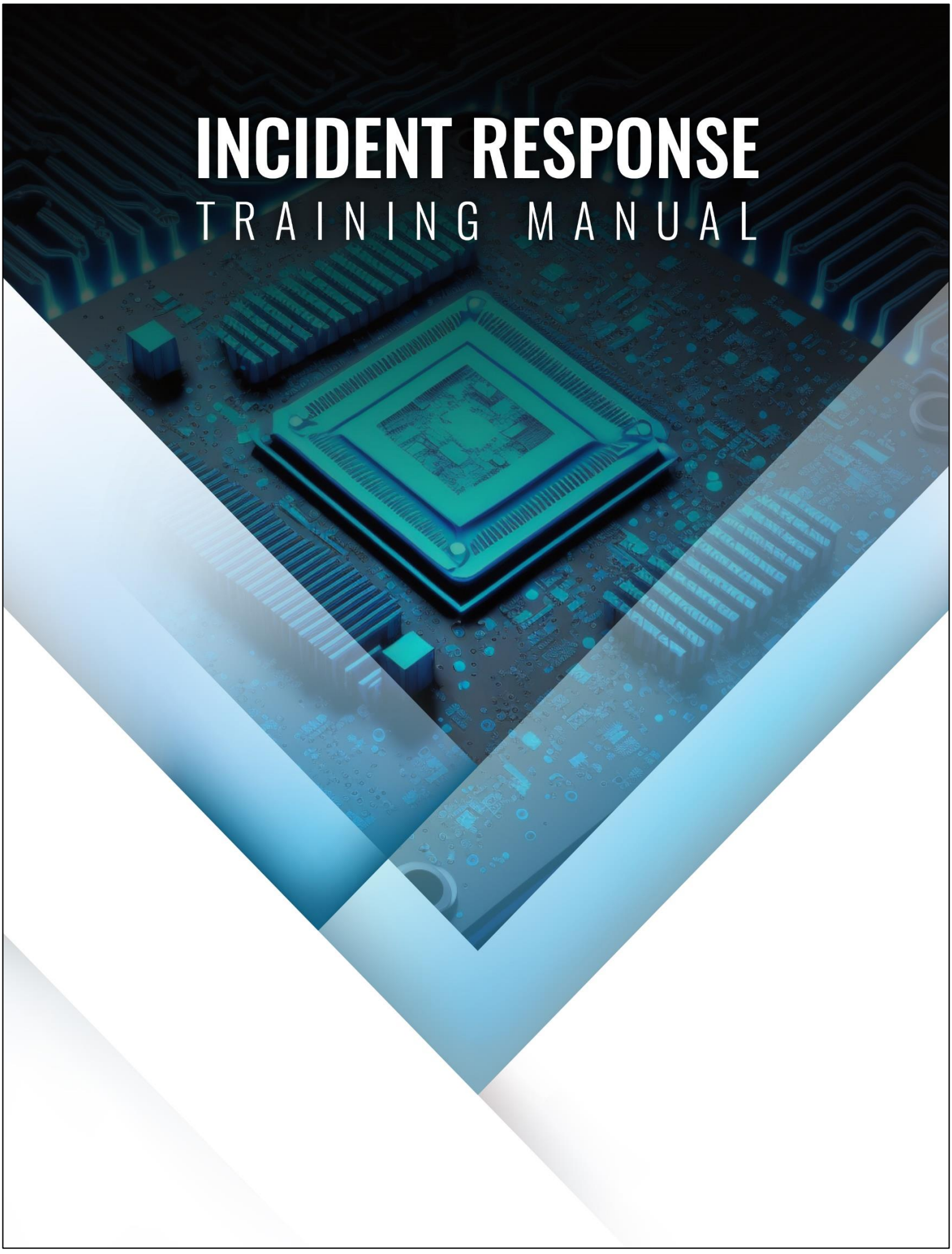
INCIDENT RESPONSE

TRAINING MANUAL



[Company Name] Incident Response Training Manual

Official Policy Title:	
Responsible Party:	
Approval Party:	
Effective Date:	
Last Update:	
Version Number:	
Policy Framework:	**Developed in accordance with NIST Special Publication (SP) 800 Series - https://csrc.nist.gov/publications/sp800**
Mapping	**NIST SP 800-53, rev. 5 [IR-2]**

Introduction

The Incident Response Training Manual referenced within this document defines the security measures to be implemented by [company name] that strive to ensure the Confidentiality, Integrity, and Availability (CIA) of information systems. Additionally, the Incident Response Training Manual is to be disseminated to all in-scope personnel within the organization. The Incident Response Training Manual is to be reviewed and updated [annually, or other designated time frame] by a responsible party at [company name].

Purpose

The purpose of the Incident Response Training Manual is to outline the organization's training objectives for ensuring all-in scope personnel have a strong foundational understanding and working knowledge of all facets of incident response, from initial detection to final resolution of such incidents. *It is therefore the requirement for all in-scope personnel to read and acknowledge - via signature - the [Company name] Incident Response Training Manual.*

Scope

The Incident Response Training Manual includes training material relating to all facets of incident response, and includes the following training modules:

- Training Module 1 - The Importance of Incident Response

- Training Module 2 - What's an Incident?
- Training Module 3 - Incident Response Preparation
- Training Module 4 - Build A Capable, Skilled Incident Response Team
- Training Module 5 - Incident Response Detection
- Training Module 6 - Attack Vectors
- Training Module 7 - Initial Response and Containment
- Training Module 8 - Eradication
- Training Module 9 - Security Analysis & Recovery and Repair
- Training Module 10 - Communication is KEY!
- Training Module 11 - Post Incident Activities and Awareness
- Training Module 12 - Be Mindful of Human Error
- Training Module 13 - Test Your Incident Readiness
- Training Module 14 - Be Vigilant!

Training Module 1 - The Importance of Incident Response

Data breaches, cyber security threats, and many other malicious exploits are challenging organizations like never before, ultimately requiring comprehensive security measures for helping ensure the confidentiality, integrity, and availability (CIA) of one's entire information systems landscape.

Unfortunately, security breaches do happen - even with the best controls in place - thus the ability to respond swiftly and effectively is a must for mitigating any further damage. It's the main reason why every organization should have a well-defined and in-depth incident response plan in place - one complete with documented policies and procedures, along with essential forms and templates to be used as necessary.

Oftentimes, the difference between an incident being stopped dead in its tracks and one that quickly turns into a catastrophic security breach are mere seconds – all the more reason for having a well-documented, agile and ready-to-implement incident response plan.

Structured protocol is extremely important for incident response initiatives as it achieves the following:

As with any topic relating to the broader subject of information security, there are a countless number of publications centering around the concept of incident response. From blogs to books - and everything in between – everybody has their opinion on what exactly is incident response, and how should organizations build and deploy such a plan. Having a healthy debate on anything in the world of information security is a good thing, and that definitely goes for incident response, one of the most critically important measures for helping secure an organization's assets.

Just remember that undertaking all necessary incident response measures is a complex endeavor indeed, therefore, establishing a successful incident response capability requires substantial planning and resources. It also requires a team effort. Remember that continually monitoring for attacks is essential - it's never a one-and-done scenario.

Establishing clear procedures for prioritizing the handling of incidents is critical, as is implementing effective methods of collecting, analyzing, and reporting data. It is also vital to build relationships and establish suitable means of communication with other internal groups (e.g., human resources, legal, etc.) and with external groups (e.g., other incident response teams, law enforcement, etc.).

If you want a definition for incident response, consider the following (per NIST): *The mitigation of violations of security policies and recommended practices.*

You now know the importance of incident response, so let's discuss what an incident actually is.

Training Module 2 - What's an Incident?

Per NIST, an 'incident' is defined as the following: 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.

Just a few examples of the almost endless number of incidents that can happen at any organization include the following:

- An attacker commands a botnet to send high volumes of connection requests to an organization's web servers, causing it to crash.
- Users are tricked into opening a "quarterly report" sent via email that is malware; running the tool has now infected their computers and established connections with an external host.
- A perpetrator obtains unauthorized access to sensitive data and threatens to release the details to the press if the organization does not pay a designated sum of money.
- A user provides illegal copies of software to others through peer-to-peer file sharing services.

And since the topic of incident response must clearly include cybersecurity, NIST defines a 'cybersecurity incident' as the following: A cybersecurity event that has been determined to have an impact on the organization prompting the need for response and recovery.

Remember, cyber and other related incidents will happen - it's the nature of the world we live in - and everyone will have an important role in helping to stop such threats. It's a team effort!

Training Module 3 - Incident Response Preparation

For incident response, the concept of "Preparation" essentially comes down to having users aware of common security threats that can potentially compromise an organization's network infrastructure, cause harm to other related systems or pose a significant financial, operational, or business threat to the organization as a whole. After all, how can a user even possibly begin to think about security issues if they're not even aware of today's growing threats?

There are numerous security threats that are potentially detrimental to any organization, Here's just a small sample:

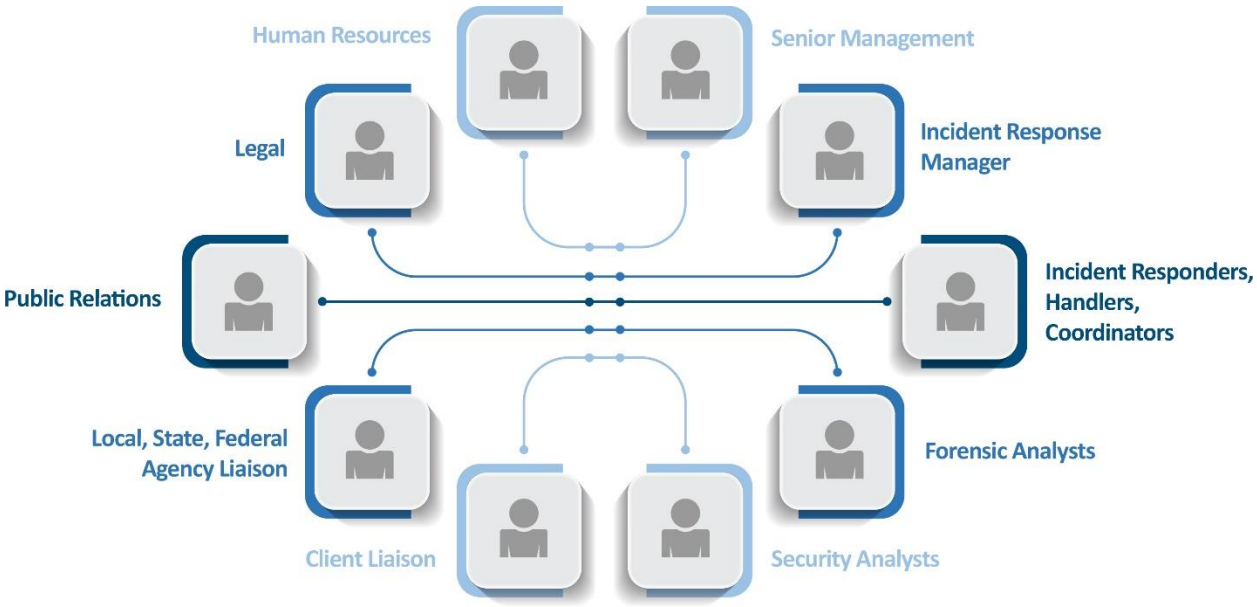
- Malicious or careless employees
- Malware (computer viruses, worms, trojan horses, most rootkits, spyware, and other malicious and unwanted software)
- Social engineering
- Ransomware
- Spam
- Spoofing and phishing
- Denial of service
- Distributed denial of service
- Man-in-the-middle attacks.
- Additional network attacks, including hacking and other common attack vectors.
- Physical and environmental conditions resulting in threats to the organization's Information Systems
- And many others

Again, the following list is just a small example of the large – and growing – threats facing organizations today (We'll get into a bigger list later). And while users who are proficient in I.T. (i.e., system administrators, network administrators, etc.) have a strong technical understanding of such threats, the large majority of employees within an organization unfortunately do not. Even more reason for learning about these threats - which is why you're undertaking training!

Unfortunately, user error by careless or untrained employees can often be the single source for a security incident that goes from bad to worse. Good security awareness training courses will cover all the above security threats – and much more – and that's our goal.

Training Module 4 - Build A Capable, Skilled Incident Response Team

Proper preparation for incident response also means having highly skilled, competent, and well-trained security experts ready to respond at a moment's notice to any threats. Therefore, a documented Incident Response Team (IRT) must be developed, one with clear roles and responsibilities for properly responding to any incident. Remember, preparation in terms of having the right people at the right place - at the right time - is just as important as the response to an actual incident.



As such, your IRT should consist of the following assigned titles and respective roles and responsibilities:

Senior Management:

- The designated individual(s) who will be the most important public face of the organization in relation to the security incident.
- Directly deliver critical public announcements.
- Having primary responsibility for mandatory breach reporting to regulators.
- Looked upon for leadership and direction in a time of crisis.
- Actively reaffirm the corporate values and culture of the business as the security incident unfolds.

Incident Response Manager:

- Responsibility and authority for oversight of any suspected or actual incident that does arise.
- Assessing severity of incident and assembling appropriate team members to act.
- Gathering all necessary information from subject matter experts.
- Making essential decisions on all phases of incident response.
- Act as the lead voice, internally, in regard to communications for all essential decisions on all phases of the incident lifecycle.
- Coordinating and directing all aspects of the incident response efforts, from initial incident alert to final resolution and post-incident reporting activities.

Incident Responders/Handlers/Coordinators:

- Collect intrusion artifacts (e.g., source code, malware, trojans) and use discovered data to enable mitigation of potential cyber defense incidents within the organization.
- Coordinate and provide expert technical support to organizational-wide cyber defense technicians to resolve cyber defense incidents.
- Coordinate incident response functions.
- Monitor external data sources (e.g., cyber defense vendor sites, Computer Emergency Response Teams, Security Focus) to maintain a strong awareness of cyber defense threat conditions and determine which security issues may have an impact on the organization.
- Perform cyber defense trend analysis and reporting.
- Perform initial, forensically sound collection of images and inspect to discern possible mitigation/remediation on organizational systems.
- Receive and analyze network alerts from various sources within the organization and determine possible causes of such alerts.
- Write and publish after-action reviews.
- Write and publish cyber defense techniques, guidance, and reports on incident findings to appropriate constituencies.

Forensic Analysts:

- Conduct analysis of log files, evidence, and other information to determine best methods for identifying the perpetrator(s) of a network intrusion.
- Confirm what is known about an intrusion and discover new information, if possible, after identifying intrusion via dynamic analysis.
- Provide technical summary of findings in accordance with established reporting procedures.
- Examine recovered data for information of relevance to the issue at hand.
- Perform file signature analysis.
- Perform file system forensic analysis.
- Collect and analyze intrusion artifacts (e.g., source code, malware, and system configuration) and use discovered data to enable mitigation of potential cyber defense incidents within the organization.

Security Analysts:

- Monitor computer networks and systems for threats and security breaches.
- Install, alter, and update security software and firewalls.
- Test systems for potential vulnerabilities.
- Develop systems and processes for security best practices throughout the organization.
- Prepare reports on security incidents and changing responses.

Human Resources:

- Provide guidance as to how best to handle situations involving employees for a given incident.
- To advise on policies that were violated or that must be adhered to, before taking any action on the employee.

Legal:

- Maintaining the confidentiality of the incident investigation.
- Protecting applicable internal communications under the attorney-client privilege and work product protections.
- Anticipating and preparing for litigation and other legal risks.
- Assist in identifying legal obligations following any data incident, including any notification requirements.
- Initiate and drive many of the actions needed to gather, secure, and analyze the data breach.
- Oversee overall legal work involved, and coordinate, manage and advise other external parties involved in the incident response team.

Public Relations:

- Oversee both internal and external incident response communication throughout the incident lifecycle.
- Determine which communication channels will be used for the respective audiences.
- Ensure that the incident response team, the organization, external stakeholders, customers, and the public are properly informed.

Local/State/Federal Agency Liaison:

- Maintain an up-to-date database on all relevant law enforcement agencies.
- As necessary, coordinate all communication efforts with law enforcement agencies.

Client Liaison:

- Work specifically with any clients that have been impacted by the incident.
- Maintain effective dialogue in terms of keeping clients abreast of various aspects of the incident.

Training Module 5 - Incident Response Detection

Detecting an incident requires a true commitment by all employees to be constantly aware of their surroundings for any type of social engineering, physical or environmental threats. Additionally, detection also requires due diligence and consistency by authorized employees regarding the secure configuration and review of network and system logs, being aware of network traffic anomalies and any suspicious or disruptive network patterns or incidents. Employees responsible for reviewing network and system logs (firewalls, routers, switches, IDS/IPS, operating systems, applications, databases, etc.) are, as a result of these reviews, to report any malicious, suspicious or disruptive event immediately to the Incident Response Team.