncsr/>

[National Incident Management System (NIMS)](https://www.fema.gov/sites/default/files/2020-07/fema_nims_doctrine-2017.pdf) - <https://www.fema.gov/emergency-managers/nims>

Texas Department of Information Resources - <https://dir.texas.gov/information-security/cybersecurity-incident-management-and-reporting>