MILWAUKEE

# 200654 - Department Incident Response Plan - Departmental Template

Incident Response Plan (IRP)

# 1 CONTENTS

# 2 OVERVIEW

This document was created to be used as a guide in the event of a Cyber Incident or Information Security Incident. The objective is to provide a well-defined, organized approach for handling of any potential threat to IT/OT systems and data.

The Department of Homeland Security (DHS) defines a cyber incident as "An event occurring on or conducted through a computer network that actually or imminently jeopardizes the confidentiality, integrity, or availability of computers, information or communications systems or networks, physical or virtual infrastructure controlled by computers or information systems, or information resident thereon." This will be expanded to include any computer event with a negative consequence that could cause any of the following but not limited to system crashes, packet flooding, unauthorized use of system privileges, unauthorized access to data, or the execution of malicious software. Any act that threatens the confidentiality, integrity and availability of the City of Milwaukee's Information Systems and data will be considered an incident.

# 3 PURPOSE

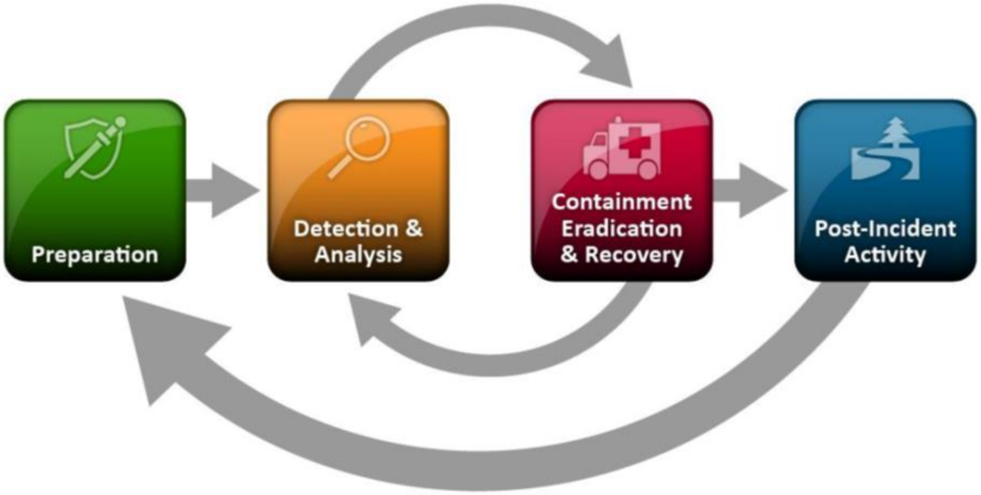
Attacks frequently compromise personal and business data, and it is critical to respond quickly and effectively when security breaches occur. One of the benefits of having an incident response capability is that it supports responding to incidents systematically (i.e., following a consistent incident handling methodology) so that the appropriate actions are taken. Incident response helps personnel to minimize loss or theft of information and disruption of services caused by incidents. Another benefit of incident response is the ability to use information gained during incident handling to better prepare for handling future incidents and to provide stronger protection for systems and data. An incident response capability also helps with dealing properly with legal issues that may arise during incidents.

# 4 SCOPE

The Incident Response Plan applies to all technical owners within the City of Milwaukee. This plan includes initial actions and procedures to respond to events that could affect critical business activities for The City of Milwaukee in the occurrence of a Cyber Security Incident.

It is intended that this plan should be used in conjunction with corresponding Continuity of Operations (COOP), Contingency (CP), and Disaster Recovery (DR) plans. Templates have been provided at the end of this document to assist with customizing the IRP for use within City departments. Departmental plan structure should be consistent with this citywide plan but the use of these templates should be considered optional.

# 5 METHODOLOGY



This Incident Response Plan covers the following activities reflecting the current design and "Best Practices" for incident response by the National Institute of Standards and Technology Publications (NIST) Special Publication 800-61 Revision 2 and Executive Order on America's Cybersecurity Workforce and follows the guidelines as set forth in the Incident Response Policy.

# 6 PREPARATION – IDENTIFY AND PROTECT

## 6.1 INCIDENT RESPONSE ROLES/RESPONSIBILITIES

The Incident Response Team is authorized to take appropriate steps deemed necessary to contain, mitigate or resolve a computer security incident. The team is responsible for investigating suspected intrusion attempts or other security incidents in a timely, cost-effective manner and report findings to management and the appropriate authorities as necessary. The Incident Response Team will include primary ITMD administration contacts and Critical Team members determined by the type and severity of the incident.

### 6.1.1 Incident Director

A senior executive is usually designated as the sponsor for the incident management program and serves as the immediate escalation point for critical decisions.

### 6.1.2 Incident Manager

An Incident Manager (or managers, depending on the duration of the incident) usually directs incident management activities, informs executive management, and escalates the incident as necessary. The Incident Manager directs incident status meetings and reporting.

### 6.1.3 Incident Response Technical Team Members

Team Members are IT employees, other City staff, or outside contractors responsible for the collection and analysis of evidence, determination of root cause, and implementation of system and service recovery.

Example duties include the following:

- Conduct computer system and telecommunications damage assessment.
- Activate alternate operating locations (for system recovery).
- Recover computer systems and network environment(s).
- Ensure all system security devices and procedures are in place.

### 6.1.4 Communications

A central component of maintaining trust is providing the public with timely and accurate information. Equally important is dispelling inaccurate information as quickly as possible. Maintaining trust is most effectively accomplished when City officials speak with one coordinated voice.

Responsibilities include establishing and executing a communications plan with procedures and protocols for both internal and external communication as well as the supporting equipment and infrastructure.

Example duties include the following:

- Coordinate all media communications.
- Review and approve all statements regarding the incident.
- Develop both internal and external communications.
- Coordinate recovery-related advertising with external vendors.

### 6.1.5 Human Resources

Human Resources is usually responsible for the well-being of employees. This includes providing information about medical coverage, pandemic or personnel loss planning, succession planning, family and casualty support, and sometimes-personal safety.

Example duties include the following:

- Account for all personnel.
- Ensure the health and safety of employees.
- Coordinate employee communications with Communications.
- Coordinate additional or temporary staffing for recovery effort.

### 6.1.6 Legal

The senior attorney and, often, risk managers advise the response team on matters involving liability, compliance, records management, and regulatory requirements.

Example duties include the following:

- Manage all required regulatory notifications.
- Provide legal counsel for response and recovery operations.

- Review and approve new contracts acquired because of the event, before the contracts are implemented.

### 6.1.7 Facilities

Facilities is usually responsible for safety, evacuation, hazards, and fire response.

Example duties include the following:

- Conduct a detailed damage assessment.
- Ensure that response activities to address fire, spills, and/or medical emergencies are performed in accordance with policies and guidelines.
- Enlist the assistance of vendors and agencies in support activities as appropriate.
- Conduct salvage and restoration activities.

### 6.1.8 Physical Security

Security typically refers to physical security and is the primary contact for law enforcement and emergency medical response.

Example duties include the following:

- Coordinate on-site security for affected facilities and all alternate operating locations.
- Control access to affected facilities.
- Monitor equipment and records being removed from facilities.

### 6.1.9 Finance

Finance is typically responsible for emergency funding for procurement, purchasing, travel, lodging, and other response requirements.

Example duties include the following:

- Ensure funds are available for recovery.
- Set up a recovery cost center.
- Estimate the impact of the incident on the company’s financial statement.
- Manage all incident-related purchasing.

## 6.2 Activation of the Incident Response Team

Cyber-related incidents vary in size and severity, which makes it important to have a process to calibrate the appropriate steps to the significance of what is taking place.

The National Institute of Standards and Technology (NIST) Special Publication NIST 800-61, Computer Security Incident Handling Guide, provides advisement on prioritizing the handling of security incidents. These incidents may be applicable to computer systems as well as paper or other media.

All Incidents will be classified based on an assessment of enterprise risk, considering both the likelihood of impact and scope and severity of impact following the 5-tier method.

| Incident Level | Definition | Actions |
|---|---|---|
| **Level 5**<br>**Emergency** | Poses an imminent threat to the provision of wide-scale critical | Meet with Incident Response Team to access scope and prioritization. |

|  |  |  |
|---|---|---|
| **(Black)** | infrastructure services, national government stability, or the lives of U.S. persons. | Communicate with Executive Management.<br>Request Assistance from STAC, MS-ISAC or other Government Agencies |
| **Level 4**<br>**Severe**<br>**(Red)** | Likely to result in a significant impact to public health or safety, national security, economic security, foreign relations, or civil liberties | Meet with Incident Response Team to access scope and prioritization.<br>Communicate with Executive Management.<br>Request Assistance from STAC, MS-ISAC or other Government Agencies |
| **Level 3**<br>**High**<br>**(Orange)** | Likely to result in a demonstrable impact to public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence | Meet with Incident Response Team to access scope and prioritization.<br>Communicate with Executive Management.<br>Request Assistance from STAC, MS-ISAC or other Government Agencies |
| **Level 2**<br>**Medium**<br>**(Yellow)** | May impact public health or safety, national security, economic security, , economic security, foreign relations, civil liberties, or public confidence | Follow Normal Procedures for Incident Remediation<br>Complete Incident Intake Form.<br>Notify departmental IT security personnel.<br>May request assistance from STAC, MS-ISAC or other Government Agencies. |
| **Level 1**<br>**Low**<br>**(Green)** | Unlikely to impact public health or safety, national security, economic security, , economic security, foreign relations, civil liberties, or public confidence | Follow Normal Procedures for Incident Remediation<br>Complete Incident Intake Form.<br>Notify departmental IT security personnel. |
| **Level 0**<br>**Baseline**<br>**(White)** | Unsubstantiated or inconsequential event. The bulk of incidents will likely fall into the baseline priority level with many of them being routine data losses or incidents that may be immediately resolved. | Follow Normal Procedures for Incident Remediation<br>Complete Incident Intake Form.<br>Notify departmental IT security personnel. |

In the event that an Emergency, Severe, or High-level incident is declared, the Incident Response Team should be activated. In a medium-intensity incident, the Incident Director will need to make a judgment call about whether to activate the Incident Response Team, but if the situation is likely to become public and raise questions about trust, the Incident Director should err on the side of activation. You can always deactivate if the intensity declines. Once activated, the Incident Director will decide which level applies, based on an initial assessment. Once the Incident Response Team is activated, team members will be notified of the activation by cell.

## 6.3 Contact Information

Contact information lists will be updated regularly, will be secured to protect confidential information and available for use by members of the crisis communications team. Incident Response Team Contacts

### 6.3.1 Declaration of an Incident

In the case of High and Critical incidents, the Incident Response Team should be activated. In a medium-intensity incident, the Incident Director will need to make a judgment call about whether to activate the Incident Response Team, but if the situation is likely to become public and raise questions about trust, the decision should err on the side of activation. You can always deactivate if the intensity declines. Once activated, the Incident Director will decide which level applies, based on an initial assessment. Once the Incident Response Team is activated, team members will be notified of the activation by cell.

### 6.3.2 Incident Response Team Members

Contact information lists will be updated regularly, will be secured to protect confidential information and available for use by members of the crisis communications team.

| **Team Management** | | | |
|---|---|---|---|
| Role | Name | Desk | Mobile |
| IR Director | | | |
| Operations Manager | | | |
| Technology Manager | | | |
| Technology Manager | | | |
| **Technical Team** | | | |
| Responsibilities | Name | Desk | Mobile |
| Technical Team Member | | | |
| Technical Team Member | | | |
| Technical Team Member | | | |
| **Support Roles** | | | |
| Communications | | | |
| Human Resources | | | |
| Legal | | | |
| Facilities | Ahmed Abubaker | x5591 | (414)708-2720 |
| Physical Security | | | |
| Finance | | | |

### 6.3.3 IMSD Service Desk

IMSDHelp@milwaukeecountywi.gov<br>
414-278-7888

## Incident Notifications

Local Government should report cybercrimes that may:

- Result in a significant loss of data, system availability, or control of systems

- Impact a large number of victims
- Indicate unauthorized access to, or malicious software present on, critical information technology systems
- Affect critical infrastructure or core government functions
- Impact national security, economic security, or public health and safety

## 6.4 Crisis Communication

A central component of maintaining trust is providing the public with timely and accurate information. Equally important is dispelling inaccurate information as quickly as possible, especially in today's perpetual cycle of traditional and social media coverage. Maintaining trust is most effectively accomplished when City officials speak with one coordinated voice. While every situation is unique, this plan provides a foundation on which we can build an appropriate response.

### 6.4.1 Communication Roles

Communication roles may vary based on the technology of the incident or event.

- Incident Director
  - Activates Incident Response Team
  - Responsible for communicating to Executive staff. Decides escalation path.
  - Responsible for internal and external communications. Determines which channels should be used, when they should be used, and what level of detail is appropriate to communicate out. Defines and distributes communication templates.
- Technology Managers
  - Delivers Technical Briefing
  - Directs the incident response process.
  - Communicates incident status and escalations to the Incident Director
- Operations Manager – Handles customer concerns. Communicates incident status or escalations to the Incident Director

### 6.4.2 Holding Statement

The Incident Director will be the primary spokesperson. An initial communication statement, a holding statement will be shared with ITMD staff and the Unified Communications Center. Below is one example of a baseline communication.

> "The City of Milwaukee is currently experiencing a disruption to our information systems. We are working to determine the extent of the situation. We will provide information updates as we acquire them."

### 6.4.3 Internal Communications

Security incidents can be high-pressure, high-stress situations. Everyone is anxious to understand the details around the investigation, scope, mitigation and more. Ensuring that stakeholders across security, infrastructure, engineering and operations teams are informed and engaged is one of the chief responsibilities of the Security Incident Manager. The Security Incident Manager should focus on providing high-level status updates without delving too deeply into the technical details of the incident, including:

- Current Risk
- Users Affected (some, many, all?)
- Timeline of events
- Mitigation steps that have been taken
- Current status of the incident
- Next steps

### 6.4.4 Communications with Outside Parties

ISP - An organization may need assistance from its ISP in blocking a major network-based attack or tracing its origin.

Owners of Attacking Addresses - If attacks are originating from an external organization's IP address space, incident handlers may want to talk to the designated security contacts for the organization to alert them to the activity or to ask them to collect evidence. It is highly recommended to coordinate such communications with US-CERT or an ISAC.

Software Vendors - Incident handlers may want to speak to a software vendor about suspicious activity. This contact could include questions regarding the significance of certain log entries or known false positives for certain intrusion detection signatures, where minimal information regarding the incident may need to be revealed. More information may need to be provided in some cases—for example, if a server appears to have been compromised through an unknown software vulnerability. Software vendors may also provide information on known threats (e.g., new attacks) to help organizations understand the current threat environment.

Other Incident Response Teams - An organization may experience an incident that is similar to ones handled by other teams; proactively sharing information can facilitate more effective and efficient incident handling (e.g., providing advance warning, increasing preparedness, developing situational awareness).

Affected External Parties - An incident may affect external parties directly—for example, an outside organization may contact the organization and claim that one of the organization's users is attacking it. Another way in which external parties may be affected is if an attacker gains access to sensitive information regarding them, such as credit card information.

### 6.4.5 Incident Response Organizations

Cyber Incidents should be reported to the Southeastern WI Threat Analysis Center (STAC). STAC will coordinate with other agencies to help address incident response. Other agency contact information is included for reference.

<u>Southeastern WI Threat Analysis Center (STAC)</u>
The STAC is one of 79 fusion centers recognized by the United States Department of Homeland Security; STAC is collocated with the Milwaukee Police Department's Intelligence Fusion Center. STAC provides a platform for collaboration among multiple federal, state, local and tribal agencies and disciplines to exchange information and intelligence, with the goal to improve the ability to detect, prevent, deter, and respond to crime and terrorism by analyzing data from various sources

Phone: 877-949-2824 (877-WIWATCH)

Email: STAC@Milwaukee.gov

Wisconsin Statewide Intelligence Center (WSIC)

The Wisconsin Statewide Intelligence Center (WSIC), operated by the Wisconsin Department of Justice-Division of Criminal Investigation, is one of two fusion centers in Wisconsin. WSIC serves as the primary focal point for threat information sharing among federal, state, local and tribal law enforcement, emergency management, fire service, public health, corrections, military and private sector partners for the state

Phone: 608-242-5393 / 888-324-9742 (888-DCI-WSIC)

FBI Field Office

Location:
3600 S. Lake Drive
St. Francis, WI 53235
Phone:
414-276-4684
https://www.fbi.gov/contact-us/field-offices/milwaukee

Department of Homeland Security - US-CERT

Email: soc@us-cert.gov
Online: https://www.us-cert.gov/forms/report
Phone: 888-282-0870

Federal Bureau of Investigation - IC3

Online: https://complaint.ic3.gov/default.aspx

# 7 DETECTION & ANALYSIS

## 7.1 INCIDENT RESPONSE TOOLKIT

- **Log Files**
  - Operating system, service and application logs
  - Network device logs
- **Configuration Files**
  - Firewall, Router, Switch
- **Offline copy of Asset Inventory**
  - Asset Inventory scheduled to run monthly
- **Target Media Wiped and Ready**
- **ISO/Image files for baseline restoration of critical systems/applications**
- **Laptop for Analysis**
- **Forensic Tools Copied to External Media**

- **Network and LAN cables**

## 7.2 Types of Incidents

New incidents can come from multiple sources. Standard Operating Procedures (SOP's) should be created to address potential incidents.

### 7.2.1 Malware

Malware is a code that is made to affect a compromised computer system without the consent of the user. This broad definition includes many particular types of malevolent software (malware) such as spyware, ransomware, command, and control.

Many well-known businesses, states, and criminal actors have been implicated of deploying malware.

Malware differs from other software in that it can spread across a network, cause changes and damage, remain undetectable, and be persistent in the infected system. It can destroy a network and bring a machine's performance to its knees.

*Ransomware*

Ransomware blocks access to a victim's data, typically threating delete it if a ransom is paid. There is no guarantee that paying a ransom will regain access to the data. Ransomware is often carried out via a Trojan delivering a payload disguised as a legitimate file.

*Drive-by Attack*

A drive-by attack is a common method of distributing malware.

A cyber attacker looks for an insecure website and plants a malicious script into PHP or HTTP in one of the pages. This script can install malware into the computer that visits this website or become an IFRAME that redirects the victim's browser into a site controlled by the attacker. In most cases, these scripts are obfuscated, and this makes the code to be complicated to analyze by security researchers. These attacks are known as drive-by because they do not require any action on the victim's part except visiting the compromised website. When they visit the compromised site, they automatically and silently become infected if their computer is vulnerable to the malware, especially if they have not applied security updates to their applications.

*Trojan Horses*

A Trojan is a malicious software program that misrepresents itself to appear useful. They spread by looking like routine software and persuading a victim to install. Trojans are considered among the most dangerous type of all malware, as they are often designed to steal financial information.

### 7.2.2 Man in the Middle

Man-in-the-middle (MITM) attacks are a type of cybersecurity breach that allows an attacker to eavesdrop a communication between two entities. The attack occurs between two legitimate communicating parties, enabling the attacker to intercept communication they should otherwise not be able to access. Thus, the name "man-in-the-middle." The attacker "listens" to the conversation by intercepting the public key message transmission and retransmits the message while interchanging the requested key with his own.

The two parties seem to communicate as usual, without knowing the message sender is an unknown perpetrator trying to modify and access the message before it is transmitted to the receiver. Thus, the intruder controls the whole communication.

### 7.2.3 DDOS

Denial-of-service (DDoS) aims at shutting down a network or service, causing it to be inaccessible to its intended users. The attacks accomplish this mission by overwhelming the target with traffic or flooding it with information that triggers a crash. In both situations, the DoS onslaught denies legitimate users such as employees, account holders, and members of the resource or service they expected.

DDoS attacks are often targeted at web servers of high-profile organizations such as trade organizations and government, media companies, commerce, and banking. Although these attacks do not result in the loss or theft of vital information or other assets, they can cost a victim money and time required to mitigate. DDoS is often used in combination to distract from other network attacks.

### 7.2.4 Phishing

Phishing is a social engineering attack entailing fraudulent communications appearing to come from a trusted source. Attempts to steal sensitive information or trick people into installing malware often come via email.

### 7.2.5 Web Attacks

*SQL Injection*

SQL injection, also known as SQLI, is a kind of attack that employs malicious code to manipulate backend databases to access information that was not intended for display. This may include numerous items including private customer details, user lists, or sensitive company data.

SQLI can have devastating effects on a business. A successful SQLI attack can cause deletion of entire tables, unauthorized viewing of user lists, and in some cases, the attacker can gain administrative access to a database. These can be highly detrimental to a business. When calculating the probable cost of SQLI, you need to consider the loss of customer trust in case personal information like addresses, credit card details, and phone numbers are stolen.

Although SQLI can be used to attack any SQL database, the culprits often target websites.

*Cross Site Scripting*

Cross-site scripting (XSS) is a kind of injection breach where the attacker sends malicious scripts into content from otherwise reputable websites. It happens when a dubious source is allowed to attach its own code into web applications, and the malicious code is bundled together with dynamic content that is then sent to the victim's browser.

Malicious code is usually sent in the form of pieces of JavaScript code executed by the target's browser. The exploits can include malicious executable scripts in many languages including Flash, HTML, Java, and Ajax. XSS attacks can be very devastating; however, alleviating the vulnerabilities that enable these attacks is relatively simple.

### 7.2.6 Breach of Privacy, Confidentiality

A breach of confidentiality happens when data or private information is disclosed to a third party without the data owner's consent. Whether an intentional breach, accidental error or theft, the data owner is entitled to take legal action for potential losses or damage that comes because of the breach.

### 7.2.7 Insider Threat

An insider threat is a threat that originates from within the organization. An insider does not have to be a present employee but rather anyone within the organization that has had proprietary access to confidential information or privileged access.

Contractors, business associates, or third party entities who have knowledge of the security practices, confidential information, or network topography can also pose a significant threat to the organization.

## 7.3 Signs of an Incident

- Precursors
    - Web server log entries identify the usage of a vulnerability scanner
    - An announcement of a new exploit
    - A threat from a group threatening the organization
- Indicators
    - Network Intrusion Detection Alert
    - Antivirus alert
    - Filename Changes
    - Configuration Change
    - Failed login attempts
    - Bounced emails with suspicious content
    - Unusual network activity
    - New accounts with privileged access

### 7.4 Incident Analysis

Take affected devices offline but do not shut them down. The goal is to stop ongoing activity by limiting communication to and from impacted systems but not commit any action that might erase clues, contaminate evidence or otherwise inadvertently aid the attacker.

Change passwords or lock credentials for all involved accounts, whether confirmed or suspected.

Perform an initial analysis to determine the scope, who or what originated the incident, and what tools or attack methods are being used. Each step of the analysis should be thoroughly documented.

- Profile Networks and Systems to help identify changes in expected activity.
- Review log files and security alerts.
- Follow the log retention policy.
- Perform an event correlation, comparing different log files.
- Keep all host clocks synchronized.
- Maintain and use a knowledge base of systems.
- Use Internet search engines for research.
- Run packet sniffers to collect detailed information.
- Consult with external incident response experts.

### 7.5 Incident Documentation

Every step from the time the incident was detected to its final resolution should be documented, signed and timestamped.

- The current status of the incident (new, in progress, forwarded for investigation, resolved, etc.)
- A summary of the incident.
- Indicators related to the incident.
- Other incidents related to the incident.
- Actions taken by incident handlers.
- Chain of custody if applicable.
- Impact assessments related to the incident.
- Contact information for the involved parties.
- A list of evidence gathered.
- Next steps to be taken.

**Note: Customizable by department:** The Incident Intake Form and IR Scoring can be found in the Lansweeper Knowledgebase under Security.

## 8 Containment, Eradication, Recovery

Acquire, preserve, secure and document evidence

## 8.1 CONTAINMENT

In the event that an organization observes a large-scale outbreak that may be reflective of a destructive malware attack, in accordance with Incident Response best practices, the immediate focus should be to contain the outbreak, and reduce the scope of additional systems which could be further impacted.

Some things to consider for each scenario

- Potential damage to and theft of resources.
- Need for evidence preservation.
- Service availability.
- Time and resources needed.
- Duration of the work around solution.
- Potential legal impact.

### 8.1.1 Strategies for containment

- Determine a vector common to all systems experiencing anomalous behavior (or having been rendered unavailable) – from which a malicious payload could have been delivered:
    - Centralized Enterprise Application,
    - Centralized File Share (for which the identified systems were mapped or had access),
    - Privileged User Account common to the identified systems,
    - Network Segment or Boundary, and
    - Common DNS Server for name resolution.
- Based upon the determination of a likely distribution vector, additional mitigation controls can be enforced to further minimize impact:
    - Implement network-based access-control lists to deny the identified application(s) the capability to directly communicate with additional systems,
        - Provide an immediate capability to isolate and sandbox specific systems or resources
    - Implement null network routes for specific IP addresses (or IP ranges) – from which the payload may be distributed,
        - An organization's internal DNS can also be leveraged for this task – as a null pointer record could be added within a DNS zone for an identified server or application
    - Readily disable access for suspected user or service account(s), and
    - For suspect file shares (which may be hosting the infection vector), remove access or disable the share path from being accessed by additional systems.

### 8.1.2 Considerations for Containment

Any changes to compromised systems, including containment actions, may destroy information required to assess the cause of an intrusion. Ensure that all necessary data for analysis is completely collected before making any system changes. Also, collect and protect all evidence that may be needed in a subsequent investigation before performing any containment actions.

## 8.2 ERADICATION AND RECOVERY

- Identify and mitigate all vulnerabilities
- Remove malware, inappropriate materials, and other components

- If more affected hosts are discovered, repeat the detection and analysis steps
- Return affected systems to an operationally ready state
- Confirm that the affected systems are functioning normally
- Implement additional monitoring and/or security features if necessary
- Ensure all steps taken have been documented

# 9 POST INCIDENT ACTIVITY

The Computer Security Incident Handling Guide (NIST 800-61) provides advisement on event analysis activities. Per section, 3.4.1 (Lessons Learned) and section 3.4.2 (Using Collected Incident Data) relevant factors for post-incident and root cause analysis include:

## 9.1 LESSONS LEARNED

Incident Response Teams should hold “lessons learned” meetings with all involved parties after a major incident, and periodically after lesser incidents as resources permit to improve security measures and incident handling processes. Questions to be answered in these meetings include:

- Exactly what happened, and at what times?
- How well did staff and management perform? Were documented procedures followed? Were procedures adequate?
- What information was needed sooner?
- Were any steps or actions taken that might have inhibited the recovery?
- What would/should staff and management do differently the next time a similar incident occurs.
- How could information sharing with other organizations have been improved?
- What corrective actions can prevent similar incidents in the future?
- What precursors or indicators should be watched for in the future to detect similar incidents?
- What additional tools or resources are needed to detect, analyze, and mitigate future incidents?

## 9.2 FOLLOW-UP REPORTING

An important post-incident activity is creating a follow-up report for each incident. Report considerations include:

- Creating a formal event chronology (including time-stamped information from systems)
- Compiling a monetary estimate of the amount of damage the incident caused
- Retaining follow-up reports as specified in retention policies.

Data collected: Organizations collect data that is actionable, based on reporting requirements and perceived value of data collected. Information of value includes number of incidents handled and relative ranking for event types and remediation efforts, and amount of labor and time elapsed for and between each phase of the event.

Root Cause Analysis: Organizations performing root cause analysis should focus on relevant objective assessment activities including:

- Reviewing of logs, forms, reports, and other incident documentation
- Identifying recorded precursors and indicators
- Determining if the incident caused damage before it was detected
- Determining if the actual cause of the incident was identified
- Determining if the incident is a recurrence of a previous incident
- Calculating the estimated monetary damage from the incident
- Identifying measures, if any, that could have prevented the incident.

Post Incident Activity - Once an incident has been closed, a review of the incident and actions taken compared to the incident management plan will reveal strengths and areas for improvement. Review the root-cause analysis at the closure of the incident. Compare actions taken to predefined procedures and identify where procedures were effective and how well they were followed.

# 10 APPENDIX A: GLOSSARY

Common IT security terms adopted from NIST Special Publication 800-37, Revision 4 and the City of Milwaukee

| Term | Definition |
|---|---|
| **Access Control** | Security control designed to permit authorized access to an IT system or application. |
| **Accessible** | Information arranged, identified, indexed, or maintained in a manner that permits the custodian of the public record to locate and retrieve the information in a readable format within a reasonable time. |
| **Authentication** | Verification of the identity of a user, user device, or other entity, or the integrity of data stored, transmitted, or otherwise exposed to unauthorized modification in an IT. |
| **Authorization** | Access privileges granted to a user, program, or process or the act of granting those privileges. |
| **Availability** | The extent to which information is operational, accessible, functional, and usable upon demand by an authorized entity (e.g., a system or user). |
| **Confidentiality** | The property that information is not made available or disclosed to unauthorized individuals, entities, or processes. |
| **Configuration Management** | The process of keeping track of changes to the system, if needed, approving them. |
| **Contingency Plan** | A plan for emergency response, backup operations, and post-disaster recovery maintained by an activity as a part of its security program that will ensure the availability of critical resources and the successful continuity of operations in an emergency. |
| **Control** | An action taken to enhance the likelihood that established goals or objectives will be achieved (in the context of this handbook, generally an action taken to reduce risk). |
| **Data** | A subset of information in an electronic format that allows it to be retrieved or transmitted. |
| **Identification** | The process that enables a user described to an IT system or service. |
| **Digital Media** | A form of electronic media where data are stored in digital (as opposed to analog) form. |
| **Information Security** | The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction to provide confidentiality, integrity, and availability. |
| **Incident** | An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies. |
| **Incident Response** | The manual and automated procedures used to respond to reported network intrusions (real or suspected); network failures and errors; and other undesirable events. |
| **Information** | Information and systems that provide value to an agency or organization. |
| **Information Asset** | Any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual. |
| **Integrity** | Integrity is the protection of information from tampering, forgery, or accidental changes. It ensures that messages are accurately received as sent, and computer errors or non-authorized individuals do not alter information. |
| **Intrusion detection** | The organization configures information systems to provide only essential capabilities, and disables unused or unnecessary components of information systems to prevent unauthorized connection of devices, unauthorized transfer of information, and unauthorized tunneling. |
| **Least Functionality** | Pertaining to techniques, which attempt to detect intrusion into a computer or network by observation of actions, security logs, or audit data. Detection of break-ins or attempts |

| Term | Definition |
|---|---|
| | either manually or via software expert systems that operate on logs or other information available on the network. |
| **Least Privilege** | Granting users, programs, or processes only the access they specifically need to perform their business task and no more. |
| **Multifactor Authentication** | Using more than one of the following factors to authenticate to a system: Something you know (e.g., user-ID, password, personal identification number (PIN), or passcode); something you have (e.g., a one-time password authentication token, 'smart card'); something you are (e.g., fingerprint, retina scan). |
| **Privileged Account** | A privileged account is an account, which provides increased access and requires additional authorization. Examples include a network, system, or security administrator account. |
| **Remote Access** | The connection of a remote computing device via communication lines such as ordinary phone lines or wide area networks to access network applications and information. |
| **Risk** | The probability that a particular threat will exploit a particular vulnerability of the system. |
| **Risk Assessment** | The process of identifying threats to information or information systems, determining the likelihood of occurrence of the threat, and identifying system vulnerabilities that could be exploited by the threat. |
| **Security (IT)** | Measures and controls that protect IT systems/information against denial of access and unauthorized (accidental or intentional) disclosure, modification, or destruction of ITs and data. IT security includes consideration of all hardware and/or software functions. |
| **System** | An interconnected set of information resources under the same direct management control that shares common functionality. A system normally includes hardware, software, applications, and communications. |
| **Threat** | A potential circumstance, entity, or event capable of exploiting vulnerability and causing harm. Threats can come from natural causes, human actions, or environmental conditions. A threat does not present a risk when there is no vulnerability. |
| **User** | Any State Entity, federal government entity, political subdivision, their employees or third-party contractors or business associates, or any other individuals who are authorized by such entities to access a system for a legitimate government purpose. |
| **Vulnerability** | A weakness that can be accidentally triggered or intentionally exploited. |

# 11 APPENDIX B: EXAMPLES OF INCIDENTS

**Incident Example –Privileged Access**

Look for indications of

- Existence of unauthorized security-related tools or exploits –file integrity monitor
- Unusual traffic to and from the host (e.g., attacker may use the host to attack other systems) – netflow
- System configuration changes, including:
    - process/service modifications or additions –tasklist/ps
    - unexpected open ports –netstat, netflow
    - system status changes (restarts, shutdowns)
    - changes to log and audit policies and data –file integrity monitor
    - network interface card set to promiscuous mode (packet sniffing)-new administrative-level user account or group –qwinsta/who/last
- Modifications of critical files, timestamps and privileges, including executable programs, OS kernels, system libraries, and configuration and data files –file integrity monitor
- Unexplained account usage (e.g., idle account in use, account in use from multiple locations at once, unexpected commands from a particular user, large number of locked-out accounts) – qwinsta/who/last
- Significant changes in expected resource usage (e.g., CPU, network activity, full logs, or file systems) –tasklist/ps
- Network and host intrusion detection alerts –NIDS/HIDS
- New files or directories with unusual names (e.g., binary characters, leading spaces, leading dots) – file integrity monitor
- Highly unusual operating system and application log messages –syslog, app logs

**Incident Example –Malicious Code**

Look for indications of

- Antivirus software alerts of infected files –avalerts
- Sudden increase in the number of emails being sent and received –email server logs
- Deleted, corrupted, or inaccessible files –file integrity monitor
- System instability and crashes
- Port scans and failed connection attempts targeted at the vulnerable service (e.g., open Windows shares, HTTP) –netflow
- Increased network usage –netflow
- Network intrusion detection alerts of Trojan horse client-server communications –NIDS
- Firewall and router log entries for Trojan horse client-server communications –firewall/router logs
- Network connections between the host and unknown remote systems –netstat
- Unusual and unexpected ports open –netstat
- Unknown processes running –tasklist/ps
- High amounts of network traffic generated by the host, particularly if directed at external host(s) – netflow

**Incident Example –Denial of Service**

Look for indications of

- User reports of system, network, or application unavailability
- Unexplained connection losses
- Network and host intrusion detection alerts –NIDS/HIDS
- Host intrusion detection alerts (until the host is overwhelmed) –HIDS
- Increased network bandwidth utilization –netflow
- Large number of connections to a single host –netstat, netflow
- Asymmetric network traffic pattern (large amount of traffic going to the host, little traffic coming from the host; large amount of traffic entering the network, little traffic leaving the network) –netflow
- Firewall and router log entries –SIEM, firewall/router logs
- Packets with unusual source addresses –netstat, netflow
- Packets with nonexistent destination addresses –netstat, netflow
- Operating system log entries –syslog
- Application log entries –syslog, app logs

# 12 APPENDIX C: INTAKE FORM

## COMPUTER SECURITY INCIDENT HANDLING FORMS

***INCIDENT IDENTIFICATION DATE***:

### General Information

**Incident Detector's Information:**
Name:
Date and Time Detected
Title:
Desk Phone: Cell Phone:
E-mail:

### Incident Summary

#### Detection Method

| | |
|---|---|
| ☐Anti-Virus | ☐User Complaint |
| ☐Intrusion Detection | ☐Other: |
| ☐Network Activity | |
| ☐Log Files/Audit | |

#### Source if Known:

| IP Address | Port | Other |
|---|---|---|
| | | |

#### Systems Affected

| Computer Name | Device Type/Function | OS/Version |
|---|---|---|
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |

## Impact

The table below defines each impact category description and its associated severity levels. Use the tables below to identify impact levels and incident details. Note: Incidents may affect multiple types of data; therefore, you may select multiple options when identifying the information impact.

| **Impact Category** | | **Category Severity Levels** |
|---|---|---|
| Functional Impact – A measure of the impact to business functionality or ability to provide services | ☐ | NO IMPACT – Event has no impact. |
| | ☐ | NO IMPACT TO SERVICES – Event has no impact to any business or Industrial Control Systems (ICS) services or delivery to entity customers. |
| | ☐ | MINIMAL IMPACT TO NON-CRITICAL SERVICES – Some small level of impact to noncritical systems and services. |
| | ☐ | MINIMAL IMPACT TO CRITICAL SERVICES –Minimal impact but to a critical system or service, such as email or active directory. |
| | ☐ | SIGNIFICANT IMPACT TO NON-CRITICAL SERVICES – A non-critical service or system has a significant impact. |
| | ☐ | DENIAL OF NON-CRITICAL SERVICES – A non-critical system is denied or destroyed. |
| | ☐ | SIGNIFICANT IMPACT TO CRITICAL SERVICES – A critical system has a significant impact, such as local administrative account compromise. |
| | ☐ | DENIAL OF CRITICAL SERVICES/LOSS OF CONTROL – A critical system has been rendered unavailable. |
| Information Impact – Describes the type of information lost, compromised, or corrupted. | ☐ | NO IMPACT – No known data impact. |
| | ☐ | SUSPECTED BUT NOT IDENTIFIED – A data loss or impact to availability is suspected, but no direct confirmation exists. |
| | ☐ | PRIVACY DATA BREACH – The confidentiality of personally identifiable information (PII6) or personal health information (PHI) was compromised. |
| | ☐ | PROPRIETARY INFORMATION BREACH – The confidentiality of unclassified proprietary information7, such as protected critical infrastructure information (PCII), intellectual property, or trade secrets was compromised. |
| | ☐ | DESTRUCTION OF NON-CRITICAL SYSTEMS – Destructive techniques, such as master boot record (MBR) overwrite; have been used against a non-critical system. |
| | ☐ | CRITICAL SYSTEMS DATA BREACH - Data pertaining to a critical system has been exfiltrated. |
| | ☐ | CORE CREDENTIAL COMPROMISE – Core system credentials (such as domain or enterprise administrative credentials) or credentials for critical systems have been exfiltrated. |
| | ☐ | DESTRUCTION OF CRITICAL SYSTEM – Destructive techniques, such as MBR overwrite; have been used against a critical system. |
| Recoverability – Identifies the scope of resources needed to recover from the incident | ☐ | REGULAR – Time to recovery is predictable with existing resources. |
| | ☐ | SUPPLEMENTED – Time to recovery is predictable with additional resources. |
| | ☐ | EXTENDED – Time to recovery is unpredictable; additional resources and outside help are needed |
| | ☐ | NOT RECOVERABLE – Recovery from the incident is not possible (e.g., sensitive data exfiltrated and posted publicly) |

## Attack Vectors

To clearly communicate incidents throughout the Federal Government and supported organizations, it is necessary for government incident response teams to adopt a common set of terms and relationships between those terms. Below is a high-level set of attack vectors and descriptions developed from NIST SP 800-61 Revision 2. Federal civilian agencies are to utilize the following attack vectors taxonomy when sending cybersecurity incident notifications to US-CERT.

| | **Attack Vector** | **Description** | **Example** |
|---|---|---|---|
| ☐ | **Unknown** | Cause of attack is unidentified. | This option is acceptable if cause (vector) is unknown upon initial report. May be updated. |
| ☐ | **Attrition** | An attack that employs brute force methods to compromise, degrade, or destroy systems, networks or services. | Denial of Service intended to impair or deny access to an application; a brute force attack against an authentication mechanism, such as passwords or digital signatures. |
| ☐ | **Web** | An attack executed from a website or web-based application. | Cross-site scripting attack used to steal credentials, or a redirect to a site that exploits a browser vulnerability and installs malware. |
| ☐ | **Email/Phishing** | An attack executed via an email message or attachment. | Exploit code disguised as an attached document, or a link to a malicious website in the body of an email message. |
| ☐ | **External/Removable Media** | An attack executed from removable media or a peripheral device. | Malicious code spreading onto a system from an infected flash drive. |
| ☐ | **Impersonation/Spoofing** | An attack involving replacement of legitimate content/services with a malicious substitute. | Spoofing, man in the middle attacks, rogue wireless access points, and structured query language injection attacks all involve impersonation. |
| ☐ | **Improper Usage** | Any incident resulting from violation of an organization’s acceptable usage policies by an authorized user, excluding the above categories. | User installs file-sharing software, leading to the loss of sensitive data; or a user performs illegal activities on a system. |
| ☐ | **Loss or Theft of Equipment** | The loss or theft of a computing device or media used by the organization | |
| ☐ | **Other** | An attack method does not fit into any other vector. | |

## Incident Status

| Status | Actions Taken | Person Reporting | Date/Time |
|---|---|---|---|
| | | | |
| | | | |
| | | | |

## Incident Notification

| Individual Notified | Notification Method | Date/Time |
|---|---|---|
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |

# 13 Appendix D: Follow Up Report

The following are examples of activities in a typical after-action review. List all participants in the review and their role in incident management. Identify lessons learned. Describe the incident

<table>
<tr><th colspan="4">Incident Response Follow Up Report</th></tr>
<tr><td colspan="4">List all participants in the review and their role in incident management</td></tr>
<tr><td><i>Name</i></td><td colspan="3"><i>Role</i></td></tr>
<tr><td></td><td colspan="3"></td></tr>
<tr><td></td><td colspan="3"></td></tr>
<tr><td></td><td colspan="3"></td></tr>
<tr><td></td><td colspan="3"></td></tr>
<tr><td></td><td colspan="3"></td></tr>
<tr><td></td><td colspan="3"></td></tr>
<tr><td></td><td colspan="3"></td></tr>
<tr><td></td><td colspan="3"></td></tr>
<tr><td></td><td colspan="3"></td></tr>
<tr><td></td><td colspan="3"></td></tr>
<tr><td colspan="4"><i>Information Covered</i></td></tr>
<tr><td colspan="4">Exactly what happened, and at what time?</td></tr>
<tr><td colspan="4">How well did staff and management perform in dealing with the incident? Were the document procedures followed? Were they adequate?</td></tr>
<tr><td colspan="4">What information was needed sooner?</td></tr>
<tr><td colspan="4">Where any steps or actions taken that might have inhibited the recovery?</td></tr>
<tr><td colspan="4">What would the staff and management do differently the next time a similar incident occurs?</td></tr>
<tr><td colspan="4">How could information sharing been improved?</td></tr>
<tr><td colspan="4">What corrective actions can prevent similar incidents in the future?</td></tr>
<tr><td colspan="4">What precursors or indicators should be watched for in the future to detect similar incidents?</td></tr>
<tr><td colspan="4">What additional tools are resources are needed to detect, analyze, and mitigate future incidents?</td></tr>
<tr><td colspan="4">Number of Incident’s handled and handling time.</td></tr>
<tr><td colspan="4"><i>Deliverables</i></td></tr>
<tr><td colspan="2">Corrective Action</td><td>Person Responsible</td><td>Date Expected</td></tr>
<tr><td colspan="2"></td><td></td><td></td></tr>
<tr><td colspan="2"></td><td></td><td></td></tr>
<tr><td colspan="2"></td><td></td><td></td></tr>
<tr><td colspan="2"></td><td></td><td></td></tr>
<tr><td colspan="2"></td><td></td><td></td></tr>
<tr><td colspan="2"></td><td></td><td></td></tr>
</table>