

Contents

[Overview 3](#_Toc151123355)

[Definitions 3](#_Toc151123356)

[Implementation 3](#_Toc151123357)

[Purpose 4](#_Toc151123358)

[Scope 4](#_Toc151123359)

[Governing Laws, Regulations, and Guidelines 4](#_Toc151123360)

[Policy Statements 4](#_Toc151123361)

[Purpose 6](#_Toc151123362)

[Before a Cybersecurity Incident 6](#_Toc151123363)

[Adopt and Implement a Cybersecurity Risk Management Framework 7](#_Toc151123364)

[During a Cybersecurity Incident 11](#_Toc151123365)

[After a Cybersecurity Incident 12](#_Toc151123366)

[Incident Reporting Form 15](#_Toc151123367)

[Incident Data List 16](#_Toc151123368)

[Incident Command Staffing Template 17](#_Toc151123369)

[Incident Notification Form 18](#_Toc151123370)

[Incident Notification Contact List 19](#_Toc151123371)

[Incident Severity Ratings 20](#_Toc151123372)

[Default Press Response 21](#_Toc151123373)

[Incident Handling Checklist 23](#_Toc151123374)

[After-action Review (AAR) Form 24](#_Toc151123375)

**ACKNOWLEDGMENTS**

Cyber Florida gratefully acknowledges inputs from the University of South Florida's Incident Response Procedure and the City of Cocoa's cybersecurity policies. This template aligns with the National Institute of Standards and Technology's [*Computer Security Incident Handling Guide*](https://csrc.nist.gov/pubs/sp/800/61/r2/final).

**DISCLAIMER**

This guide is made available by The Florida Center for Cybersecurity for general educational purposes only and should not be used in lieu of obtaining competent legal advice from a licensed attorney and/or cybersecurity professional with the sufficient expertise necessary to address your organization's specific needs. Use of this guide does not create any special or fiduciary relationship between you and The Florida Center for Cybersecurity or the University of South Florida.

©2024 THE FLORIDA CENTER FOR CYBERSECURITY (CYBER FLORIDA) AT THE UNIVERSITY OF SOUTH FLORIDA

# Overview

This document is intended to help small organizations be better prepared to respond to and recover from cybersecurity incidents. Aligned to the standards of the National Institute of Standards and Technology (NIST), this guide can be used to help your organization establish an incident response policy.

# Definitions

**Cybersecurity incident:** An observable occurrence in an organization's technology infrastructure that can compromise business operations or information security.

**Social engineering:** Using deception to manipulate individuals into divulging information that may be used for fraudulent purposes.

**Phishing:** Sending emails or other messages that appear to be from reputable individuals or companies but are, in fact, from cybercriminals attempting to induce individuals to reveal personal information, such as passwords and credit card numbers.

**ICS:** An Incident Command System (ICS) is a standard response and recovery incident management tool nationally recognized and used by local government and private sector bodies. This template follows standard functions and roles.

# Implementation

An organization's IT group typically creates cybersecurity policies for its specific needs. After an initial test, policies are usually reviewed by experts for relevance, by the legal team for compliance, and, finally, approved by leadership. Once approved, the organization should communicate the policies to all affected employees, typically coordinating with Human Resources.

Once the organization adopts the policy, the directly responsible individuals identified in the plan section of this document are responsible for implementing the specific recommendations. For additional information, consider joining the [Florida Local Government Information Systems Association (FLGISA)](https://www.flgisa.org/) and other groups recommended by the [Florida Digital Service](https://digital.fl.gov/).

Incident Response Policy

# Purpose

The purpose of this policy is to ensure that ORGANIZATION NAME is capable of satisfactorily identifying and responding to cybersecurity incidents. Effective incident handling capability requires coordination among many organizational entities, including authorizing officials, mission owners, system owners, human resources offices, physical and personnel security offices, legal departments, operations personnel, procurement offices, the risk compliance manager, and, potentially, end users. Cybersecurity incident handling capabilities can help quickly identify threats and minimize consequences should a malicious actor exploit a vulnerability.

# Scope

This policy applies to all users and technology components of ORGANIZATION NAME 's critical cyber services. These include the following:

* End users in the organization
* IT administrators and cybersecurity incident responders
* Sensitive data stored in the organization or at service providers (e.g., social security numbers, credit card numbers)
* Devices that provide computing, storage, and networking capabilities (e.g., servers, desktops, mobile devices)
* Devices that provide other technology capabilities (e.g., firewalls, sensors, cameras, building automation systems)

# Governing Laws, Regulations, and Guidelines

|  |  |
| --- | --- |
| **Source** | **Regulation/ Section** |
| The Florida Senate | [CS/HB 7055](https://www.flsenate.gov/Session/Bill/2022/7055/BillText/er/PDF): Cybersecurity |
| NIST | [NIST SP 800-61, rev 2](https://csrc.nist.gov/pubs/sp/800/61/r2/final) |

# Policy Statements

## Incident Handling Capability

ORGANIZATION NAME will develop and implement incident-handling capabilities to cover all information system components that fall within the scope of this policy. The incident handling capability will include a defined plan and procedure to handle all stages of cybersecurity incidents: preparation, detection, analysis, response, containment, and recovery.

## Organizational Roles and Authorities

ORGANIZATION NAME will define the organizational cybersecurity structure, roles, responsibilities, and levels of authority to handle cybersecurity incidents.

## Incident Reporting Responsibility

ORGANIZATION NAME will track, document, and report incidents to appropriate authorities as required by governing laws and regulations.

## Prioritization and Severity Ratings of Incidents

ORGANIZATION NAME will define how it will assign a severity rating to cybersecurity incidents to critical cyber services and prioritize them for response and recovery.

## Performance Measures

ORGANIZATION NAME will develop objective measures for the impacts of cybersecurity incidents, including losses incurred and costs of response.

## Reporting Forms

ORGANIZATION NAME will develop forms to be used by its members to report cybersecurity incidents.

Incident Response Plan

# Purpose

The purpose of this incident response plan is to help ORGANIZATION NAME prevent, detect, and defend against cybersecurity threats and recover from incidents. The plan supports the organization's overall mission of minimizing service disruptions to its customers.

The plan has been approved by the senior leadership team. This plan will help ORGANIZATION NAME before, during, and after a confirmed or suspected cybersecurity incident. This plan clarifies the roles and responsibilities of individuals involved in handling cybersecurity incidents and the key activities involved in handling cybersecurity incidents.

The individual directly responsible for each of these activities is expected to ensure that the corresponding activity is completed satisfactorily, subject to the organization's budget constraints.

# Before a Cybersecurity Incident

## Develop a Cybersecurity Incident Reporting Procedure

**Directly responsible individual:** NAME AND CONTACT INFO

Create a cybersecurity [Incident Reporting Form](#_Incident_Reporting_Form) and a central point to report suspected cybersecurity incidents. The central reporting point can be an email address or phone number to which anyone in your organization can report a suspected cybersecurity incident. Typically, the CISO or designee is responsible for developing this reporting procedure.

## Develop Incident Response Performance Measures

**Directly responsible individual:** NAME AND CONTACT INFO

Develop the [Incident Data List](#_Incident_Data_List) for each cybersecurity incident. Actionable data regarding each incident can improve incident response over time. This objective and subjective data can indicate systemic security weaknesses and threats and changes in incident trends, ultimately improving the organization's security controls. The data can also measure the success of the incident response team and determine needed investments to improve the team's incident response capabilities. Decide what incident data to collect based on reporting requirements and the expected return from the data collection efforts. Typically, the CISO or designee is responsible for developing these performance measures.

# Adopt and Implement a Cybersecurity Risk Management Framework

**Directly responsible individual:** NAME AND CONTACT INFO

A Risk Management Framework (RMF) integrates security into the organization's business processes. The framework allows organizations to select the most effective security controls within the organization's budgetary and regulatory constraints. As a baseline, use the NIST risk management framework (<https://csrc.nist.gov/projects/risk-management/about-rmf>) as a starting point. The CISO or designee is typically responsible for selecting the risk management framework.

## Identify Critical Suppliers and External Partners

**Directly responsible individual:** NAME AND CONTACT INFO

Suppliers, their supply chains, and their products or services are potentially harmful to critical cyber infrastructure. For example, a compromised device at an air-conditioning service company can insert malicious code into the organization when the compromised device connects to the organization's network to repair a defective AC unit. The responsible individual should include important suppliers and external partners in incident response planning. The purchasing organization is typically responsible for identifying critical suppliers and external partners.

## Train Staff

**Directly responsible individual:** NAME AND CONTACT INFO

Update onboarding and recurring role-based training procedures to help all team members understand their role in maintaining the organization's security and reporting suspected cybersecurity incidents. Include critical suppliers and external partners in incident response and reporting training. Include examples of recent incidents relevant to your industry and organization to communicate the seriousness of cybersecurity incidents. Educate end users about social engineering and phishing. Share the cybersecurity incident reporting procedure with all team members and encourage them to report suspected cybersecurity incidents. Consider rewarding people who come forward to report suspicious events as part of your commitment to a culture of security. Be gracious when people report false alarms. Support team members likely to be involved in incident response (e.g., incident manager, technical manager, communications manager) in obtaining specialized training for these roles. The HR organization is typically responsible for incorporating incident reporting procedures into onboarding and training programs.

## Develop Incident Staffing and Stakeholder Notification Procedures

**Directly responsible individual:** NAME AND CONTACT INFO

Use the [Incident Command Staffing Template](#_Incident_Command_Staffing) to determine the roles everyone in the organization will play during a cybersecurity incident. Use the Incident Notification Contact List to identify people who must be notified during and after an incident. Identify alternates for key roles. Often, these reporting needs are not on anyone's mind during a cybersecurity incident. Typically, a member of the senior leadership is responsible for developing incident staffing and notification procedures because it involves experts from across the organization.

## Develop Incident Severity Rating Procedure

**Directly responsible individual:** NAME AND CONTACT INFO

Use the [Incident Severity Ratings table](#_Incident_Severity_Ratings) to assess the severity of the incident and prioritize your response. Not all incidents require the same intensity of response effort. An outage of the tax payment website during tax payment season is more severe than an outage of the same website outside tax season. Well-defined incident severity ratings help organizations allocate incident response resources appropriately. Typically, the CIO or designee is responsible for developing the incident severity ratings.

## Prepare Press Responses in Advance

**Directly responsible individual:** NAME AND CONTACT INFO

Develop a [default response](#_Default_press_response) to share with reporters when a cybersecurity incident happens. Anticipate what you will say if a reporter calls you, claiming that criminals are seeking ransom to unlock your systems. You will not likely have time to prepare this statement if such an incident happens. The general counsel or in-house lawyer is typically responsible for preparing this default press response.

## Enable Forensic Data Collection on Organization Devices

**Directly responsible individual:** NAME AND CONTACT INFO

Enabling logging for audit and forensics purposes on organization devices will simplify incident detection, containment, and review. Logs can quickly grow in size and occupy available disk storage space. Therefore, as part of enabling forensic data collection, determine how long the organization should retain audit logs on file. The selected risk management framework will include recommendations for log retention periods. Typically, the CISO or designee adds logging requirements to the organization's device configuration settings.

## Select an Outside Technical Resource/Firm if Resources Permit

**Directly responsible individual:** NAME AND CONTACT INFO

Investigating cybersecurity incidents will likely require high levels of technical expertise beyond your organization's abilities. Select outside experts who can help with technical investigations if necessary. The CIO, CISO, or designee typically selects the external technical resource.

## Conduct Attack Simulation Exercises

**Directly responsible individual:** NAME AND CONTACT INFO

Attack simulation exercises are role-playing games where a facilitator presents a scenario to the team and sees how everyone plays their roles. For example, the exercise might begin with a marketing executive receiving an email from a reporter about rumors of a hack. The facilitator will provide other updates during the game. These exercises are also called tabletop exercises (TTX). Conduct tabletop exercises at regular intervals. They are a fun and inexpensive way for your team to improve its cybersecurity incident-handling capabilities. Typically, the CIO, CISO, or designee organizes tests and simulations at periodic intervals.

## Learn Your Local Law Enforcement Agency's (LEA) Notification Procedures

**Directly responsible individual:** NAME AND CONTACT INFO

Investigation of cybersecurity incidents is typically the responsibility of your local law enforcement agencies. Identify your local police or FBI representatives who will conduct these investigations and learn about their incident notification contacts and procedures. Develop the necessary relationships before an incident happens. Typically, the CISO, general counsel, government relations officer, or designee is responsible for identifying and incorporating these notification procedures in the stakeholder notification procedures.

## Meet Your Department Of Homeland Security (DHS) CISA Regional Team

**Directly responsible individual:** NAME AND CONTACT INFO

CISA (Cybersecurity and Infrastructure Security Agency) is a federal agency that provides risk and risk mitigation advice to its partners. CISA, to include state-level and locally deployed Security Advisors (<https://www.cisa.gov/security-advisors>), can help you in various ways, and it is useful to know your regional CISA partner from <https://www.cisa.gov/about/regions>. Maintain regular contact with your local, regional, and state CISA teams. Typically, the CISO or designee is responsible for maintaining these relationships.

## Review This Plan with General Counsel or an Attorney

**Directly responsible individual:** NAME AND CONTACT INFO

Review your cybersecurity incident handling plan with an attorney. Your attorney may suggest modifications to this plan to meet your unique needs. Attorneys can also suggest how to engage with outside incident response vendors, law enforcement, and other stakeholders. Typically, the CIO, CISO, or designee is responsible for this review.

## Print and Distribute These Documents and Contact List

**Directly responsible individual:** NAME AND CONTACT INFO

During a cybersecurity incident, electronic resources such as document stores, laptops, and email could be inaccessible. To minimize disruption, print your cybersecurity incident response policy, plan, procedures, and contact lists and distribute these printouts to everyone you expect to play a role in an incident. Typically, the CISO or designee distributes these documents, with endorsement from senior leadership.

## Require Incident Information Sharing from Critical Suppliers and External Partners

**Directly responsible individual:** NAME AND CONTACT INFO

Require suppliers to track and document incidents, response decisions, and activities. Require prime contractors to push down this requirement to their relevant sub-contractors to help continuously improve the resilience of the organization's critical cyber infrastructure. Typically, the purchasing organization includes these information-sharing requirements in service agreements.

## Review Annually

**Directly responsible individual:** NAME AND CONTACT INFO

Test your incident handling capabilities at least once each year and review the results. It is a good idea to use external expertise to conduct these annual tests and reviews. The tests will determine the effectiveness of your current capabilities and identify potential weaknesses or deficiencies. Include suppliers and vendors central to your critical cyber services in these tests. Update your incident response plans at the conclusion of the test and review. The update should also incorporate the organization's experiences from the previous year. Distribute the updated plans and procedures to key stakeholders. Typically, the CIO or a member of the senior leadership is responsible for regular annual reviews.

# During a Cybersecurity Incident

## Assign a Unified Incident Command Manager by Following ICS Principles

**Directly responsible individual:** NAME AND CONTACT INFO

Assign a person to lead the organization's response to the incident. The incident command manager could be someone who does not perform technical duties. Rather, they manage communication flows, update stakeholders, and delegate tasks. They conduct an initial analysis of alerts and declare a cybersecurity incident if appropriate.

During a crisis, those responding to the incident often lose track of time and fail to inform other stakeholders in time, leaving them wondering about the state of the response and the anticipated timeline to restore normal operations. The IM monitors the clock to avoid that common problem. The command manager may also lead the retrospective meeting (outlined below) to gather lessons learned. Typically, the CISO or designee assigns the unified incident command manager.

## Assign an Information Technology/ Operational Technology (IT/OT) Technical Specialist

**Directly responsible individual:** NAME AND CONTACT INFO

Assign a person to lead the organization's technical response to the incident. The IT/ OT specialist is the subject matter expert to contain the disruption and restore service. Depending upon the severity of the incident, the IT/ OT specialist may perform the technical tasks themselves or bring in other internal and possibly external technical experts to assist with containing the damage and restoring service to normalcy. The IT/ OT specialist seeks the assistance of the incident manager for coordination with other stakeholders. The IT/ OT specialist should develop and maintain an incident handling checklist to streamline the technical response. The Procedures section includes an initial [Incident Handling Checklist](#_Incident_handling_checklist) from NIST 800.61. The CIO, CISO, or designee typically assigns the IT/ OT technical specialist.

## Assign a Public Information/Affairs Officer (PIO/PAO)

**Directly responsible individual:** NAME AND CONTACT INFO

Assign a person to handle the organization's communications during the incident. The communications manager interacts with the press, posts updates on social media, and interacts with external stakeholders such as local, state, and federal emergency management and cyber incident response agencies. Use the [Incident Notification Form](#_Incident_notification_form) to gather the required information. This form is based on the Florida Digital Service guidelines for compliance with Florida Statutes section 282.3185(5) for local government cybersecurity incident notification. All ransomware incidents and any level 3, 4, or 5 cybersecurity incidents should be reported as soon as possible but no later than 48 hours after discovering the cybersecurity incident and no later than 12 hours after discovering the ransomware incident. The CIO or senior leadership team member typically assigns a PIO/ PAO.

# After a Cybersecurity Incident

## Conduct an After-Action Review (AAR)

**Directly responsible individual:** NAME AND CONTACT INFO

Require the unified incident commander (assigned during the incident) to call a retrospective meeting. Invite the IT/ OT manager, PIO/ PAO, and all members of their teams involved in the incident response to the meeting. Use the [After-action Review Form](#_After-action_Review_(AAR)) to capture the required information. The AAR allows participants to collect lessons learned and share what worked well and what needs improvement for future incident responses.

At the retrospective meeting, the incident commander first reports the known incident timeline and asks for additions and edits. The [Incident Data List](#_Incident_Data_List) is populated. After the timeline is defined and performance measures collected, the team analyzes the incident response and suggests areas for improvement during future incidents.

The retrospective examines people, processes, and technologies. Security incidents are routinely due to a sequence of events and not just due to a single person or event. For effective after-action reviews, discussions based on non-attribution are more effective than organizational elements defending their function. All participants must feel free to openly discuss the incident in a safe and supportive environment, focusing on improvements. The CISO or designee typically ensures that the after-action review is scheduled and attended.

## Update Policies, Plans, and Procedures from Lessons Learned

**Directly responsible individual:** NAME AND CONTACT INFO

Require the incident manager to use the inputs from the retrospective meeting to identify updates to policies, plans, processes, and technologies based on the data gathered at the retrospective meeting. The incident manager implements updates that are within their area of responsibility. Send recommendations for updates that require intervention from other organization members or external partners to the CIO or their designee. Typically, the CISO or designee is responsible for implementing the updates and forwarding them to the organization's leadership for appropriate action.

## Communicate Findings from After-Action Review

**Directly responsible individual:** NAME AND CONTACT INFO

Communicate the findings from the after-action review and the updates implemented in response to the AAR. Share the findings with those affected by the incident and those involved in the response. Share information appropriately with critical suppliers and external partners. This transparency builds trust and promotes the responsible use of technology in the organization. Typically, the CISO or their designee is responsible for communicating the findings from the retrospective to the organization.

Incident Response Procedures

Incident response procedures are detailed checklists, forms, and other specific instructions to follow when responding to information security incidents.

When the incident is in progress, all internal and external stakeholders affected by the incident are under stress and not in a position to offer suggestions or information. It is, therefore, useful to develop these procedures before an incident happens and use the experience from the incident response to update these procedures.

The procedures listed below correspond to specific elements of the incident response plan. Hyperlinks connect each procedural element to the corresponding plan elements.

Update these procedures to fit your organization's needs as you gain experience with incident response.

# Incident Reporting Form

## Plan Element: Develop a Cybersecurity Incident Reporting Procedure

**Date and time of incident report:** Click or tap here to enter text.

Contact information for the incident reporter

**Name****:** Click or tap here to enter text.

**Organizational unit:** Click or tap here to enter text.

**Role:** Click or tap here to enter text.

**Email address:** Click or tap here to enter text.

**Phone number:** Click or tap here to enter text.

**Mailing address:** Click or tap here to enter text.

**INCIDENT DETAILS**

When was the incident detected/ discovered?

Click or tap here to enter text.

Physical location of the incident (e.g., office number, device name/ id)

Click or tap here to enter text.

Description of the incident (e.g., how it was detected, what occurred)

Click or tap here to enter text.

Current status of the incident (e.g., ongoing attack)

Click or tap here to enter text.

Response actions performed (e.g., shut off host, disconnected host from network)

Click or tap here to enter text.

General comments

Click or tap here to enter text.

# Incident Data List

## Plan Element: Develop Incident Response Performance Measures

|  |  |  |
| --- | --- | --- |
| **#** | **Data Element** | **Value** |
| 1 | Devices affected | Click or tap here to enter text. |
| 2 | Systems affected | Click or tap here to enter text. |
| 3 | Users affected | Click or tap here to enter text. |
| 4 | Outage or service degradation impact (person-hours) | Click or tap here to enter text. |
| 5 | Detection delay (hours) | Click or tap here to enter text. |
| 6 | Service loss | $Click or tap here to enter text. |
| 7 | Response effort cost to date | $Click or tap here to enter text. |

# Incident Command Staffing Template

## Plan Element: Develop Incident Staffing and Stakeholder Notification Procedures

|  |  |  |
| --- | --- | --- |
| **#** | **Task** | **Name and contact information** |
| 1 | Identify incident/ unified commander | Click or tap here to enter text. |
| 2 | Identify cybersecurity incident response team members | Technical: Click or tap here to enter text.  Operations: Click or tap here to enter text.  Communication, reporting: Click or tap here to enter text.  Logistics: Click or tap here to enter text.  Legal: Click or tap here to enter text.  HR: Click or tap here to enter text.  Liaison :Click or tap here to enter text. |

# Incident Notification Form

## Plan Element: Assign a Public Information/Affairs Officer (PIO/PAO)

1. Summary of the facts surrounding the cybersecurity incident or ransomware incident

Click or tap here to enter text.

1. Date and location of most recent data backup. Include information on whether the backup was affected by the incident and if the backup is stored on a cloud server.

Click or tap here to enter text.

1. Types of data compromised by the cybersecurity incident or ransomware incident

Click or tap here to enter text.

1. Estimated fiscal impact of the cybersecurity incident or ransomware incident

Click or tap here to enter text.

1. In the case of a ransomware incident, the details of the ransom demanded

Click or tap here to enter text.

1. A statement requesting or declining assistance from the Cybersecurity Operations Center, the Cybercrime Office of the Department of Law Enforcement, or the sheriff who has jurisdiction over the local government.

Click or tap here to enter text.

# Incident Notification Contact List

## Plan Element: Develop Incident Staffing and Stakeholder Notification Procedures

|  |  |  |
| --- | --- | --- |
| 1 | Establish reporting email address | EMAIL ADDRESS established as reporting email address for cybersecurity incidents |
| 2 | Communicate reporting address to organization | <Address included in trainings, periodic communications> |
| 3 | People to be notified about minor incidents (severity ratings 1 – 2) | CISO: CISO NAME AND CONTACT  Cybersecurity Insurance Carrier: Click or tap here to enter text.  FLDS: [CSOC@digital.fl.gov](mailto:CSOC@digital.fl.gov) or <http://IR.digital.fl.gov> or (850) 412-6074  FDLE: <https://www.fdle.state.fl.us/FCO/FDLE-Cybercrime-Office.aspx>  Local law enforcement: Click or tap here to enter text. |
| 4 | People to be notified about major incidents (severity ratings 3 – 5) | CISO: CISO NAME AND CONTACT  Cybersecurity Insurance Carrier: Click or tap here to enter text.  FLDS: [CSOC@digital.fl.gov](mailto:CSOC@digital.fl.gov) or <http://IR.digital.fl.gov> or (850) 412-6074  FDLE: <https://www.fdle.state.fl.us/FCO/FDLE-Cybercrime-Office.aspx>  SOC: SOC MANAGER NAME AND CONTACT.  Local law enforcement: Click or tap here to enter text. |
| 5 | People to be notified of final report of minor incidents (severity ratings 1 – 2) | CISO: CISO NAME AND CONTACT  Cybersecurity Insurance Carrier: Click or tap here to enter text.  FLDS: [CSOC@digital.fl.gov](mailto:CSOC@digital.fl.gov) or <http://IR.digital.fl.gov> or (850) 412-6074  FDLE: <https://www.fdle.state.fl.us/FCO/FDLE-Cybercrime-Office.aspx>  Local law enforcement: |
| 6 | People to be notified of final report of major incidents (severity ratings 3 – 5) | CISO: CISO NAME AND CONTACT  Cybersecurity Insurance Carrier: Click or tap here to enter text.  FLDS: [CSOC@digital.fl.gov](mailto:CSOC@digital.fl.gov) or <http://IR.digital.fl.gov> or (850) 412-6074  FDLE: <https://www.fdle.state.fl.us/FCO/FDLE-Cybercrime-Office.aspx>  SOC: SOC MANAGER NAME AND CONTACT  Local law enforcement: Click or tap here to enter text. |

# Incident Severity Ratings

## Plan Element: Develop Incident Severity Rating Procedure

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Area of impact | | | |
| **Impact level** | **Financial impact** | **User impact** | **Reputation impact** | **Regulator impact** |
| **5 (severe)** | Severe loss affecting the organization | Complete service failure across the organization exceeding one day | Organization becomes a meme for misconduct | One or more departments shut down or executives face personal penalty |
| **4 (high)** | Moderate loss affecting the organization | Complete service failure in one department exceeding one day | Long-term national media coverage of incident | Regulator issues notice to comply under penalty of fines |
| **3 (medium)** | Financial loss requiring budget adjustment across multiple departments | Partial local service disruption exceeding one day | Short-term national media coverage of incident | Regulator issues an enforceable undertaking |
| **2 (low)** | Financial loss requiring budget adjustment within a department | Partial local service disruption of less than one day | Local media coverage of incident | Regulator requires regular updates until resolution |
| **1 (insignificant)** | Financial loss within annual budget | Insignificant service disruption | No awareness of incident outside organization | No regulator interest |

# Default Press Response

## Plan Element: Prepare Press Responses in Advance

An initial draft is provided below:

FOR IMMEDIATE RELEASE

ORGANIZATION NAME

DATE

ORGANIZATION NAME Reports Cybersecurity Incident: Immediate Action Taken to Protect Data and Systems

CITY, DATE— ORGANIZATION NAME –today reported that it has experienced a cybersecurity incident that may have impacted the security of certain data and systems. ORGANIZATION NAME has taken immediate action to investigate and mitigate the incident, working closely with cybersecurity experts to address the situation.

**Nature of Incident:** The incident involves ENTER BRIEF DESCRIPTION OF THE INCIDENT, i.e. MALWARE, UNAUTHORIZED ACCESS

**Scope of Impact:** While the investigation is ongoing, ORGANIZATION NAME believes that PROVIDE AN INITIAL ASSESSMENT OF THE IMPACT, SYSTEMS AFFECTED, DATA COMPROMISED.

**Immediate Actions Taken:**

ISOLATION AND CONTAINMENT OF AFFECTED SYSTEMS.

ENGAGEMENT OF LEADING CYBERSECURITY EXPERTS TO INVESTIGATE.

NOTIFICATION OF APPROPRIATE LAW ENFORCEMENT AGENCIES.

**Data Protection Measures:**

SPECIFY ANY MEASURES TAKEN OR RECOMMENDED FOR AFFECTED INDIVIDUALS, SUCH AS PASSWORD RESETS, CREDIT MONITORING, ETC.

**Ongoing Investigation:**

BRIEF UPDATE ON THE CURRENT STATUS OF THE INVESTIGATION

REASSURANCE THAT THE COMPANY IS WORKING DILIGENTLY TO RESOLVE THE ISSUE.

ORGANIZATION NAMEdeeply regrets any inconvenience this incident may have caused and is committed to keeping its customers, partners, and the public informed as new information becomes available. ORGANIZATION NAME remains dedicated to the highest cybersecurity standards and will take all necessary steps to prevent future incidents.

**About** ORGANIZATION NAME

ORGANIZATION OVERVIEW AND MISSION

**Forward-Looking Statements**

This press release may contain forward-looking statements that involve risks and uncertainties. Actual results may differ materially from the results predicted. ORGANIZATION NAME disclaims any obligation to update or revise publicly any forward-looking statements, whether as a result of new information, future events, or otherwise.

###

For more information, please contact: NAME AND CONTACT INFO.

For media inquiries: NAME AND CONTACT INFO.

For customer inquiries: NAME AND CONTACT INFO.

# Incident Handling Checklist

## Plan Element: Assign an Information Technology/ Operational Technology (IT/OT) Technical Specialist

|  |  |  |  |
| --- | --- | --- | --- |
| **Stage** | **#** | **Action** | **Completed?** |
| Detection and analysis | 1 | Determine whether an incident has occurred |  |
| 1.1 | Analyze the precursors and indicators |  |
| 1.2 | Look for correlating information |  |
| 1.3 | Perform research (e.g., search engines, knowledge base) |  |
| 2 | Begin documenting the investigation and gathering evidence |  |
| 3 | Prioritize handling the incident based on relevant factors (e.g., functional impact, information impact, recoverability effort,) |  |
| 4 | Report the incident to the appropriate internal personnel and external organizations |  |
| 4.1 | Engage internal and external teams and stakeholders |  |
| Containment, eradication and recovery | 5 | Acquire, preserve, secure, and document evidence immediately before, during, and for a period after the incident |  |
| 6 | Contain the incident |  |
| 7 | Eradicate the incident |  |
| 7.1 | Remove malware, inappropriate materials, and other components |  |
| 7.2 | Identify and mitigate all vulnerabilities that were exploited |  |
| 7.3 | If more affected hosts are discovered (e.g., new malware infections), repeat the Detection and Analysis steps (1.1, 1.2) to identify all other affected hosts, then contain (6) and eradicate (7) the incident for them |  |
| 8 | Recover from the incident |  |
| 8.1 | Return affected systems to an operationally ready state |  |
| 8.2 | Confirm that the affected systems are functioning normally |  |
| 8.3 | If necessary, implement additional monitoring to look for future related activity Post-Incident Activity |  |
| Post-incident | 9 | Conduct retrospective meeting |  |
| 10 | Prepare and distribute follow-up report |  |

# After-action Review (AAR) Form[[1]](#footnote-2)

## Plan Element: Conduct an After-Action Review

Incident summary (include what happened, why, severity, duration of impact)

### Click or tap here to enter text.

Impact (services affected, internal and external users affected, how to minimize impact in future)

Click or tap here to enter text.

Timeline

Click or tap here to enter text.

Detection (how discovered, how to minimize detection delay in future)

Click or tap here to enter text.

Containment response (who responded, what did they do, how to contain better in future)

Click or tap here to enter text.

Recovery response (how was service restored, incident closed, how to speed recovery in future)

Click or tap here to enter text.

Root cause identification

Click or tap here to enter text.

Final root cause

Click or tap here to enter text.

Lessons learned (what went well, what could have been improved)

Click or tap here to enter text.

How will the evidence be stored and used in subsequent investigations

Click or tap here to enter text.

References

CISA, Incident Response Plan (IRP) Basics, <https://www.cisa.gov/sites/default/files/publications/Incident-Response-Plan-Basics_508c.pdf>

CISA, National cyber incident scoring system, <https://www.cisa.gov/sites/default/files/2023-01/cisa_national_cyber_incident_scoring_system_s508c.pdf>

City of Cocoa, Information Technology and Cybersecurity Policies

University of South Florida, Incident Response Procedures

MS-ISAC, #StopRansomware Guide, <https://www.cisa.gov/resources-tools/resources/stopransomware-guide>, https://www.cisa.gov/resources-tools/resources/stopransomware-guide

NIST SP 800-161r1, Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations

NIST 800-171, Assessing Security Requirements for Controlled Unclassified Information, <https://csrc.nist.gov/pubs/sp/800/171/a/final>

NIST 800-61, Computer Security Incident Handling Guide, [csrc.nist.gov/pubs/sp/800/61/final](file:///C:\Users\bjlangley\AppData\Local\Microsoft\Windows\INetCache\Content.Outlook\PJ2CUWMJ\csrc.nist.gov\pubs\sp\800\61\final)

Florida Digital Service, Local Government Cybersecurity Resource Packet, 2023

1. This template is based on Atlassian’s template, available at <https://www.atlassian.com/incident-management/postmortem/templates> (accessed Oct 2023) [↑](#footnote-ref-2)