|  |  |
| --- | --- |
| [Organization Name] | **No:**  [Policy Number] |
| **IT Standard**:  **Cyber Incident Response** | **Updated:** 10/26/2024 |
| **Issued By:**  [Policy Authority]  **Owner:**  [Policy Owner] |

# 1.0 Purpose and Benefits

This standard outlines the general steps for responding to computer security incidents. In addition to providing a standardized process flow, it (1) identifies the incident response (IR) stakeholders and establishes their roles and responsibilities; (2) describes incident triggering sources, incident types, and incident severity levels; and (3) includes requirements for annual testing, post-incident lessons-learned activities, and collection of IR metrics for use in gauging IR effectiveness.

The goals of IR, as outlined in this standard, are to:

1. Confirm whether an incident occurred;
2. Provide a defined incident notification process;
3. Promote the accumulation and documentation of accurate information;
4. Establish controls for proper retrieval and handling of evidence;
5. Contain the incident and stop any unwanted activity quickly and efficiently;
6. Minimize disruption to network operations;
7. Provide accurate reports and useful recommendations to management; and
8. Prevent and/or mitigate future incidents from occurring.

# 2.0 Authority

This policy is established under the authority of organizational management and is guided by best practices outlined in the National Institute of Standards and Technology (NIST) Cybersecurity Framework 2.0. While not mandated by law, the organization adopts this framework to enhance its cybersecurity posture and protect its information assets. The authority for enforcement and adherence to this policy is vested in the [Policy Authority], who is responsible for ensuring compliance across all departments.

# 3.0 Scope

This policy applies to all employees, contractors, third-party vendors, and any individuals or entities accessing, using, or managing the organization's information systems, networks, and physical infrastructure, regardless of the medium or format of the information. It covers all electronic, paper-based, and verbal communication, including, but not limited to, data processing systems, cloud services, email platforms, mobile devices, databases, and other digital storage mechanisms that store, transmit, or process sensitive organizational information.

The policy encompasses internal and external users, whether they access the organization's systems on-site or remotely, and includes all physical infrastructure such as data centers, workstations, and hardware that interact with or support the organization's information environment. Additionally, it extends to any devices, both personal and organizational, that connect to the corporate network or handle company data.

All users are responsible for protecting the confidentiality, integrity, and availability of information, complying with this policy and relevant laws, and familiarizing themselves with the organization's security policies and procedures to ensure the protection of organizational assets. Failure to comply with these requirements may result in disciplinary action, including termination of access rights or contractual agreements.

# 4.0 Information Statement

This policy establishes a comprehensive framework for responding to computer security incidents within the organization. Its primary purpose is to standardize the incident response (IR) process, ensuring that all stakeholders understand their roles and responsibilities in addressing security threats effectively. The policy outlines procedures for identifying, containing, eradicating, and recovering from incidents while promoting best practices in communication, documentation, and evidence handling.

By incorporating annual testing and post-incident reviews, the organization aims to continuously improve its IR capabilities, minimize operational disruptions, and mitigate future threats. Overall, this policy serves to enhance the organization's cybersecurity posture and protect its information assets by providing clear guidelines for proactive incident management and response.

* 1. IR Stakeholder Roles and Responsibilities

In order to respond effectively to a computer security incident, it is critical that all IR stakeholders fully understand not only their roles and responsibilities in the IR process, but also the roles and responsibilities of each IR stakeholder. This is necessary to (1) avoid duplication of effort; (2) minimize procedural gaps that may occur; and (3) ensure rapid response to computer security incidents.

IR stakeholders include:

1. [Authority] – The [Authority], or his/her designee, provides for overall coordination of IR including the escalation of an incident. The [Authority] leads incident response services for the organization.
2. Entity Leadership - Provides mainly IR oversight, with their [Authority] or designee, being the most ‘hands-on’ in terms of IR management activities.
3. Security Operations Center – The Security Operations (SOC) Center serves as a central group for detection, analysis, tracking, response to and reporting of cyber threats and incidents. The SOC responds to incidents by providing hands-on technical IR and will recommend steps for staff to remediate and mitigate such that it reduces the likelihood of future incidents.
4. In addition, the SOC facilitates collaboration and information sharing with other entities that may be experiencing the same or similar incidents, to help resolve the problem more quickly than if done separately. The SOC collects information on the types of vulnerabilities that are being exploited and the frequency of attacks and shares preventative information to help other organizations protect themselves from similar attacks.
5. First Responders – IT staff, such as network managers, system administrators, and other technical personnel, will be called upon, as needed, to provide support and tactical response to the Security Operations Center. All digital forensic analysis must be performed by, or under the direction of, the SOC.
6. Agency Incident Response Teams –Predefined teams must be ready which include, at minimum, Executive Management, Legal and the Public Information Officer. In some cases, Human Resources and Labor Relations may become involved.
7. External Entities - In consultation with the Security Operations Center, external entities may conduct hands-on IR activities, such as investigative response activities, or may provide guidance. For example, a security solutions vendor may provide assistance on security appliance settings. External entities include vendors, service providers, or law enforcement including, but not limited to:
   1. Multi-State Information Sharing and Analysis Center (MS-ISAC)
   2. Federal Bureau of Investigation (FBI)
   3. Internet Service Providers
   4. Security Solutions Vendors
   5. Data Holder Vendors
   6. IR Process Flow

This IR process flow covers how to respond to specific situations for IR stakeholders to ensure an effective and efficient response. The focus of the IR process is to eradicate the problem as quickly as possible, while gathering actionable intelligence, to restore business functions, improve detection, and prevent reoccurrence. An entity can adopt the six step IR process flow as depicted below[[1]](#footnote-2):

*Figure 4.1 – Incident Response Process Flow*

**Step 1: Preparation**

Proper planning and preparation for an incident before it occurs ensures a more effective and efficient IR process. Activities associated with this step, include establishing IR teams; updating IR tools, policies/procedures, and forms/checklists; and ensuring IR communication procedures and IR stakeholder contact lists are accurate and up-to-date. An entity must have a defined and up to date Contact List and establish multiple communication channels with all entities and individuals on the IR Contact List.

An entity must assign responsibility for a central point of contact to coordinate identification and reporting up to the [Authority]. Typically, this is performed by the entity’s designated security representative. As per the Information Security Policy, all employees are required to report suspected information security incidents or weaknesses to the appropriate manager and designated security representative.

The Security Operations Center will establish standard operating procedures (SOPs) for IR to reflect industry standards and best practice. These SOPs will be followed during incident response. Any exception must be documented. The Security Operations Center must routinely vet and validate the tools and techniques used for IR. In order to operate efficiently and effectively, the IR process must be regularly tested. This must occur at least annually. This testing can be accomplished with mock incident training or tabletop exercises using realistic scenarios to provide a high-level outline and systematic walkthrough of the IR process and, to the extent possible, must include all IR stakeholders. These training scenarios must include specific 'discussion points' that represent key learning opportunities, and incorporate lessons-learned, which can then be integrated into the IR process as part of its review.

**Step 2: Identification**

Identification involves review of anomalies to determine whether or not an incident has occurred, and, if one has occurred, determining the nature of the incident. Identification begins with an event, an anomaly that has been reported or noticed in a system or network. Detection can be accomplished through technical sources (e.g., operations staff, anti-virus software), non-technical sources (e.g., user security awareness and reporting), or both.

It is important to recognize that not every network or system event will be a security incident. A first responder must be assigned to determine if there is an incident, categorize the incident and escalate as necessary. Typically, this will be the entity’s designated security representative.

To be effective in IR, incidents must be classified, and escalated as soon as possible to the proper IR stakeholders to promote collaboration and information sharing. Incident classification requires the use of established incident categories together with an incident severity matrix as a means for prioritizing incidents and determining appropriate IR activities.

Incident Categories

It is important to categorize common incidents experienced throughout the enterprise. By doing so, IR stakeholders can better focus their IR activities. It should be noted that incidents can have more than one category and categorization may change as the investigation unfolds. An entity can adopt the six (6) US-CERT[[2]](#footnote-3) incident categories as follows:

| Incident Categories | | |
| --- | --- | --- |
| Category | Name | Description |
| 0 | Exercise / Network Defense Testing | Used during state, federal, international exercises and approved activity testing of internal/external network defenses or responses. |
| 1 | Unauthorized Access | An individual gains logical or physical access without permission to a local government network, system, application, data, or other resource. |
| 2 | Denial of Service | An attack that successfully prevents or impairs the normal authorized functionality of networks, systems, or applications by exhausting resources. This activity includes being the victim of or participating in the Denial of Service (DoS). |
| 3 | Malicious Code | Successful installation of malicious software (e.g., virus, worm, Trojan horse, or other code-based malicious entity) that infects an operating system or application. |
| 4 | Improper Usage | A person who knowingly or unknowingly violates acceptable computing use policies. |
| 5 | Scans / Probes / Attempted Access | Includes any activity that seeks to access or identify an entity’s computer, open ports, protocols, service, or any combination for later exploit. This activity does not directly result in a compromise or denial of service. Unauthorized internal scans are considered incidents. Most external scans are considered to be routine, and on a case-by-case basis may require response and investigation. |
| 6 | Investigation | Unconfirmed incidents that are potentially malicious or anomalous activity deemed by the reporting entity to warrant further review. |

*Table 4.2 – Incident Categories*

Incident Severity Matrix

All information security incidents should be categorized according to severity level to assist in determining the extent to which a formal IR is required. Severity levels are based on the perceived business impact of the incident. Severity levels may change as the investigation unfolds. General definitions and description of each severity level are as follows:

|  |  |  |
| --- | --- | --- |
| Incident Severity Matrix | | |
| Level | Definition | Examples |
| High | Incidents that have a severe impact on operations | * Compromise of sensitive data * Widespread malcode attack * Unauthorized access to critical systems * DoS affecting the entire enterprise |
| Medium | Incidents that have a significant impact, or the potential to have a severe impact, on operations | * Small-scale DoS attack * Website compromises * Unauthorized access (brute force attacks against FTP, ssh, and other protocols) |
| Low | Incidents that have a minimal impact with the potential for significant or severe impact on operations | * Network probes or system scans * Isolated virus infections * Acceptable use violations |

*Table 4.3 – Incident Severity Matrix*

Escalation Procedures

During an incident, clear and effective communication is critical. As such, an escalation procedure should address all lines of communication in the event an incident occurs. This includes not only internal communication but external communications as well. Communication should flow through all involved IR stakeholders so that everyone has the necessary information to act and carry out their responsibilities in a timely manner. Notification must be made as soon as possible but should not delay the entity from taking appropriate actions to isolate and contain damage.

Each entity must have an IR escalation procedure that consists of (1) an escalation matrix, (2) an up-to-date contact list with alternate contacts, and (3) multiple communications channels, all in an effort to ensure appropriate and accurate information is disseminated quickly to the appropriate IR stakeholders.

Incident Scoping

Initial scoping is provided by the entity and includes:

* Identifying potential targets (e.g., known compromised systems, likely affected systems, key systems);
* Defining external touch points (e.g., Internet, wireless, 3rd party, remote access connections);
* Prioritizing likely scenarios (e.g., internal vs., external threat, targeted attack vs., target of opportunity); and
* Visualizing in-scope environment (e.g., network diagram, data flow).

Considerations for incident scoping activities are as follows:

* Relying on relevant and verified evidence sources;
* Reducing false positives and volume of data;
* Avoiding excessive scope and ‘scope creep’; and
* Realizing operational and resource limitations may affect scope.

As additional incident-related information develops during the IR process and as additional stakeholders become involved, an incident typically requires re-scoping.

Incident Tracking & Reporting

A secure centralized tracking system, that can accommodate ‘need to know’ access, leads to a more efficient and systematic IR effort, as well as provides an audit trail should the efforts lead to legal prosecution of the threat.

At a minimum, documentation of the incident must contain the following information:

* Date / time the incident was reported
* Type of Incident
* Reporting source of incident
* Summary of the incident
* Current status of the incident
* All actions taken concerning the incident
* Contact information for all involved parties
* Evidence gathered during incident investigation
* Relevant comments from IR team members
* Proposed next steps to be taken

**Step 3: Containment**

This step focuses on containing the threat to minimize damage. It is during this step that information is collected to determine how the attack took place. All affected systems within the enterprise should be identified so that containment (and eradication and recovery) is effective and complete.

Incident containment involves ‘stopping the bleeding’ and preventing the incident from spreading. Containment can be accomplished by isolating infected systems, blocking suspicious network activity, and disabling services among other actions. Containment varies for each incident depending on the severity and risk of continuing operations. Entity leadership makes decisions regarding containment measures based on recommendations from the [Authority].

**Step 4: Eradication**

Eradication involves removing elements of the threat from the enterprise network. Specific eradication measures depend on the type of incident, number of systems involved, and the types of operating systems and applications involved. Typical eradication measures include reimaging infected systems and enhanced monitoring of system activity.

Analysis of information collected is an iterative process and occurs/reoccurs during both the containment and eradication phases.

**Step 5: Recovery**

Once the root cause of an incident has been eradicated, the recovery phase can begin. The goals of this step are to: (1) remediate any vulnerabilities contributing to the incident (and thus prevent future incidents) and (2) recover by restoring operations to normal. A phased approach is often used to return systems to normal operation, harden them to prevent similar future incidents and heighten monitoring for an appropriate period of time. Typical recovery activities include rebuilding systems from trusted images/gold standards, restoring systems from clean backups and replacing compromised files with clean versions.

Care must be taken to ensure that files restored from backup do not reintroduce malicious code or vulnerabilities from the incident and that the system is clean and secure before returning to production use. Once recovery has been completed, the IR lead must validate/certify that the incident has been resolved.

**Step 6: Lessons Learned**

An IR process is only as good as the ability to execute it successfully. Lessons learned can be the results of actual IR activities or IR capability testing, and these results should be used to improve the IR process by identifying systemic weaknesses and deficiencies and taking steps to improve on these. It is important that this take place relatively soon after the incident is closed.

Lessons learned, or post mortem, discussions provide (1) a record of steps taken to respond to an attack, (2) investigative results into determining the root cause of the attack, (3) potential improvements to make, such as IR stakeholder training and certifications, process and procedural updates, and technical modifications. Knowledge gained can be used in an effort to prevent and/or mitigate future incidents in the form of proactive services. This may include testing the IR process, conducting vulnerability assessments, providing computer security training, reviewing security policies and procedures, and disseminating cyber security reminders.

Both incident reports and the results of these lesson-learned discussions will be placed into a database for future use and shared with all IR stakeholders for situational awareness and professional development.

* 1. Incident Response Metrics

IR metrics must be compiled for each incident and reported to the [Authority] for enterprise situational awareness when possible and practical.

These metrics allow IR stakeholders (1) to measure IR effectiveness (and reveal potential gaps) over time; (2) identify trends in terms of threat activities and in doing so; (3) to provide justification for additional resources, to include additional personnel, training, and tools.

| IR Metrics | | |
| --- | --- | --- |
| Category | Measurement | Description |
| Incidents | # Total Incidents / Year | Total amount of incidents responded to per year |
| # Incidents by Type / Year | Total number of incidents by category responded to per year |
| Time | # Personnel Hours / Incident | Total amount of labor spent resolving incident |
| # Days / Incident | Total amount of days spent resolving incident |
| # System Down-Time Hours / Incident | Total hours of system down-time until incident resolved |
| Cost | Estimated Monetary Cost / Incident | Total estimated monetary cost per incident, to include containment, eradication, and recovery, as well as collection & analysis activities (this may include labor costs, external entity assistance, tool procurements, travel, etc.) |
| Damage | # Systems Affected / Incident | Total number of systems affected per incident |
| # Records Compromised / Incident | Total number of records compromised per incident |
| Forensics | # Total Forensics Leveraged Incidents / Year | Total number of incidents requiring forensics (collection & analysis) per year |
| # System Images Analyzed / Incident | Total number of system images analyzed per incident |
| # System Memory Dumps Examined / Incident | Total number of system physical memory dumps examined per incident |

*Table 4.4 – Incident Response Metrics*

# 5.0 Compliance

This policy shall take effect upon publication. Compliance is expected with all enterprise policies and standards. Policies and standards may be amended at any time; compliance with amended policies and standards is expected.

If compliance with this standard is not feasible or technically possible, or if deviation from this policy is necessary to support a business function, entities shall request an exception through the following process.

# 6.0 Policy Exceptions

Requests for exceptions to this policy must be submitted to the [Authority] by the requesting department. Each request should include the scope and justification for the exception, potential risks, proposed mitigation measures, and a timeframe for achieving compliance. The [Authority] will review and discuss these requests with the department.

# 7.0 Definitions of Key Terms

|  |  |
| --- | --- |
| **Term** | **Definition** |
| Information Systems | Any combination of hardware, software, data, and personnel that processes, stores, or transmits information, including but not limited to computers, servers, networks, and applications. |
| Users | Individuals or entities, including employees, contractors, and third-party vendors, who access or interact with the organization’s information systems and data. |
|  |  |

# 8.0 Contact Information

Submit all inquiries and requests for future enhancements to the policy owner at:

[Policy Owner’s Contact Info]

[Organization Address]

# 9.0 Review and Revision

This policy should be reviewed at least annually to keep pace with evolving regulations, threat landscapes, and organizational changes. However, more frequent reviews may be necessary following regulatory updates, cybersecurity incidents, significant technology changes, organizational shifts, or compliance audits. This policy should be revised based on these reviews and those revisions noted below.

|  |  |  |
| --- | --- | --- |
| **Date** | **Description of Change** | **Reviewer** |
|  |  |  |

# 10.0 Related Documents

[National Institute of Standards and Technology (NIST) SP: 800-61 - Computer Security Incident Handling Guide](https://csrc.nist.gov/pubs/sp/800/61/r2/final)

[National Institute of Standards and Technology (NIST) SP: 800-50 - Building a Cybersecurity and Privacy Learning Program](https://csrc.nist.gov/pubs/sp/800/50/r1/final)

[National Institute of Standards and Technology (NIST) SP: 800-84 - Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities](https://csrc.nist.gov/pubs/sp/800/84/final)

[National Institute of Standards and Technology (NIST) SP: 800-92 - Guide to Computer Security Log Management](https://csrc.nist.gov/pubs/sp/800/92/final)

1. Based on the SANS Institute Incident Handling Step-by-Step [↑](#footnote-ref-2)
2. http://www.us-cert.gov/government-users/reporting-requirements [↑](#footnote-ref-3)