Company Logo

Info-Tech Research Group
Security, Risk & Compliance

Security Incident Management Plan

Last revised: MM/DD/YY

Security Incident Management Plan

Introduction: How to Use This Template

Use this template to outline the high-level response process to guide your incident responders in the event of a security incident. While runbooks will be created to handle specific incident types, this plan is used as a general-purpose guide to any incident's remediation.

To use this template, simply customize any text below to fit the needs of your organization. The grey text can be edited for your organization's specific details, but the black text can also be altered to best reflect your organization's processes. All content below is provided as an example.

Be sure to replace the header and footer with your organization's information.

Revision History

Version	Change	Author(s)	Date of Change
1.0	Initial Draft		

Supporting Documents

[Update this list as these documents are developed.]

- Security Incident Management Policy
- Security Incident Management RACI Tool
- Security Incident Response Interdepartmental Communications Template
- Security Incident Communications Guidelines
- Security Incident Runbooks:
    - Ransomware Runbook
    - Malware Runbook
    - Compromised Credential Runbook
    - Malicious Email Runbook
    - Distributed Denial of Service (DDoS) Runbook
    - Data Breach Runbook
- Post-Incident Analysis Report Template
- Security Incident Metrics Tool

Introduction

Purpose

The purpose of this document is to define a high-level incident response plan for any security incident. It is used to define general communication processes for managing security incidents, which may help minimize the impact and scope of the incident on the organization.

Defining standard incident handling protocols helps reduce ambiguity in the case of an incident and helps keep stakeholders accountable and aware of the incident.

This incident management plan will be regularly reviewed, evaluated, and updated as part of [Organization's] on-going security program. This also involves appropriate training of resources expected to respond to security incidents, as well as the training of general employees regarding [Organization's] expectations of them in regards to security responsibilities.

Definitions

Term	Definition
Security Event	Identified occurrence of a system, service, or network state indicating a possible breach of information security policy or failure of controls, including false alarms.
Security Incident	Single or series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security.
Managed Security Service Provider (MSSP)/Security Operations	An organization will either outsource or insource the monitoring of perimeter network, antivirus/malware solutions, proxy/email gateways, and SIEM events. Once an event been confirmed to be an incident, it will be escalated to threat intelligence, incident response, vulnerability management, or other teams (as appropriate).
Incident Responder	A member of an incident response team, which is established to handle the intake, communication, and remediation of security incidents. If there is no dedicated incident response team, staff responding to incidents when required may be referred to as "incident responders."
Threat Escalation Protocol (TEP)	Incidents should be assessed based on their impact on the organization and the scope of IT systems within the organization. The combination of these two factors will provide insight into the threat escalation protocol, indicating the types of stakeholders typically needed for those types of incidents.

Organizational Approach to Incident Response

As per incident management procedures, our organizational approach to incident response and management will follow the general guidelines in alignment with NIST SP 800-61 Rev. 2, which includes the following phases:

- Detection
- Analysis
- Containment
- Eradication
- Recovery
- Post-Incident Activities

Communication/Notifications

This program fits into the enterprise's overall incident management program by following similar procedural protocol. By adhering to similar processes across the board, we are able to maintain consistency and to ensure that responses are comprehensive, preventing as many potential incident information gaps as possible.

Communicating the incident both internally and externally (as needed) is an important part of this process. However, depending on the nature of the incident, communications may occur at different stages and are likely to

be necessary more than once to update stakeholder groups as new information becomes available during the incident response process.

As part of the incident management program, the following runbooks have been developed, which can be used to help plan communications strategies for each incident type:
[Customize to match your organization's runbooks. If your organization has not developed runbooks, be sure to consult Info-Tech's ***Develop and Implement a Security Incident Management Program*** blueprint.]

- Ransomware
- Malware
- Compromised Credentials
- Malicious Email
- Distributed Denial of Service (DDoS)
- Data Breach

Other incident types include [list runbook types that will possibly be developed within the next year or so]:

- Compromised Asset
- Denial of Service (DoS)
- Destruction/Loss of Property
- Insider Activity – Accidental
- Insider Activity – Malicious
- Unauthorized Access
- Unlawful Activity

Roles and Responsibilities

Individuals needed and responsible for responding to a security incident make up a security incident response team (SIRT), also known as the incident responders. Members may include the following [customize the list below]:

- End Users
- Help Desk
- MSSP/Security Operations
- Cybersecurity
- IT Operations
- CISO
- Legal, HR, PR
- Senior Management
- External

The RACI tool below is used to identify and avoid confusion in roles and responsibilities during an incident remediation. The acronym stands for:

- **Responsible.** The person(s) who does the work to accomplish the activity; they have been tasked with completing the activity, and/or getting a decision made.
- **Accountable.** The person(s) who is accountable for the completion of the activity. Ideally, this is a single person and is often an executive or program sponsor.
- **Consulted.** The person(s) who provides information. This is usually several people, typically called subject matter experts (SMEs).
- **Informed.** The person(s) who is updated on progress. These are resources that are affected by the outcome of the activities and need to be kept up to date.

The RACI tool is available for download on Info-Tech's website: *Security Incident Management RACI Tool*. Ensure there is a link or reference to a copy of the tool. Consider including a screenshot of the tool in an Appendix.

Incident Assessment

Incidents should be assessed based on their impact to the organization and the scope of IT systems within the organization. The combination of these two factors will provide insights necessary to develop an effective **TEP,** indicating the types of stakeholders typically needed for those kind of incidents.

Impact Criteria

Evaluate the impact on business functions, information, and recovery efforts. Overall incident impact should be assessed based on the *highest* impact level of the three incident types below: [To be modified to fit the member organization's needs – below is an example.]

1. **Functional impact:** The impact as it relates to the availability and delivery of services and business functions. Is a critical system affected? Does it hinder functionality for users?
2. **Information impact:** The impact as it relates to the confidentiality, integrity, and availability of the organization's data. What sensitivity of data is affected? What does it mean for the organization (e.g. notification requirements, regulatory fines)?
3. **Recoverability impact:** The time and resources required to recover from the incident. What needs to be done for recovery?

Table 1. Impact Criteria

[Customize the criteria based on the acceptable handling responses of your organization.]

Impact Criteria	
Rating	Definition (example)
High	There is a **high** impact if at least one of the following is true: • The organization is no longer able to provide some critical service(s) to any users and a critical business function cannot be performed OR • Regulated or highly sensitive data has been compromised. Regulatory actions may be required OR • Full recovery from the incident is not possible or will require significant external resources. There is severe reputational damage OR • Financial loss is $50,000 or greater.
Medium	There is a **medium** impact if at least one of the following is true and the impact was **not** high: • The organization is no longer able to provide some secondary services to any users OR • The organization is no longer able to provide some critical services to a subset of users, but a workaround is available OR • Sensitive/confidential data has been exposed, but no regulatory actions are required OR • Recovery from the incident is possible, but requires additional resources (e.g. overtime) OR • Financial loss is between $10,000 to $50,000.
Low	There is **low** impact if at least one of the following is true and the impact was not high or medium: • The organization is experiencing minimal effects to services. All services are available, but efficiency has been affected OR • Public data has been affected, but no regulatory actions or penalties are required OR • Recovery from the incident is possible and predictable with existing processes OR • Financial loss is less than $10,000.
None	There is **no** impact if all of the following are true (e.g. false alarm; not a true security incident): • There is no effect to the organization's ability to provide service to users AND • No information was exposed or affected in an unauthorized manner AND • No significant recovery time or resources are required AND • Financial loss is negligible.

Scope Criteria

Evaluate the scope (i.e. breadth/magnitude) of the incident on systems, users, endpoints, etc. Incident scope is a critical component that aids in decision making throughout the incident management process. [To be modified to fit the member organization's needs – below is an example with arbitrary numbers.]

Table 2. Scope Criteria

[Customize the criteria based on the acceptable handling responses of your organization.]

Scope Criteria	
Rating	Definition
High	>99 individuals, systems, or processes affected AND/OR 1+ server was compromised, AND/OR 1+ executive was targeted, AND/OR >9 sensitive records exposed, AND/OR a crime was committed.
Medium	11-99 individuals, systems, or processes affected AND/OR 1-9 sensitive records exposed.
Low	<10 individuals, systems, or processes affected.

Threat Escalation Protocol

A TEP outlines the types of stakeholders needed during the incident management process. Informing and consulting these stakeholders during the incident management process is crucial when defending the organization against incidents. A threat escalation protocol clearly defines escalation procedures for incidents. [To be modified to fit the member organization's needs – below is an example. **All colors and tier levels can be changed.**]

Table 3. Threat Escalation Protocol

Threat Escalation Protocol (TEP)			
Impact	Scope		
	High	Medium	Low
High	Tier 1	Tier 1	Tier 2
Medium	Tier 1	Tier 2	Tier 2
Low	Tier 2	Tier 2	Tier 3

Threat Escalation Protocol (TEP)	Criteria	Stakeholders
TEP Tier 1	• High impact, high scope • High impact, medium scope • Medium impact, high scope	• End User • Help Desk • Cybersecurity • IT Operations • CISO • Legal, HR, PR • Senior Management • External Third Parties

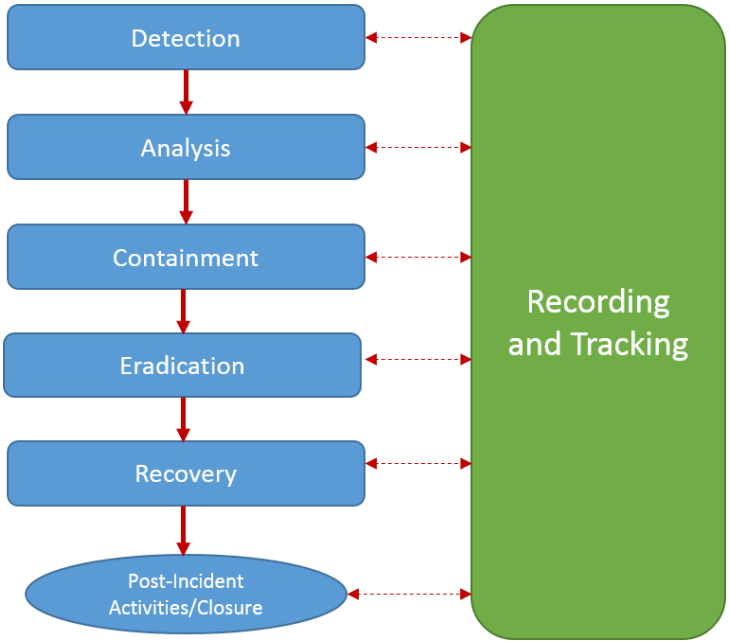
TEP Tier 2	• High impact, low scope • Medium impact, medium scope • Medium impact, low scope • Low impact, high scope • Low impact, medium scope	• End User • Help Desk • Cybersecurity • IT Operations • CISO
TEP Tier 3	• Low impact, medium scope • Low impact, low scope	• End User • Help Desk • Cybersecurity

Process

High-Level Process Workflow Diagram

Insert your high-level process workflow diagram below.

Example:



Response Procedures

The actions required to deal with incidents are detailed below for each relevant stakeholder (team), in each of the six phases (detection, analysis, containment, eradication, recovery, and post-incident activities).

Detection Phase

During the detection phase, teams evaluate a potential security incident. Once an incident has been detected, a help desk ticket or incident record/ticket is opened to initiate the detection phase.

Incident triggers can include:

1. End users reporting to help desk
2. Technology trigger (FW, IDS/IPS, etc.)
3. Pen tests (vulnerability management)
4. Hunt function (threat intel)
5. Notify by law enforcement or by ISAC

Technologies involved in this phase include:

[Customize this list to your organization's detection technologies.]

- Firewalls
- IDS/IPS
- Web proxy
- Antivirus
- Anti-malware
- Email gateway
- SIEM
- DLP
- UBA
- Vulnerability scanners

Team	Description	Questions	Action
Detection: End User	During the detection phase, the end user may report suspicious behaviors or issues and system/service disruptions.	• Did I receive a suspicious email? • How do I resolve the issue with my endpoint? • Why is a system or service not available or behaving abnormally? • Is my device possibly lost or stolen? • Why can't I access my data or account?	☐ Report a suspected incident or issue to help desk. Examples include: ○ Data is missing/altered. ○ Passwords aren't working. ○ Experiencing significant number of pop-up ads. ○ Computer keeps crashing. ○ Account/network cannot be accessed.
Detection: Help Desk	During the detection phase, help desk staff will monitor calls and submitted tickets.	• Are any end users experiencing potential security incidents?	☐ Open a help desk ticket. (see Appendix for examples of information to be included in a help desk ticket.) ☐ Determine if incident needs to be escalated to other stakeholders. ☐ Assign help desk ticket to appropriate team and/or begin the Analysis phase.

Detection: MSSP/Security Operations Note: This section is to be filled out if there is an MSSP and/or a security operations team. Some of the cybersecurity team responsibilities may fall into here as well.	During the detection phase, MSSP/security operations staff monitor firewall, IDS/IPS, web proxy, antivirus, anti-malware, email gateway, SIEM, DLP, UBA, and other **events,** and escalate to **incidents** to the cybersecurity team.	• Are any security events being identified through a technology or user?	☐ Answer inbound security-related calls. ☐ Investigate and respond to security events. ☐ Establish cases through the use of a ticketing system. ☐ Handle security-related user complaints and queries. ☐ Escalate according to established procedures. ☐ Review events from sources such as a firewall, IDS/IPS, web proxy connections, antivirus, anti-malware, email gateway, SIEM logs, or other security technologies.
Detection: Cybersecurity	During the detection phase, cybersecurity staff monitor firewall, IDS/IPS, web proxy, antivirus, anti-malware, email gateway, SIEM, DLP, UBA, and other **events,** and escalate to **incidents** as needed.	• Are assets or services being impacted by a security incident? • Has data been exposed or exfiltrated? • Has an executive been targeted or affected by a security incident? • Are security technologies identifying one or a series of events?	☐ Identify suspicious behavior of assets or services. ☐ Review events from sources such as a firewall, IDS/IPS, DLP, web proxy connections, antivirus, anti-malware, email gateway, SIEM logs, or other security. ☐ Determine if incident needs to be escalated to initiate the incident management process.
Detection: IT Operations	No incident management responsibilities.		
Detection: CISO	No incident management responsibilities.		
Detection: Legal, HR, PR	No incident management responsibilities.		
Detection: Senior Management	No incident management responsibilities.		
Detection: External	During the detection phase, an external entity such as law enforcement may notify the organization of an incident.	• Is there a publically facing security incident detected by law enforcement?	☐ Inform the organization and continue established processes if a crime was committed.

Analysis Phase

During the analysis phase, teams will investigate the incident to determine the impact and scope of the threat. Depending on the impact and scope, a threat escalation tier level will be assigned, indicating the number of teams that will be involved in the remediation of the incident, and the notification of the threat will be escalated as appropriate. A third party may be involved if deep forensic analysis is needed.

Technologies involved in this phase include:

[Customize this list to your organization's detection technologies.]

- Firewalls
- IDS/IPS
- Web proxy
- Email gateway
- SIEM or other log correlator
- Digital forensics tools, including:
  - File viewing and analysis tools
  - OS analysis tools
  - Network analysis tools
  - Database analysis tools
- Threat intelligence

Team	Description	Questions	Action
Analysis: End User	During the analysis phase, end users will provide information related to the incident as required.	• What are the events that led up to this suspected incident? • What did I do as a result?	☐ Provide information related to the incident to the help desk.

Analysis: Help Desk	During the analysis phase, help desk staff directly interact with the end user, ask incident-related questions, take actions, and document findings in the help desk ticket.	• What may have caused the incident?
		  ○ Did the end user click a hyperlink or open a file attachment?
		  ○ Did the end user visit a suspicious website?
		  ○ Did the end user download software recently?
		  ○ Did the end user plug in a flash drive?
		• What type of user is affected – i.e. what privileges does the user have?
		• Are any locally stored suspicious file extensions identified?
		• Has the end user been denied access when accessing data or a server?
		• If a device was misplaced, where was it last seen?
		• What types of data or equipment were involved?
			☐ Open a help desk ticket, if not opened.
			☐ Gather answers to incident-related questions and document findings in the ticket.
			☐ Identify incident-related keywords *(malware, ransomware, distributed denial of service [DDoS], compromised credentials)*.
			☐ Search ticketing platform to identify other impacted end users. If multiple end users are impacted, create a parent/child ticket.
			☐ Determine the impact and scope of the incident.
			☐ Assign help desk ticket to cybersecurity team, as appropriate.
			☐ Facilitate end-user notifications.
			☐ If the incident was a false positive, update the ticket and close the incident record.

Analysis: MSSP/Security Operations	During the analysis phase, MSSP/Security Operations will provide the incident coordination support incident responders need and take necessary actions.	• What types of data, information, or equipment were involved? • Does this event need to be escalated to an incident for the cybersecurity team?	☐ Gather answers to incident-related questions. ☐ Perform IoC search in firewall, IDS, IPS, email gateway, and system and server logs. ☐ Investigate and respond to security events. ☐ Escalate to cybersecurity if it is an incident.

Analysis: Cybersecurity	During the analysis phase, cybersecurity staff will analyze appropriate logs, conduct open source intelligence research, provide technical support, provide incident coordination support, interact with the end user directly, ask incident-related questions, take actions, and document findings in the incident record.	• What may have caused the incident?
		  ○ Did the end user click a hyperlink or open a file attachment?
		  ○ Did the end user visit a suspicious website?
		  ○ Did the end user download software recently?
		  ○ Did the end user plug in a flash drive?
		• What type of user is affected, i.e. what privileges does the user have?
		• Are any locally stored suspicious file extensions identified?
		• Has the end user been denied access when accessing data or a server?
		• If a device was misplaced, where was it last seen? What types of data or equipment were involved?
			☐ Gather answers to incident-related questions.
			☐ Conduct open-source threat intelligence analysis to identify comparative IoCs.
			☐ Perform IoC search in firewall, IDS, IPS, email gateway, and system and server logs.
			☐ Determine if any end-user device or devices were compromised.
			☐ Assess if any servers were impacted and decide if any server infections are to be assigned to the infrastructure team.
			☐ Based on the scope and impact, determine the **TEP** tier level. Inform necessary parties, as required.
			☐ If there are any indications that a crime was committed, immediately escalate to the CISO.
			☐ If the incident was a false positive, update the ticket and close the incident record.

Analysis: IT Operations	During the analysis phase, IT operations staff will analyze any appropriate server logs, conduct open-source intelligence research, provide technical support, ask incident-related questions, take actions, and document findings in the incident record.	• Are any other IoCs identified within the organization? • Has the end user been denied access when accessing data or a server? • What types of data, information, or equipment were involved?	☐ Determine any impact to servers, applications, storage, or other systems. ☐ Determine the scope of the incident, such as how much of the network was impacted, how many endpoints, or how many files were compromised. ☐ Determine the scope and impact of the incident, and the resulting TEP tier level.
Analysis: CISO	During the analysis phase, CISO will notify and coordinate with the relevant stakeholders and senior management.	• Has a crime been committed? • Has data been lost or stolen? • Are any business applications impacted?	☐ Publish corporate-wide situational awareness alerts to inform end users of any system outages. ☐ Coordinate and inform senior management of any incident updates.

		• Does a disaster recovery plan need to be enacted?	☐ Approve disaster recovery plan enactment, if necessary. ☐ Report any external criminal activities to senior management. ☐ Engage Legal, HR, and PR to address the incident, as appropriate. ☐ Determine if any incident information should be shared with external parties.
Analysis: Legal, Human Resources (HR), Public Relations (PR)	During the analysis phase, legal, HR, and PR staff will analyze any insider activity, legal requirements, and brand/ reputational damage.	• Are there potential legal repercussions to the incident? • Was there any insider activity or other misuse of assets? • Was there any brand or reputational damage?	Legal: ☐ Determine if any regulatory, legal, or compliance mandates have been violated or impacted. ☐ Determine if any breach notifications are required. ☐ Begin process to notify required parties. Human Resources: ☐ Determine if any employee acceptable-use or security policies have been violated. ☐ Determine if any preliminary employee disciplinary actions are required immediately. Public Relations: ☐ Determine if any public reputational or brand damage has occurred. If so, begin process/campaign to address it.
Analysis: Senior Management	During the incident management analysis phase, senior management staff will notify and coordinate with the relevant stakeholders.	• Was there any insider activity or other misuse of assets? • Have any core business functions been affected? • Was there any brand or reputational damage? • Has a crime been committed? • Has data been lost, and does a disaster recovery plan need to be enacted?	☐ Provide an incident summary and updates to the board of directors/ stakeholders. ☐ Approve reporting crime to law enforcement, if necessary. ☐ Analyze and approve emergency budget, resource, or control requests, as appropriate. ☐ Approve communication of incident information with external parties.
Analysis: External	No incident management responsibilities.		

Containment Phase

During the containment phase, teams will isolate and contain the incident to limit its ability to spread to the rest of the organization.

Technologies involved in this phase include:

[Customize this list to your organization's detection technologies.]

- Network isolation
- Endpoint isolation
- Endpoint containerization

Team	Description	Questions	Action
Containment: End User	No containment responsibilities beyond ongoing cooperation with incident responders.		
Containment: Help Desk	During the containment phase, the help desk will maintain communications with any impacted end users.	• Do any end users need to be notified?	☐ Maintain communications with any impacted end users. ○ Inform users if any critical systems or data will be unavailable or affected during the response process.
Containment: MSSP/Security Operations	During the containment phase, MSSP/Security Operations provide support to isolate the incident.	• What incident coordination support does the cybersecurity team need?	☐ Provide incident coordination support. ☐ Isolate or disconnect any infected endpoints from the network, if necessary. ☐ Determine if other actions are necessary to contain the spread of the incident.
Containment: Cybersecurity	During the containment phase, the cybersecurity team will provide support to isolate the incident and remove compromised assets/users, if necessary.	• How can the issue be isolated with minimal disruption (sandboxing, quarantining, revoking user access, etc.)? • What stakeholders need to be notified?	☐ Provide incident coordination support. ☐ Isolate or disconnect any infected endpoints from the network, shut down organizational Internet access, if necessary. ☐ Disable compromised user accounts, change passwords, or remove privileges, if necessary. ☐ Determine if other actions are necessary to contain the spread of the incident. ☐ Notify affected users and stakeholders.
Containment: IT Operations	During the containment phase, IT Operations will remove any infected servers from the network.	• Was a server infected? Can it be quarantined?	☐ Create an OS-level image of any endpoint, servers, or storage arrays to prevent future data loss. ☐ Isolate or disconnect any servers and/or infected endpoints. ☐ Disable compromised accounts or change passwords. Change the password to the affected system.

Containment: CISO	During the containment phase, the CISO will evaluate any control weaknesses and make recommendations for remediation.	• Are the current security controls sufficient?	☐ Provide senior management with incident updates. ☐ Approved additional resourcing of controls or processes, as necessary for the containment of the incident.
Containment: Legal, HR, PR	During the containment phase, PR may address the public and other stakeholders to inform them of the status of the incident and contain possible rumors, speculation, and reputational damages. Legal and HR will continue ongoing efforts that began in the Analysis phase.	• What types of communication are required? • Are there any Legal and HR processes that need to be continued?	Legal: ☐ Continue legal actions as necessary, informing affected parties as required by regulations. PR: ☐ If necessary, address the affected stakeholders (including the public), informing them of the steps that have been taken to contain the incident and future steps to fully remediate the incident. HR: ☐ Continue HR actions, as necessary, particularly containing any further employee misuse or violations.
Containment: Senior Management	During the containment phase, senior management will determine if any core business function is impacted and will provide final approval for drastic measures.	• Do any business-critical services, systems, or data need to be taken offline for effective containment of the incident?	☐ Determine if any additional stakeholders need to be notified. Provide the notification. ☐ Provide final approval for taking business-critical systems offline or other major containment decisions.
Containment: External	No incident management responsibilities.		

Eradication Phase

During the eradication phase, teams will eliminate components of the incident, such as deleting malware and removing unauthorized user access, as well as identifying and mitigating all vulnerabilities that were exploited. During eradication, it is important to identify all affected hosts within the organization so that they can be remediated. For some incidents, eradication is either not necessary or is performed during recovery.

Technologies involved in this phase include:

[Customize this list to your organization's detection technologies.]

- Network isolation
- Endpoint isolation
- Endpoint containerization

Team	Description	Questions	Action
Eradication: End User	No eradication responsibilities beyond ongoing cooperation with incident responders.		
Eradication: Help Desk	During the eradication phase, the help desk will maintain communications with impacted end users and reissue devices, if necessary.	• Does the end user need to be notified of any updates? • Do any users need new/updated devices issued?	☐ Seize, prepare replacement, and reissue endpoint, if necessary. ☐ Maintain communications with any impacted end users.
Eradication: MSSP/Security Operations Note: This section is to be filled out if there is an MSSP and/or a security operations team. Some of the cybersecurity team responsibilities may fall into here as well.	During the eradication phase, MSSP/Security Operations will ensure possible sources of compromise are eliminated.	• Are there any infected endpoints still on the network? • Are there any compromised user accounts still on the network?	☐ Eliminate the root cause of the incident (e.g. remove malware/virus, block all unauthorized users, de-escalate elevated privileges). ☐ Inform cybersecurity team of any organizational security control gaps, if necessary.
Eradication: Cybersecurity	During the eradication phase, the cybersecurity team will ensure possible sources of	• Are there any infected endpoints still on the network? • Are there any compromised user accounts still on the network?	☐ Backup affected systems for later investigation and forensics. ☐ Eliminate the root cause of the incident (e.g. remove malware/virus, block all unauthorized users, de-escalate elevated privileges).

	compromise are eliminated.		☐ Inform the CISO of any organizational security control gaps, if necessary.
Eradication: IT Operations	During the eradication phase, IT Operations will install patches and eliminate other possible sources of the incident.	• Have systems been adequately patched? • What data needs to be restored? • Are there any control gaps that allowed this incident to occur?	☐ Install system/security patches to resolve malware/network/other vulnerabilities. ☐ Build replacement server. ☐ Disable breached user accounts.
Eradication: CISO	During the eradication phase, the CISO will approve new or updated controls.	• Do any new controls need to be implemented? • Do any controls need to be updated? • Are there any control gaps that allowed this incident to occur?	☐ Approve new controls and the updating of existing ones.
Eradication: Legal, HR, PR	During the eradication phase, Legal, HR, and PR staff will evaluate if any new findings have led to new actions, otherwise they will continue any ongoing processes.	• Are there any changes to Legal, HR, or PR requirements?	☐ Reassess if any new findings have changed the required Legal, HR, or PR actions. If so, address those requirements. ☐ Otherwise continue Legal, HR, and PR efforts already begun.
Eradication: Senior Management	No specific eradication responsibilities beyond ongoing support and approval, as necessary.		
Eradication: External	No incident management responsibilities.		

Recovery Phase

During the recovery phase, teams will enact processes and procedures for recovery and full restoration of any systems, devices, or accounts during the incident. In recovery, responders will restore systems to normal operation, confirm that the systems are functioning normally, and (if applicable) remediate vulnerabilities to prevent similar incidents.
Recovery may involve actions such as restoring systems from clean backups, rebuilding systems from scratch, replacing compromised files with clean versions, installing patches, changing passwords, re-issuing devices, and tightening network perimeter security (e.g. firewall rulesets, boundary router access control lists).

Technologies involved in this phase include:

[Customize this list to your organization's detection technologies.]

- System backup tools
- Patches
- Vulnerability scanners

Team	Description	Questions	Action
Recovery: End User	No recovery responsibilities beyond ongoing cooperation with incident responders.		
Recovery: Help Desk	During the recovery phase, the help desk will maintain communications and coordinate recovery with affected end users.	• Does the end user need to be notified? What do they need to know? • Is the ticket up-to-date?	☐ Maintain communications with any impacted end users. Inform users: ○ When operations are back to normal. ○ Of any required changes (e.g. updates to systems, passwords). ○ Of updated training and awareness material regarding the incident. ☐ Re-issue end-user devices and credentials, if necessary. ☐ Ensure help desk ticket is updated with all relevant information.
Recovery: MSSP/Security Operations Note: This section is to be filled out if there is an MSSP and/or a security operations team. Some of the cybersecurity team responsibilities	During the recovery phase, MSSP/Security Operations will document any relevant findings in the incident ticket.	• Are operations back to normal? • Does the incident ticket include the MSSP/Security Operations information?	☐ Perform vulnerability assessment, antivirus, and anti-malware scans on any endpoints or servers to ensure that operations are back to normal. ☐ Ensure the incident record/ticket is updated with relevant information.

may fall into here as well.			
Recovery: Cybersecurity	During the recovery phase, the cybersecurity team will verify that operations have been successfully restored and that the incident ticket is up-to-date.	• Is the incident report comprehensive? • Has the incident been successfully remediated?	☐ Perform vulnerability assessment, antivirus, and anti-malware scans on any endpoints or servers to ensure that operations are back to normal. ☐ Ensure incident record/ticket is updated with relevant information. ☐ Advise the CISO of any controls, processes, or policies that need to be updated.
Recovery: IT Operations	During the recovery phase, IT Operations will recover and restore systems back to regular operations.	• Do any other servers or systems need to be restored?	☐ Rectify any component that was compromised; restore systems and data, as necessary. ☐ Determine the relative integrity appropriateness of backing the system up. ☐ Once restored, perform system/ network/device validation and testing to verify that the system functions the way it was intended/had functioned in the past. Coordinate with the business units as needed.
Recovery: CISO	During the recovery phase, the CISO will evaluate any weaknesses in security controls or policies as appropriate.	• Do any controls or policies need to be updated?	☐ Review any security policies or controls, as appropriate. ☐ Inform senior management that operations have been restored.
Recovery: Legal, HR, PR	During the recovery phase, Legal, HR, and PR staff will complete their respective processes, and ensure all actions are documented.	• Do any employees need disciplinary action? • What message needs to be communicated to stakeholders/the public? • What legal or regulatory next steps are required?	☐ Legal: Follow-up with any legal implications and requirements. ☐ HR: Ensure employee records are updated with any infractions (e.g. misuse of corporate resources causing an incident) and subsequent disciplinary actions. If disciplinary actions have not been issued yet, begin process in coordination with the employee's manager. ☐ PR: Communicate with stakeholders/public that the incident has been resolved, including next steps.
Recovery: Senior Management	No incident management responsibilities.		
Recovery: External	No incident management responsibilities.		

Post-Incident Phase

During the post-incident phase, teams will perform root-cause analysis and lessons learned activities with various teams and stakeholders within the organization. Any recommended outcomes should be implemented to ensure continuous improvement, and all related active tickets should be updated and closed. This phase involves performing a post-mortem, root-cause analysis, and lessons learned activities with various teams and stakeholders within the organization. Any recommended outcomes should be implemented to ensure continuous improvement, and all related active tickets should be updated and closed.

Team	Description	Questions	Action
Post-Incident: End User	During the post-incident phase, affected users may provide additional details for post-incident meetings/reports and may participate in additional awareness and training.	• What happened? • What was learned? • What has changed?	☐ If necessary, a primary affected user may answer questions regarding the source of the incident. ☐ General end users may participate in updated awareness and training as a result of the incident.
Post-Incident: Help Desk	During the post-incident phase, the help desk may participate in post-incident meetings, as necessary.	• What happened? • How did we respond? • What should we do next time?	☐ Participate in lessons learned (post-mortem) meetings, as necessary.
Post-Incident: MSSP/Security Operations	During the post-incident phase, the MSSP/Security Operations may participate in post-incident meetings, as necessary.	• What happened? • How did we respond? • What should we do next time?	☐ Participate in lessons learned meetings, as necessary.
Post-Incident: Cybersecurity	During the post-incident phase, cybersecurity will support any post-incident activities, as appropriate.	• What happened? • How did we respond? • What should we do next time? • Are there any cybersecurity processes that need to be improved?	☐ Participate in lessons learned meetings, as necessary. ☐ Update and close incident ticket.
Post-Incident; IT Operations	During the post-incident phase, IT Operations will support any post-incident activities, as appropriate.	• What happened? • How did we respond? • What should we do next time? • Are there any IT operations processes that need to be improved?	☐ Participate in any post-incident meetings, as appropriate.
Post-Incident: CISO	During the post-incident phase, the CISO will facilitate any post-incident activities.	• How can the incident response process be improved?	☐ Determine if a full-fledged post-mortem/lesson learned meeting is necessary. ☐ Determine who should participate (e.g. end users, Legal, HR, PR). ☐ Facilitate post-incident meetings (or assign the responsibility to another

			individual). Ensure a record is maintained.
Post-Incident; Legal, HR, PR	During the post-incident phase, Legal, HR, and PR staff will support any post-incident activities, as appropriate.	• Are there any Legal, HR, or PR processes that need to be improved?	☐ Participate in any post-incident meetings, as appropriate. ☐ If new findings become known as a result of post-incident activities, follow-up with any new or ongoing Legal, HR, and PR duties that have not already been addressed. ☐ Legal: Follow up with any legal actions, if required. ☐ HR: Follow up with any employee disciplinary action, if required. ☐ PR: Follow up on public and internal communications to address the resolution of the incident and steps being taken to prevent reoccurrences.
Post-Incident: Senior Management	During the incident management post-incident phase, senior management will support any post-incident activities, as appropriate.	• Are there any senior management processes that need to be improved?	☐ Participate in any post-incident meetings, as appropriate. ☐ Address stakeholders/board of directors, if necessary. ☐ Approve future investments to help prevent reoccurrences.
Post-Incident: External	No incident management responsibilities.		

Appendix

Help Desk Ticket Information

The following are examples of the information that should be collected by the help desk when generating an incident ticket:

- Contact name and number of person reporting the incident.
- Type of data, systems, or equipment involved.
- Category of the incident and surrounding circumstances.
- Whether the compromise puts any person or other data/systems/equipment at risk.
- Location of the incident.
- Inventory numbers of any equipment affected.
- Date and time the security incident occurred.
- Location of data, systems, or equipment affected.

Incident Impact Definitions

The following are example definitions of functional, informational, and recoverability impact. **Customize** these to reflect your tolerance for impact. These definitions are consolidated into the impact criteria in Table 1. [Remove this section if not getting into this level of granularity.]

Table A-1. Definitions of Functional Impact

Ranking	Definition
None	No effect to the organization's ability to provide all services to all users.
Low	Minimally effective; the organization can still provide all critical services to all users but has lost efficiency.
Medium	Organization has lost the ability to provide a critical service to a subset of system users.
High	Organization is no longer able to provide several critical services to any users.

Table A-2. Definitions of Information Impact

Ranking	Definition
None	No meaningful information is exfiltrated or otherwise lost.
Low	Publicly available information is affected.
Medium	Internal private/confidential information is compromised.
High	Regulated data (e.g. personal data, credit card data) or highly confidential organizational material (e.g. trade secret) is breached.

Table A-3. Definitions of Recoverability Impact

Ranking	Definition
None	No significant time/cost to recovery is necessary.
Low	Recoverable through standard service desk process.
Medium	Recoverable through extended effort that can be achieved with existing internal resources.
High	External support is required for recoverability **or** not recoverable.