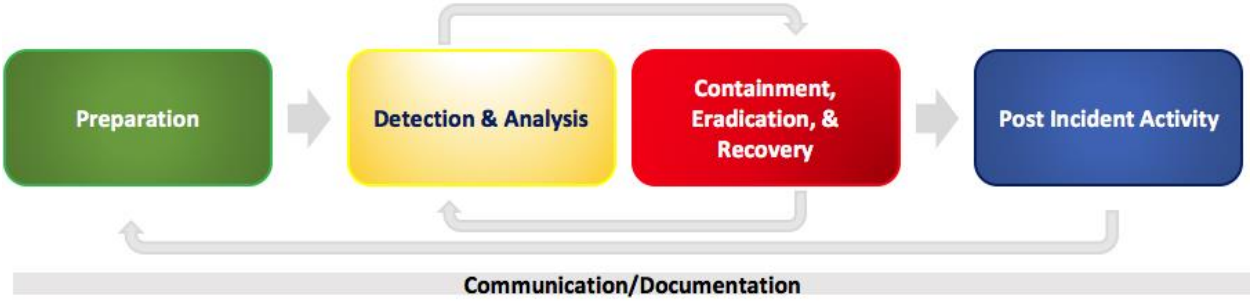
NATIONAL CAPITAL REGION THREAT INTELLIGENCE CONSORTIUM
Cyber Center
Cyber Advisory

# The NTIC Cyber Center Guide for Cyber Incident Response Planning

TLP: **WHITE** | This guide is provided to assist organizations in preparing for a cyber-attack that could negatively impact the confidentiality, integrity, or availability of their data. Implementing a comprehensive cyber incident response plan can greatly aid organizations by minimizing damage to equipment and reducing disruption to business operations. The following is an introduction to the four phases of the Cybersecurity Incident Lifecycle, which characterizes the continuous efforts organizations make to handle incidents and ensures continuous improvements in their overall security posture.




1. **Preparation**
   - Develop an incident response policy, approved by the highest level within your organization, that contains the following key elements:
     - Statement of management commitment
     - Purpose and objectives
     - Scope (to whom and what it applies and under what circumstances)
     - Definitions of computer security incidents and related terminology
     - Organizational structure and definition of roles, responsibilities, and level of authority
     - Prioritization or severity ratings of incidents
     - Performance measures
     - Reporting and contact forms
   - Develop standard operating procedures (SOPs) based on your incident response policy and relative to the specific technical processes, techniques, checklists, and forms to be used by your cyber security incident response team (CSIRT).
   - Assign staff to your organization's CSIRT, ensuring that each staff member acknowledges and understands your organization's policy and procedures relevant to his or her role and level of authority within the team.
     - In addition to core members responsible for directly responding to incidents, CSIRTs should also include technical subject matter experts, IT support staff, legal counsel, human resources, public relations staff, and senior management. *Smaller organizations that choose to outsource some or all of the CSIRT roles to an incident response provider should still maintain an internal policy and plan for early stage incident response before the provider's team arrives.*
     - Designate an incident leader who has primary accountability for coordinating all response efforts.
   - Coordinate communication and information sharing between your CSIRT and internal parties, such as management and employees within your organization, and external parties, such as law enforcement, information sharing partners, hardware & software vendors, other impacted organizations, and the media. Establish points of contact with all relevant parties ahead of time and include this information in your incident response plan.
   - Create an incident response checklist that will guide your CSIRT effectively and ensure that no steps are accidentally omitted during an incident.

- Identify and acquire tools and resources to be used by your CSIRT during an incident including checklists, chain of custody forms, hardware, software, storage facilities, and evidence gathering accessories.
- Classify incidents by threat types and severity to assist in the prioritization and scope of response efforts.
- Identify the types of data your organization stores and where it is located, including key assets that may be targeted in an attack.
- Identify critical processes and develop a plan to ensure continuity during an incident.
- Establish redundant systems and back up critical data often, storing backups off the network and testing them regularly to ensure integrity and accessibility to reduce recovery times.
- Establish a network performance baseline to better identify anomalies and recognize suspicious activity during the detection & analysis phase.
- Create and include a log retention policy as part of your incident response plan.
- Audit all network user accounts to better identify unauthorized access.
- Identify and inventory all devices on your organization's network to better identify rogue and potentially malicious and unauthorized activity.
- Train all levels of staff on cybersecurity best practices, indicators of compromise (IoCs), and current cyber threats, along with how to report an incident.
- Regularly conduct tabletop exercises to ensure understanding of current procedures.

**2. Detection & Analysis**

- Identify precursors to, and indicators of, a cyber incident. This information can be obtained through a variety of active and passive monitoring tools such as intrusion detection systems (IDS), intrusion prevention systems (IPS), security information and event management (SIEM) products, antivirus and antimalware software, file integrity monitoring tools, system event logs, and network device logs.
- Maintain a working knowledge of the current cyber threat landscape and awareness of current IoCs through automated indicator sharing (AIS) to quickly identify and block new and emerging threats.
- Perform event correlation across multiple logs to validate the occurrence of an incident.
- Begin documenting all data regarding an incident from the moment it is detected.
- Notify appropriate personnel of the confirmed incident as outlined in your incident response policy.

**3. Containment, Eradication, & Recovery**

- Isolate the impacted system(s) or device(s) from the network to prevent the threat from spreading.
- Gather and preserve evidence using sound forensic techniques. Collect identifying information of impacted systems and devices as well as all individuals who handled the evidence and where the evidence is stored.
- Remove any and all artifacts of the incident. Remove malicious code from impacted systems, sanitize compromised media, and secure compromised user accounts via password resents and implementation of multi-factor authentication.
- Perform a root cause analysis of the incident.
- Restore normal operations and adjust network and system security controls accordingly. Clean, rebuild, patch, and test affected systems, reconfigure firewall rulesets, and update malware signatures.

**4. Post-Incident Activity**

- Revert back to original change control processes and document any changes made during incident response.
- Conduct lessons-learned sessions for everyone involved in the response effort to highlight deficiencies in current procedures and improve response and recovery times for future incidents.
- Develop a formal after-action report that includes the chronology of events, root cause, location and description of collected evidence, specific actions taken by the CSIRT, the estimated impact on the organization and stakeholders, results of recovery efforts, and issues identified during the incident review.