Cybersecurity Incident Response Background

A security incident response plan defines the steps needed to prepare for, detect, contain, and recover from a cybersecurity incident. If you can invest time in the planning and practice stages, the effort will pay-off multiple times over in the unfortunate situation of having to execute.

An incident is any irregular, adverse, or unauthorized activity that occurs within any part of the organization's technology infrastructure. This includes unauthorized probing, browsing, and disruption which could cause any adverse effects on the information system. A security incident is an incident or series of incidents that violate the security policy. Security incidents include penetration of computer systems, exploitation of technical or administrative vulnerabilities, and introduction of computer viruses or other forms of malicious code.

Common Information that must be protected from unauthorized disclosure or public release based on state or federal law or other legal agreement. This includes any communication or record (whether oral, written, electronically stored, or transmitted, or in any other form) that consists of or includes any or all the following:

- Federal Tax Information sourced from the Internal Revenue Service (IRS) under an IRS data sharing agreement with the agency.
- Personal Identifying Information.
- Sensitive Personal Information.
- Protected Health Information, whether electronic, paper, secure, or unsecure.
- Social Security Administration data sourced from the Social Security Administration under a data sharing agreement with the agency.
- All non-public budget, expense, payment, and other financial information.
- All privileged work product.
- Information made confidential by administrative or judicial proceedings.
- All information designated as confidential under the laws of the State of South Dakota and of the United States, or by agreement.
- Information identified in a contract or data use agreement to which an agency contractor specifically seeks to obtain access for an authorized purpose that has not been made public.

Organizations must be aware of SDCL 22-40-20, Notice of Breach of security system.
https://sdlegislature.gov/Statutes/Codified_Laws/2047703

This document provides samples of

1. Incident Classification scheme.
2. Technical Infrastructure information to document ahead of time.
3. Key contacts to document ahead of time.
4. Incident Response Planning considerations.
5. Incident Response Checklist to be used in case of a real event.
6. Incident Response Report to use as an after-incident document.

The documentation can be used in a manner to customize for your organization.

Cybersecurity Incident Response Background

More information for understanding the importance and details of an Incident Response plan can be found at **https://www.cisa.gov/uscert/ncas/current-activity/2021/11/16/new-federal-government-cybersecurity-incident-and-vulnerability**

The standardized processes and procedures described:
• Facilitate better coordination and effective response among affected organizations,
• Enable tracking of cross-organizational successful actions,
• Allow for cataloging of incidents to better manage future events, and
• Guide analysis and discovery.

The template is designed for incidents that involve confirmed malicious cyber activity for which a major incident has been declared or not yet been reasonably ruled out.
For example:

- Incidents involving ransomware, lateral movement, credential access, exfiltration of data.
- Network intrusions involving more than one user, application, or system.
- Compromised administrator accounts.

The template does not apply to activity that does not appear to have such major incident potential, such as:

- "Spills" of classified information or other incidents that are believed to result from unintentional behavior only
- Users clicking on phishing emails when no compromise results
- Commodity malware on a single machine or lost hardware that, in either case, is not likely to result in demonstrable harm to the national security interests, foreign relations, or economy of the United States or to the public confidence, civil liberties, or public health and safety of the American people.

Prepare for major incidents *before they occur* to mitigate any impact on the organization. Preparation activities include:

- Educating users on cyber threats and notification procedures.
- Documenting critical aspects and details of the infrastructure.
- Prioritize systems and applications to be restored.
- Documenting key players to contact.
- Building the infrastructure within the technology environment to detect suspicious and malicious activity.
- Leveraging cyber threat intelligence (CTI) to proactively identify potential malicious activity
- Identify what I/T log resources are available and where they are stored.
- Create a "core" Incident Response team. Identify those key individuals who will participate in the response from a leadership and technical response perspective.
- Building and practicing an incident response plan.

Cybersecurity Incident Response Background

Generally, here are the steps taken during an incident.

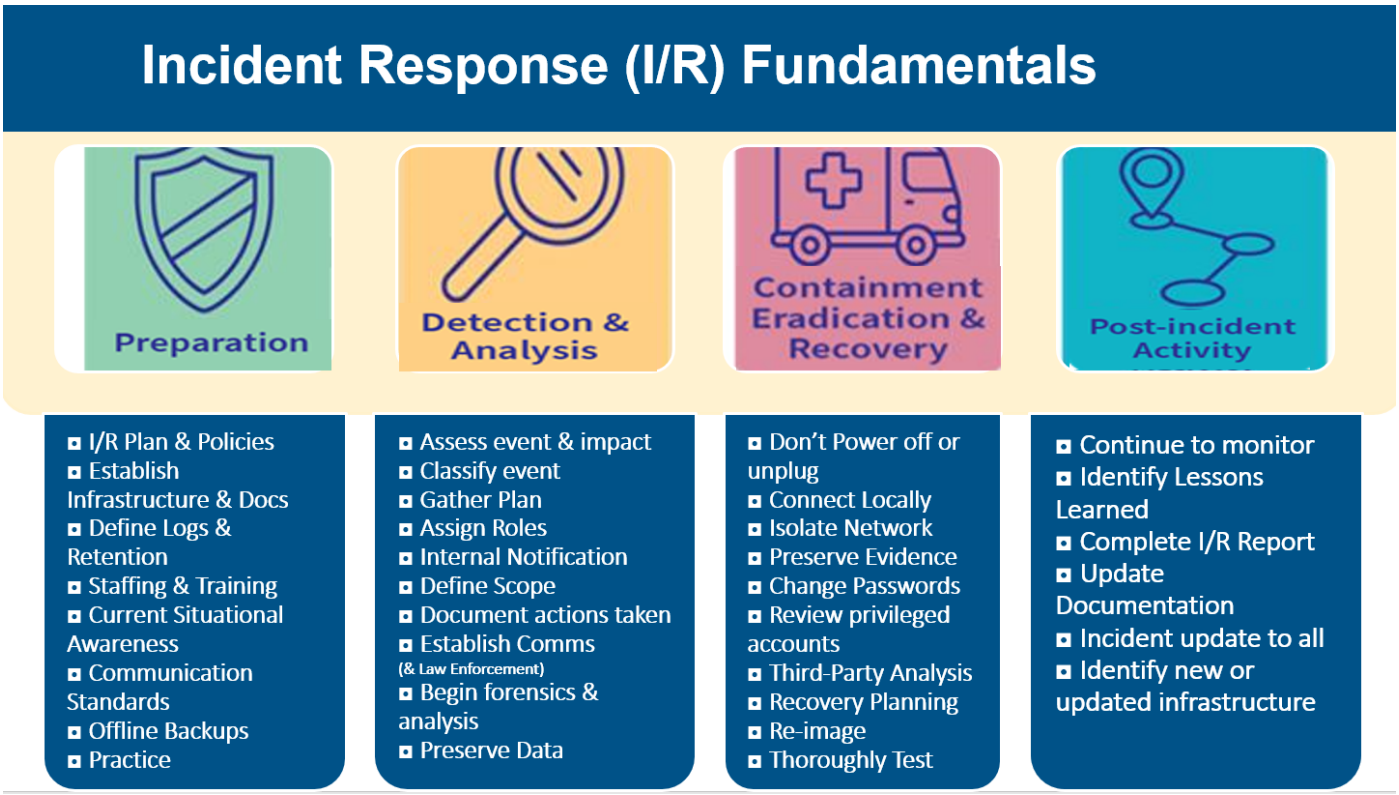
- A security event occurs, and a notification comes to the organization. Notification can occur internally from employees, contractors, vendors, customers, state, or federal resources.
- A technology staff reviews the security event.
- Basic technical details to be gathered:
    - Background of the alert.
    - What does the message say? Screenshot or picture of message.
    - What device(s) are impacted
    - What information is impacted
    - Who is impacted?
    - How many systems are impacted?
    - Type of event
    - Timelines of the event
- Analysis occurs of the known factors. This analysis could range from minutes to hours.
- The analyst makes a preliminary determination of the Prioritization (Critical, High, Medium, Informational).
- If a Critical or High priority is determined, then a security incident has been discovered and continue through the defined process.
- Documentation throughout the process is critical to maintain the history of actions.
- Assignment of responsibilities so individuals know the roles they are expected to perform.
- Communication with all interested parties is essential. Identify the communications tools & methods will be utilized. Email, texting, collaboration tools, etc. Define the intervals communications are to be delivered team wide.
- The incident is worked to isolate the impact, restore services, and hopefully identify the root cause.
- Finally – practicing Incident Response activities with staff is critical to remain calm during an actual incident.

The tables, checklists and procedures herein are designed for you to edit to meet your organizations specifics needs.

Cybersecurity Incident Response Background

Initially, you must determine what qualifies as an incident for your organization. There's a wide scope of events in the cybersecurity space. Some are minor, others are very significant.

Event Classification	Priority Characteristics (Examples)
4: *INFORMATIONAL*	**Low Risk – No Vulnerability. Event.** • No action required. • No measurable effect identified. • Information of interest has been discovered or shared.
INCIDENT (Below this line)	
3: *MEDIUM*	**Low Risk – Low Vulnerability. Minor Incident** • Negligible effect on one or more business units. • Virus/Malware/Phishing/Account reset which affects less than _ workstations • A single application has been compromised. • Exercising the entire Incident Response process is optional.
2: *HIGH / SEVERE*	**High Risk – Medium Vulnerability. Major Incident.** • Non-public information has been compromised. • Critical organization-wide infrastructure is impacted. Requires immediate action from involved parties. • Any Ransomware event or Virus/Malware which affects __ or more workstations
1: *CRITICAL / Organization-Wide*	**Critical Risk – Great Vulnerability. Major Incident** • Personally Identifiable or Health Information or other confidential information has been compromised. • County-wide services are impacted. • Virus/Malware or Ransomware which affects more than __ workstations


Incident Response (I/R) Fundamentals
Preparation
Detection & Analysis
Containment Eradication & Recovery
Post-incident Activity
I/R Plan & Policies
Establish Infrastructure & Docs
Define Logs & Retention
Staffing & Training
Current Situational Awareness
Communication Standards
Offline Backups
Practice
Assess event & impact
Classify event
Gather Plan
Assign Roles
Internal Notification
Define Scope
Document actions taken
Establish Comms
(& Law Enforcement)
Begin forensics & analysis
Preserve Data
Don't Power off or unplug
Connect Locally
Isolate Network
Preserve Evidence
Change Passwords
Review privileged accounts
Third-Party Analysis
Recovery Planning
Re-image
Thoroughly Test
Continue to monitor
Identify Lessons Learned
Complete I/R Report
Update Documentation
Incident update to all
Identify new or updated infrastructure

Key Technical Information to document.

Where can this information be securely stored in case network access is not available?

Security Asset	Description	IP Address	Name or Domain Name
I/T Infrastructure			
Network Diagram			
Domain Controller(s)			
Other Servers			
Firewall			
Router			
Intrusion Detection \ Prevention			
Domain Name Server			
VPN Appliance			
Web Server			
Email Server			
File Server			
Database Server			
Print Servers			
Printers			
Copiers			
Business Software Applications (list all)			

Cybersecurity Incident Response Background

Security Asset	Description	IP Address	Name or Domain Name
Logs retained			
Log locations			
Backup resources			
Network Switches			
Wireless Controller			
Wireless Access Points			
Telephone System Controller			
Workstation Inventory			
Directory Details			
Key Account information			

Cybersecurity Incident Response Background

Security Asset	Description	IP Address	Name or Domain Name
O\T Infrastructure			
Network Diagram			
Historian			
Data Acquisition Server			
Database Server			
Configuration Server			
Engineering Workstations			
Control Room Workstations			
Network Switches			
Firewalls			
Communications hardware			
Sensors			

Cybersecurity Incident Response Background

Key Contacts (Prioritize in order of contacting)

Name	Phone Numbers (Office, Cell, Home)	Email (organizational & personal)	Role
I/T Staff			
I/T Contractors			
I/T Vendors			
I/T Security Vendors			
County Auditor			
Staff \ Employees			
County Emergency Manager			
Legal Counsel			
Finance Officer			
Other Key County Staff			
Cyber Insurance Agent & Carrier			
Commissioners			
Communications / Press Director			
Internet Service Provider			
State Officials			
Local Law Enforcement			
Local Hospital \ Clinic			

Cybersecurity Incident Response Background

Name	Phone Numbers (Office, Cell, Home)	Email (organizational & personal)	Role
Cybersecurity & Infrastructure Security Agency	888-282-0870	central@CISA.DHS.gov Jim.edman@cisa.dhs.gov	
Federal Bureau of Investigation	855-292-3937	cywatch@ic.fbi.gov	
South Dakota Fusion Center	866-466-5263		
Bureau of Information & Telecommunications			
Federal Health & Human Services (HIPAA)			
Federal CJIS			
Other Regulatory Agencies			
FirstNet Subscriptions			

Cybersecurity Incident Response Background

Next is an Incident Response Planning guide. It can walk you through the steps for defining your Incident Response Plan. Those steps include:

1. Policies and Procedures
2. Instrumentation
3. Train Response Personnel
4. Cyber Threat Intelligence
5. Active Defense
6. Communications and Logistics
7. Operational Security
8. Technical Infrastructure
9. Detect Activity

Incident Response Planning

Step	Incident Response Preparation	Action Taken	Date
1. Policies and Procedures			
a. Document Incident Response plan with procedures for escalating and reporting major incidents and those with impact on agency mission.			
b. Document procedure for designating incident coordination lead.			
c. Identify key incident response personnel and responsibilities. Provide point of contact names, roles, phone numbers, and email addresses. (See Key Contacts table)			
d. Identify system and application owners (See Key Technical Information table for 1d. 1e.)			
e. Identify system IPs, system security plan, system/enclave boundaries, mission essential status, etc. Network diagrams.			
f. Document contingency plan for additional resourcing or "surge support" with assigned roles and responsibilities.			
2. Instrumentation			
a. Implement detection and monitoring capabilities to include anti-virus, endpoint detection and response, data loss prevention, intrusion detection – intrusion prevention systems, logs, net flows, packet captures and security information and event management (SIEM) systems to provide accurate picture of infrastructure (systems, networks, cloud			

platforms, and contractor-hosted networks).			
b. Establish a baseline for systems and networks to understand what "normal" activity is to enable defenders to identify any deviations.			
c. Implement EINSTEIN capabilities.			
d. Implement continuous diagnostic and mitigation capabilities.			
e. Identify logging requirements including log retention and log management requirements (state and federal).			
3. Train Response Personnel			
a. Train and exercise agency and staffing personnel to prepare for major incidents.			
b. Conduct recovery exercises to test full organizational Continuity Of Operations Planning (failover/backup/recovery systems).			
4. Cyber Threat Intelligence			
a. Monitor intelligence feeds for threat or vulnerability advisories from a variety of sources: government, trusted partners, open source, and commercial entities. Subscribe to MS ISAC and CISA information feeds. https://www.cisecurity.org/ms-isac/			
b. Integrate threat feeds into SIEM and other defensive capabilities to identify and block known malicious behavior.			
c. Analyze suspicious activity reports from users, contractors, service providers; or incident reports from other internal or external organizational components.			
d. Collect incident data (indicators, TTPs, countermeasures) and			

share with CISA and other partners (law enforcement, etc.). Intelligence Sharing service.			
e. Set up CISA Automated Indicator Sharing (AIS) or share via Cyber Threat Indicator and Defensive Measures Submission System. https://www.cisa.gov/ais			
5. Active Defense			
a. For those with advanced capabilities and staff, establish active defense mechanisms (i.e., honeypots, honeynets, honeytokens, fake accounts, etc.,) to create tripwires to detect adversary intrusions and to study the adversary behavior to understand more about their tactics, techniques & procedures.			
6. Communications & Logistics			
a. Establish a communications strategy. This includes: • Identify key contacts • Defining an out-of-band email communication protocol • Designating a war room • Establishing a comm channel (Teams, WebEx, Adobe, Signal, phone bridge or chat room)			
b. Establish procedures mechanisms for coordinating major incidents with CISA.			
c. Designate CISA reporting Point of Contact (POC). Provide POC name, phone number and email address. Implement info sharing format and platform to CISA.			
d. Define methods for handing classified, personally identifiable information, personal health information, other sensitive information, and data, if required.			
7. Operational Security			

a. Segment/manage Security Operations Center systems separately from broader enterprise IT systems. Manage sensors and security devices via out-of-band means (network, etc.).			
b. Develop method to notify users of compromised systems via phone rather than email			
c. Use hardened workstations to conduct monitoring and response activities.			
d. Ensure defensive systems have robust backup and recovery processes.			
e. Implement processes to avoid "tipping off" an attacker to reduce likelihood of detection of IR-sensitive information (e.g., do not submit malware samples to a public analysis service or notify users of compromised systems via email).			
8. Technical Infrastructure			
a. Establish secure storage (i.e., only accessible by incident responders) for incident data and reporting.			
b. Implement capabilities to contain, replicate, analyze, and reconstitute compromised hosts.			
c. Deploy tools to collect forensic evidence such as disk and active memory imaging.			
d. Implement capability to handle/detonate malware, sandbox software, and other analysis tools.			
e. Implement a ticketing or case management system.			
9. Detect Activity			
a. Implement security information and event management and sensor rules and signatures to			

search for indicators of compromise.			
b. Analyze logs and alerts for signs of suspicious or malicious activity			

Following is an Incident Response Checklist. A template to use during an actual Incident to systemically follow appropriate steps and actions. Those steps include:

1. **Detection & Analysis**
    a. Receive, identify, and assess the incident report
    b. If multiple reports are received, conduct a hasty prioritization process.
    c. Locate and implement the Incident Response Plan.
    d. Begin internal notification to key contacts
    e. Begin external notification to appropriate leadership, staff, directorates, etc.
    f. Begin thorough documentation process.
    g. Begin gathering evidence.
2. **Containment**
    a. Follow guidance from Technology staff \ consultant.
    b. Do not power off or unplug affected system(s) from the network until advised to do so unless there is obvious destruction to the system or the network taking place at the time.
    c. Do not attempt to identify or track-down the attacker.
    d. Do not connect remotely to affected system(s).
    e. Isolate network segments if needed, required, or advised.
    f. Assist and collaborate with investigating officials as needed or required.
3. **Eradication & Recovery**
    a. Continue following guidance from Technology staff \ consultant.
    b. Use extreme care and caution to preserve any/all evidence.
    c. Mitigate all vulnerabilities as directed.
    d. Change all administrative passwords.
    e. Review all privileged access credentials.
    f. When directed, allow affected end-user(s) to return to normal activity.
    g. When directed, return affected hardware system(s) to service.
    h. Implement additional monitoring as needed or directed.
    a. Conduct additional education and training as needed or directed.
    b. If required, employee discipline will be managed by organizational leadership.
4. **Post-Incident Activity**
    a. Complete an Executive Summary for internal and external leadership.
    b. Conduct a Lessons-Learned / Hotwash session with all parties involved.
    c. Update Incident Response Plan and other policies as needed.
5. **Coordination with CISA**

Incident Response Checklist

Step	Incident Response Procedure	Action Taken	Date
Detection & Analysis			
1. Declare Incident			
a. Perform Initial Categorization of Incident (Critical or High)			
b. Designate Incident Coordinator Lead			
c. Notify Communications Tree			
2. Determine Investigation Scope			
a. Identify type & extent of incident			
b. Assess Operational impact			
3. Collect & Preserve Data			
a. Collect & preserve the data necessary to for incident verification, categorization, prioritization, mitigation, reporting, attribution, and potential evidence. Do not blindly shut machines down or reboot them. Reference NIST-800-61r2.			
b. Log all evidence and note how the evidence was acquired,			
4. Perform Technical Analysis			
a. Develop a technical & contextual understanding of the incident.			
b. Based on analysis thus far and available cyber threat intelligence (CTI)			
c. Update scope as investigation progresses and information evolves. Report most recent findings and incident status to CISA.			

d. **Terminating condition:** Technical analysis is complete when the incident has been verified, the scope has been determined, the method(s) of persistent access to the network has/have been identified, the impact has been assessed, a hypothesis for the narrative of exploitation has been cultivated (TTPs and IOCs), and all stakeholders are proceeding with a common operating picture.			
Correlate Events & Document Timeline			
e. Analyze logs to correlate events and adversary activity.			
f. Establish an incident timeline that records events, description of events, date-time group (UTC) of occurrences, impacts, and data sources. Keep updated with all relevant findings.			
Identify Anomalous Activity			
g. Assess affected systems and networks for subtleties of adversary behavior which often may look legitimate			
h. Identify deviations from established baseline activity - particularly important to identify attempts to leverage legitimate credentials and native capabilities and tools (i.e., living off the land techniques).			
Identify Root Cause & Enabling Conditions			
i. Attempt to identify the root cause of the incident and collect threat information that can be used in further searches and inform subsequent response efforts.			
j. Identify and document the conditions that enabled the adversary to access and operate within the environment			
k. Assess networks and systems for changes that may have been			

made to either evade defenses or facilitate persistent access.			
l. Identify attack vector. This includes how the adversary accessing the environment (e.g., malware, RDP, VPN).			
m. Assess access (depth and breadth). This includes All compromised systems, users, services, and networks.			
Gather Incident Indicators			
n. Review available CTI for precedent of similar activity			
o. Analyze adversary tools. Assess tools to extract IOCs for short-term containment.			
p. Identify and document indicators that can be used for correlative analysis on the network.			
q. Share extracted threat information (atomic, computed, and behavioral indicators, context, and countermeasures) with internal response teams and CISA.			
Analyze for Common Adversary Tactics, Techniques and Procedures (TTPs)			
r. Identify initial access [Mitre Attack Tactic TA0001] techniques (e.g., spear phishing, supply chain compromise).			
s. If access is facilitated by malware, identify associated command and control [Mitre Attack Tactic TA0011] (e.g., identify port, protocol, profile, domain, IP address).			
t. Identify the techniques used by the adversary to achieve code execution [Mitre Attack Tactic TA0002].			
u. Assess compromised hosts to identify persistence [Mitre Attack Tactic TA0003] mechanisms			

v. Identify lateral movement [Mitre Attack Tactic TA0008] techniques. Determine the techniques used by the adversary to access remote hosts.			
w. Identify the adversary's level of credential access [Mitre Attack Tactic TA0006] and/or privilege escalation.			
x. Identify the method of remote access, credentials used to authenticate, and level of privilege. If access is by legitimate but compromised application (e.g., RDP, VPN), identifies the method.			
y. Identify mechanism used for data exfiltration [Mitre Attack Tactic TA0010].			
Validate and Refine Investigative Scope			
z. Identify new potentially impacted systems, devices, and associated accounts			
aa. Feed new IOCs and TTPs into detection tools.			
bb. Continue to update the scope and communicate updated scope to all stakeholders to ensure a common operating picture.			
5. Third-Party Analysis and Support			
a. Identify if third-party analysis support is needed for incident investigation or response. Is a third-party for intrusion detection and incident response support services needed?			
b. Does incident qualify for CISA incident response and hunt assistance?			
c. Coordinate and facilitate access if incorporating third-party analysis support into response efforts.			

d. Coordinate response activities with service providers for systems hosted outside.			
6. Adjust Tools			
a. Tune tools to slow the pace of advance and decrease dwell time by incorporating IOCs to protect/detect specific activity.			
b. Introduce higher-fidelity modifications to tools. Tune tools to focus on tactics that must be used by the adversary to obtain operational objectives (e.g., execution, credential access, and lateral movement).			
Containment			
7. Contain Activity (Short Term Mitigations)			
a. Determine Appropriate Containment strategy, including: ● Requirements to preserve evidence ● Availability of services (e.g., network connectivity, services continuity) ● Resource Constraints ● Duration of containment steps			
b. System backup(s) to preserve evidence and continued investigation.			
c. Coordinate with law enforcement to collect and preserve evidence (as required by (Step 3a) prior to eradication, if applicable.			
d. Isolate affected systems and networks including: • Perimeter containment • Internal network containment • Host-based/Endpoint containment • Temporarily disconnect public-facing systems from the Internet, etc.			
e. Close specific ports and mail servers. Update firewall filtering.			

f. Change system admin passwords, rotate private keys and service/application account secrets where compromise is suspected revoke privileged access.			
g. Perform blocking (and logging) of unauthorized accesses, malware sources, and egress traffic to known attacker Internet Protocol (IP) addresses.			
h. Prevent Domain Name Server (DNS) resolution of known attacker domain names.			
i. Prevent compromised system(s) from connecting to other systems on the network.			
j. Advanced SOCs may direct adversary to sandbox to monitor activity, gather additional evidence, and identify TTPs.			
k. Monitor for signs of threat actor response to containment activities.			
l. Report updated timeline and findings (including new atomic and behavioral indicators) to CISA.			
m. If new signs of compromise are found, return to technical analysis (Step 4) to re-scope the incident.			
n. **Terminating condition:** Upon successful containment (i.e., no new signs of compromise), preserve evidence for reference and law enforcement investigation (if applicable), adjust detection tools, and move to eradication.			
Eradication & Recovery			
8. Execute Eradication Plan			
a. Develop a well-coordinated eradication plan that considers scenarios for threat actor use of alternative attack vectors and			

multiple persistence mechanisms.			
b. Provide incident status to CISA & other entities until all eradication activities are complete.			
c. Remove artifacts of the incident from affected systems, networks, etc.			
d. Reimage affected systems from clean backups (i.e., 'gold' sources).			
e. Rebuild hardware (if rootkits involved).			
f. Scan for malware to ensure removal of malicious code.			
g. Monitor closely for signs of threat actor response to eradication activities			
h. Allow adequate time to ensure all systems are clear of threat actor persistence mechanisms (such as backdoors) since adversaries often use more than one mechanism.			
i. Update the timeline to incorporate all pertinent events from this step.			
j. Complete all actions for eradication.			
k. Continue with detection and analysis activities after executing the eradication plan to monitor for any signs of adversary re-entry or use of new access methods.			
l. If new adversary activity is discovered at the completion of the eradication step, contain the new activity and return to Technical Analysis (Step 4) until the true scope of the compromise and infection vectors are identified.			
m. If eradication is successful, move to Recovery.			

9. Execute Restoration Plan			
a. Restore agency systems to operational use: recovering mission/business data.			
b. Revert all changes made during incident.			
c. Reset passwords on compromised accounts			
d. Implement multi-factor authentication for all access methods.			
e. Install updates and patches.			
f. Tighten perimeter security (e.g., firewall rulesets, boundary router access control lists) and zero trust access rules.			
g. Test systems thoroughly (including security controls assessment) to validate systems are operating normally before bringing back online in production networks.			
h. Consider emulating adversarial TTPs to verify countermeasures are effective.			
i. Review all relevant CTI to ensure situational awareness of the threat actor activity.			
j. Update incident timeline to incorporate all pertinent events from Recovery step.			
k. Complete all actions for recovery.			
Post-Incident Activities			
10. Post-Incident Activities			
a. Document the incident, inform leadership, harden the environment to prevent similar incidents, and apply lessons learned to improve the handling of future incidents.			
Adjust Sensors, Alerts and Log Collection			

b. Add enterprise-wide detections to mitigate against adversary TTPs that were successfully executed.			
c. Identify and address operational "blind spots" to adequate coverage moving forward.			
d. Continue to monitor the agency environment for evidence of persistent presence.			
Finalize Reports			
e. Provide post-incident updates as required by law and policy.			
f. Publish post-incident report. Provide a step-by-step review of the entire incident and answer the Who, What, Where, Why, and How questions.			
g. Provide CISA with post-incident update with seven (7) days of resolution			
h. Work with CISA to provide required artifacts, and/or take additional response action.			
Perform Hotwash			
i. Conduct lessons learned analysis with all involved parties to assess existing security measures and the incident handling process recently experienced.			
j. Identify if Incident Response processes were followed and if they were sufficient.			
k. Identify any policies and procedures in need of modification to prevent similar incidents from occurring.			
l. Identify how information sharing with locals, CISA and other stakeholders can be improved during Incident Response.			
m. Identify any gaps in incident responder training.			

n. Identify any unclear or undefined roles, responsibilities, interfaces, and authorities.			
o. Identify precursors or indicators that should be monitored to detect similar incidents.			
p. Identify if infrastructure for defense was sufficient. If not, identify the gaps.			
q. Identify if additional tools or resources are needed to improve detection and analysis and help mitigate future incidents.			
r. Identify any deficiencies in the incident response planning process. If no deficiencies identified, identify how to implement more rigor in incident response planning.			
Coordination with CISA			
11. Coordination with CISA			
a. Notify CISA with initial incident report within 1 hour after incident determination.			
b. Receive incident tracking number and CISA National Cyber Incident Scoring System (NCISS) priority level from CISA.			
c. Comply with additional state or federal reporting requirements as mandated by state or federal policy			
d. Provide incident updates until all eradication activities are complete.			
e. Report incident updates to include: • Updated scope • Updated timeline (findings, response efforts, etc.) • New indicators of adversary activity • Updated understanding of impact • Updated status of outstanding efforts			

• Estimation of time until containment, eradication, and recovery are completed			
f. Share relevant atomic and behavioral indicators and countermeasures with CISA throughout the Incident Response process.			
g. Provide post-incident updates.			
h. Service providers and contractors who operate systems on behalf of your entity must promptly report incidents to you. Build that incident response requirements into your contracts and agreements.			

Lastly, following is a sample Incident Response Report that can be used to summarize the incident, actions taken and follow-up activities to be pursued.

Incident Response Report

Sample Incident Response Checklist					
Incident Information					
Incident Assessment	☐ Negligible ☐ Minor ☐ Significant ☐ Critical				
Incident #		**Date Reported:**		**Time Reported:**	
Agency/Dept		**Date of Incident:**		**Time of Incident:**	
Reporting Party:			**Title/Role:**		
Contact email:			**Contact Phone #**		
Responding Party:			**Title/Role:**		
Contact email:			**Contact Phone #**		
Contact Supervisor:	☐ Yes ☐ No	**Contact Information:**			
Contact Management:	☐ Yes ☐ No	**Contact Information:**			
Theft:	☐ Yes ☐ No	**Police Case Report #:** *(if applicable)*			
Investigator:			**Investigator Phone #:**		
Location:			☐Logical ☐Physical		
Compromised Systems – Detailed Information					
Number of devices affected	☐1 – 50 ☐ 51-100 ☐ 101-1000 ☐More than 100				
Computer name(s)					
IP Address(es)					
Operating System(s)					
Application software affected:					
Last time machine was patched:					

Incident Response Report

Functions of affected machines:	

Incident Summary

IP Address of Attacker	Destination Port/Protocols	Country of Attacker	Other Information

Initial Damage Assessment

Additional Information

Incident Details	
Type of Incident (Check all that apply)	
Malware	**Malware (continued)**
☐ Trojan	☐ Capture App Data
☐ Ransomware	☐ Capture Stored Data
☐ Worm	☐ Export Data
☐ Backdoor	☐ Remote Injection
☐ DoS	☐ Email attachment
☐ Downloader	☐ Email Link
☐ Password Dumper	☐ Other

Incident Response Report

Hacking ☐ Brute Force ☐ Web Application ☐ Backdoor ☐ Exploit Vulnerability ☐ Use of backdoor ☐ Other	**Misuse of Resources** ☐ Unauthorized Use of Software ☐ Privilege Abuse ☐ Inappropriate Use of Email ☐ Inappropriate Use of Internet ☐ Inappropriate Use of Company Resources ☐ Storage or Distribution of Unauthorized Software
Misuse ☐ Misconfiguration ☐ Privilege abuse ☐ Password Dumper	**Social Engineering** ☐Phishing ☐Pretexting ☐Baiting
Probes/scans ☐ Attempted Intrusion Reconnaissance Activity ☐ Other	**Other** ☐Other (please specify)

Optional: Below fields only apply if incident type is Malware			
Name(s) of Malware			
Vendor *(customize to your organization)*	☐Norton ☐ Trend Micro ☐ Malwarebytes ☐ McAfee ☐ Kaspersky ☐Webroot ☐Bitdefender ☐Avira ☐ Other _____		
Source IP Address:		**URL:**	
Resulting Impact or Damage			

Incident Response Report

Actions Taken:	☐System Taken Offline ☐Scanned/Cleaned ☐Reimaged ☐Analyzed ☐Submitted to Vendor for further analysis

Timeline of Incident Activities		
Date	**Time**	**Details (Describe chronological order of events)**

Analysis
Impact on IT services or resources
Response to Incident
Next Steps
Changes to be implemented

Current State of Incident	☐Active ☐Open ☐Closed

Evidence Chain of Custody Tracking			
Description of Evidence			
Date Seized:		**Time Seized:**	

Incident Response Report

Tag #	Date Received	Quantity	Description (Model, Serial #, Condition)

Chain of Custody

Tag #	Date Received	Released By (Signature)	Received By (Signature)	Comments

Communications Log

Description of Communications

Date	Time	Details *(Description of Communications: Phone, Emails, Text, In-person, etc.)*

Other Information

Additional Notifications	**If PII is involved, have affected parties been notified?**
☐ FBI ☐ CISA ☐ Human Resources ☐ Public Affairs ☐Legal Counsel ☐Other Agencies *(please specify)*	☐No ☐Yes *(please specify)*

Lessons Learned

Describe lessons learned and actions submitted to backlog to work

Report Information

Reporting Staff Signature		**Date**	
Supervisor Signature		**Date**	

Form Revisions (Internal Use Only)

Date Revised		Who Revised?	

Revision Description
