

Insider Threat Incident Response Playbook

Title	Insider Threat Incident Response Playbook
Version	V1.0
Date issued	DD-MM-YYYY
Status	In progress
Document owner	abc
Creator name	xyz
Creator organization name	ECC
Subject category	Insider Threat Incident Response Management
Access constraints	NA
Review cycle	Annually

1. Introduction

1.1 Incident Overview

An insider attack can include the use of privileged access to abuse rules or intentionally threaten the information or information systems of an organization. Insiders can easily bypass security policies, corrupt valuable resources, and access sensitive information. They can also misuse organizational assets to directly affect the confidentiality, integrity, and availability of information systems.

Assume that a disgruntled employee of CyberK Solutions is misusing their organizational credentials to send sensitive data to a competitor organization. A security alert has been reported to the service desk for unauthorized data transfer to an external network. The service desk is responsible for validating the alert and assigning an appropriate incident response team to handle the incident at the earliest.

1.2 Purpose of Playbook

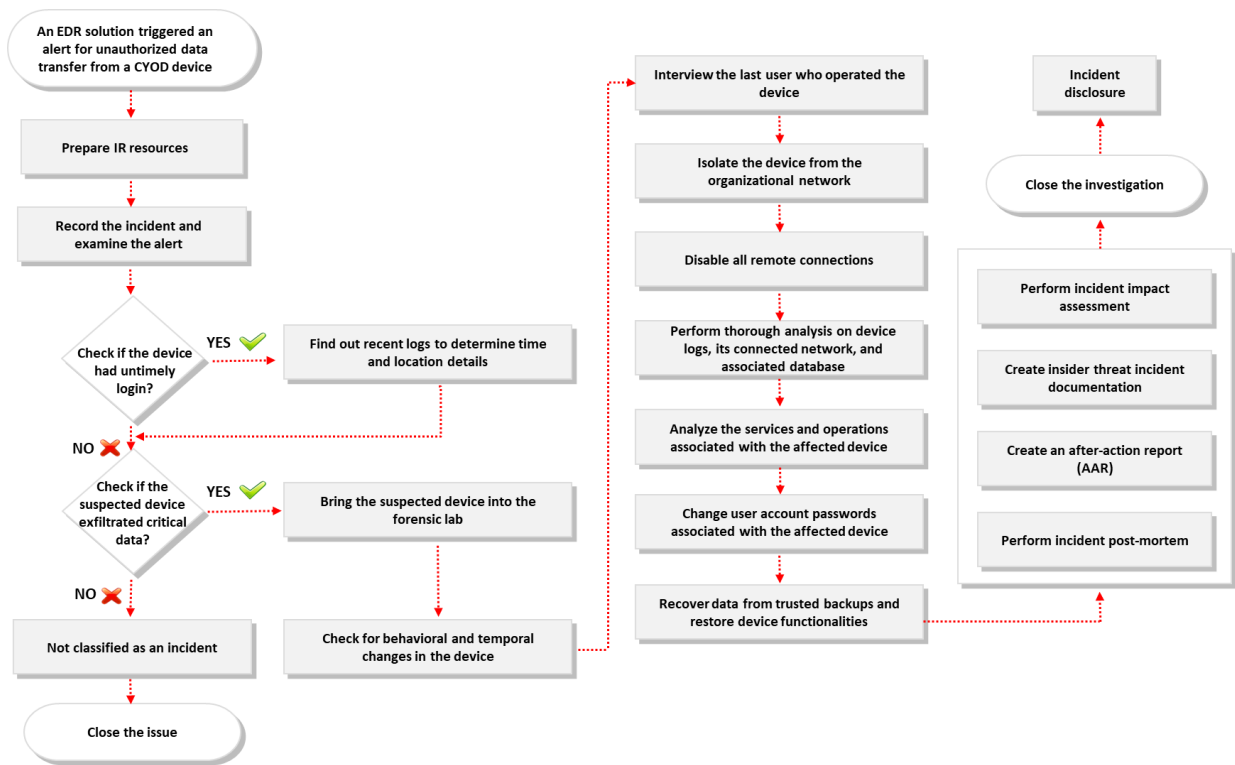
The main purpose of this playbook is to provide guidance for handling insider threats in an organization. This playbook includes step-wise guidance for the IH&R team to handle and respond to similar incidents, implement mitigative actions, and defend against insider threats in an organization.

1.3 Scope

This playbook is developed for the use of incident responders to handle and respond to insider threats in an organization. Additionally, this document must be used alongside the incident response plan of organizations. The scope of this document is listed below (not limited to):

- Determine the impact of the insider threat incident
- Understand and document various user actions associated with the insider threat incident; for example:
 - Details of suspicious employees
 - Systems used to perform data transfer
 - Type of data accessed by the suspect employee
 - Amount of data transferred
- Identify any related activities by checking the following:
 - Any intruder in organizational premises
 - Any abnormal behavior of employees
 - Any unusual time and location of access
 - Any non-deliverable email
 - Any sign of suspicious activity, etc.
- Investigate the incident
- Effectively implement remediation and recovery activities

1.4 Workflow Diagram



Workflow diagram for insider threat incident response

2. Preparation

2.1 Objectives

The main objective of the preparation phase is to prepare organizations to handle and respond to insider threat incidents in an effective and timely manner. Another objective of this phase is to define the roles of employees and their reporting mechanisms for mitigating insider threats.

2.2 Activities Involved

[Activities may differ according to organizational policies, but they are not limited to the following.]

- Prepare for incident response:
 - Prepare, review, and practice incident response procedures in accordance with the incident response plan
 - Develop and implement security policies to mitigate insider threats such as data theft, modification, and IT sabotage
 - Preserve details of previous insider incidents, if any, and investigate them carefully while preparing the incident response plan
 - Identify and prioritize the critical assets of the organization and define a risk management strategy to safeguard them

- Regularly audit and maintain records of all critical assets such as servers, computer systems, and accessories
- Enable logging for all access attempts and regularly audit them
- Implement strict password and account management policies for all employees and enforce a reporting mechanism for unauthorized account access and potential attempts at social engineering
- Implement the principle of least privileges for granting access to organizational resources
- Implement policies for the separation of duties and provide minimum privileges required by employees to perform their duties
- Record physical entry and exit, system logins, network activities, accessed files, uploads and downloads, privilege misuse, etc. for all employees
- Use physical monitoring devices such as CCTV cameras and alarms across organizational premises
- Monitor employee activities such as phone calls and emails
- Use employee monitoring software to track computer activities via screen capturing and monitoring their data, keystroke, idle time, printer, removable drives, and audio/video
- Log and audit access violations and attempts to violate physical space and other equipment
- Ensure that terminated employees do not have access to the physical space or non-public areas in the organization
- Deploy data loss prevention, log management, IDS, SIEM, and behavior analysis tools
- Perform thorough background check on new employees before hiring
- Ensure that access or ID cards are provided to all employees and visitors, which should be worn or displayed at all times
- Implement application whitelisting and blacklisting to prevent employees from downloading and executing malicious software
- Establish a proactive and evolving insider threat detection governance program
- Establish proper controls for devices if they are lost or stolen, such as remote wiping, encryption, and MFA

- Provide easy access to the required documentation such as incident response plan and network architecture to respond to insider threat incidents. Links of important documents are given below:
 - Reference 1:
 - Reference 2:
 - Reference 3:
- Prepare a questionnaire that should be asked by tech support personnel from the complainants to identify the type of insider threat
- Inform employees:
 - Create employee awareness regarding the need for security policies and access controls, their responsibilities and constraints of employment, and consequences of violations
 - Train employees to identify and report policy violation or suspicious espionage events
 - Create awareness and train employees on safeguarding organizational data
 - Train employees to detect and avert social engineering attempts
 - Conduct regular security awareness training sessions to sensitize employees to threats and the organization's security controls
 - Ensure that employees understand the security risks involved in exchanging information over the phone, voice mails, messages, or unencrypted emails
 - Define the proper escalation method that must be followed while investigating similar incidents
 - Provide proper contact information of personnel who can be contacted by users in case of an insider threat incident

2.3 Stakeholders Involved/Communication Established

The stakeholders involved in the aforementioned activities and their communication modes are listed below:

Activities	Stakeholders Involved	Communication Mode/Channel
Prepare for incident response ○ Create incident response processes and procedures	CISO	Email, Phone, Text Message
	Information Security Manager	Email, Phone, Text Message
	IT Manager/Director	Email, Phone, Text Message

<ul style="list-style-type: none"> ○ Define roles and responsibilities ○ Review recent incident reports ○ Incorporate threat intelligence ○ Maintain network architecture and data flow diagrams ○ Define threat indicators and incorporate alerting solutions 	Service Desk	Email, Phone, Text Message
	Service Delivery Manager	Email, Phone, Text Message
	IH&R Team	Email, Phone, Text Message
	Administrators	Email, Phone, Text Message
	Legal Team	Email, Phone, Text Message
	Federal Agency	Email, Phone, Text Message
	Business Continuity Lead	Email, Phone, Text Message
<p>Inform employees</p> <ul style="list-style-type: none"> ○ Conduct training and awareness on how to identify and report insider threats 	Information Security Manager	Email, Phone, Text Message
	IT Manager/Director	Email, Phone, Text Message
	HR Manager	Email, Phone, Text Message
	Administrators	Email, Phone, Text Message
	IH&R Team	Email, Phone, Text Message

2.4 Additional Information (if any)

Note: Refer to the following templates and checklists to fill the necessary details:

- Preparation to Insider Threat Incidents Checklist.docx
- IH&R Plan Template.docx
- IH&R Plan Checklist.docx
- IH&R Policy and Procedure Template.docx

3. Detection and Notification

3.1 Objectives

The main objective of the detection phase is to perform initial investigation on the reported incident and determine whether it is an insider threat. Additionally, this phase involves assigning the appropriate IH&R team members to handle the incident.

3.2 Activities Involved

[Activities may differ according to organizational policies, but they are not limited to the following.]

- Detect and report the insider threat incident:
 - Check for behavioral and temporal changes in employees using tools such as Splunk User Behavior Analytics and IBM QRadar
 - Use insider threat detection tools such as ManageEngine Firewall Analyzer, which generates security and traffic reports, to identify internal threats in the network
 - Use tools such as DataRobot, Ekran System, and Incydr to analyze user behavior, monitor user activities, and detect malicious incidents and suspicious users
 - Check for mismatch in the timeline of an event, which can be suspicious and indicate an insider threat
 - Check for any unauthorized access to physical assets across organizational premises
 - Monitor employees with suspicious business activities such as unusual login time, unusual office timing, and unauthorized browsing and downloads
 - Monitor any abnormal access of systems and user accounts
 - Identify any irresponsible social media behavior
 - Identify any attempt to access restricted zones across the organization
 - Identify unexpected resignations from employees, which can be a potential risk of insider threat, and monitor their activities
 - Monitor employees who are overly enthusiastic to undertake additional work and expand their access to critical data or resources
 - Identify employees in the notice period because those served with termination notices may abuse their privileges to harm the organization
 - Check for alerts of data exfiltration
 - Check for alerts of log modification deletion or access
 - Monitor network usage patterns for any changes indicating malicious activity
 - Check for multiple failed login attempts because an insider can try to log in to unauthorized systems or applications through brute-force attacks
 - Perform mole detection to identify employees pretending to be a dedicated worker but secretly perform malicious activities
 - Perform profiling, which is an ideal way to detect insiders by identifying their behavior patterns

- Escalate the insider threat incident to higher authorities with the proper escalation procedure
- Gather the following information from the initial investigation:
 - Type of insider attack
 - Location of incident
 - Who, how, and when was the incident reported
 - Users/employees/business operations/services affected by the incident
 - Name and number of employees involved in the incident
 - Type of data exfiltrated
 - Any encryption technology implemented
 - Attempts to remotely access the company's resources
 - Involvement of tracking software
 - Availability of data backup

3.3 Stakeholders Involved/Communication Established

The stakeholders involved in the aforementioned activities and their communication modes are listed below:

Activities	Stakeholders Involved	Communication Mode/Channel
Detecting the incident ○ Monitor insider threat detection tools ○ Respond to both manual and automated alerts ○ Escalate the incident via the ticketing system (if not escalated)	Information Security Manager	Email, Phone, Text Message
	IH&R Team	Email, Phone, Text Message
	Resilience Lead	Email, Phone, Text Message
	Business Continuity Lead	Email, Phone, Text Message
	Policy Area Lead	Email, Phone, Text Message
Initial investigation ○ Collect initial evidence data ○ Classify and prioritize the incident	Information Security Manager	Email, Phone, Text Message
	IH&R Team	Email, Phone, Text Message
	IT Manager/Director	Email, Phone, Text Message
	Head of IT	Email, Phone, Text Message

Notification of the incident ○ Follow the defined IH&R plan to notify the incident	Information Security Manager	Email, Phone, Text Message
	IH&R Team	Email, Phone, Text Message
	Policy Area Lead	Email, Phone, Text Message
	Business Continuity Lead	Email, Phone, Text Message

3.4 Additional Information (if any)

Note: Refer to the following documents to fill the necessary details:

- e. Incident Identification and Validation Template.docx
- f. Incident Notification Form-New.docx
- g. Insider Threats Detection Template.docx
- h. Incident Information Collection Form.docx
- i. Checklist for Preliminary Interviews.docx

4. Containment

4.1 Objectives

The main objective of the containment phase is to minimize the damage caused by insider attack and prevent further damage. The containment of insider threats may require both human elements and technical controls.

4.2 Containment Steps/Activities

[Activities may differ according to organizational policies, but they are not limited to the following.]

- Activities to contain the insider threat incident:
 - Disable or reset user account passwords accessed through the victim device
 - Disable active directory accounts, if any, for the victim device
 - Configure alerts for the device whenever it is connected to a network
 - Remove the insider's ability to access organizational premises
 - Examine and contain attack vectors such as malware, portable storage devices, secret cameras, phone tapping devices, and recording devices
 - Inform the affected department and request them to check for potential losses
 - Change the passwords of all user systems and accounts.
 - Continuously monitor employees, contractors, third-party vendors, and outsiders identified as spies until their employment is terminated

- Thoroughly check suspected employees for portable devices containing stolen data and gather all account data used during the incident
- Block all unauthorized communication channels used by insiders to exfiltrate data
- Register a complaint under the appropriate jurisdiction and take proper legal action
- The HR team should block all access to suspicious employees and continuously monitor them until further decision from the management
- Communicate the progress:
 - Regularly inform the respective stakeholders and authorities about the status of the incident handling process

4.3 Stakeholders Involved/Communication Established

The stakeholders involved in the aforementioned activities and their communication modes are listed below:

Activities	Stakeholders Involved	Communication Mode/Channel
Containment activities	Information Security Manager	Email, Phone, Text Message
	IH&R Team	Email, Phone, Text Message
	Resilience Lead	Email, Phone, Text Message
	Business Continuity Lead	Email, Phone, Text Message
	Policy Area Lead	Email, Phone, Text Message

4.4 Additional Information (if any)

Note: Refer to the following documents to fill the necessary details:

- j. Containment of Insider Threats Checklist.docx
- k. Incident Containment Checklist.docx
- l. Incident Containment Template.docx

5. Analysis

5.1 Objectives

The main objective of this phase is to analyze the security incident and determine its scope. Another objective of this phase is to detect and report the impact of the incident to establish forensic investigation requirements and develop an effective mitigation strategy based on analysis results.

5.2 Activities Involved

[Activities may differ according to organizational policies, but they are not limited to the following.]

- Analyze the scope of the insider threat incident
 - Identify if any sensitive data were compromised
 - Identify whether employee safety is at risk
 - Identify if any organizational services or operations were affected
 - Determine if there exists any evidence for identifying the adversary
 - Check for unauthorized access to personal or sensitive corporate data
- Perform network traffic analysis using tools such as Wireshark to detect anomalous network activities of malicious insiders
- Analyze network, server, and database logs to find suspicious user activities such as multiple login attempts, unauthorized file access, and privilege escalation
- Perform system analysis and analyze the following (if applicable):

○ Logged-on user(s)	○ File systems
○ Login attempts	○ Registry settings
○ Network information	○ Event logs
○ Open files	○ Connected devices
○ Network status and connection	○ Slack space
○ Process information	○ Virtual memory
○ Mapped drives	○ Hibernate files
○ Shares	○ Page file
○ Clipboard contents	○ Hidden ADS streams
○ Service/driver information	○ Web browser cache, cookies, and temporary files
○ Command history	

- Perform database analysis using tools such as SysTools SQL Log Analyzer to examine the extent of data leak or theft in a database
- Check for unauthorized employees or personnel in board or official meetings
- Check whether any employee had access to restricted areas containing organizational assets
- Use surveillance camera footage from across the organization for further investigation
- Document the results obtained
- Preserve the evidence for further legal actions

5.3 Stakeholders Involved/Communication Established

The stakeholders involved in the aforementioned activities and their communication modes are listed below:

Activities	Stakeholders Involved	Communication Mode/Channel
Initiate evidence gathering and forensic analysis	Information Security Manager	Email, Phone, Text Message
	IH&R Team	Email, Phone, Text Message
Analyze the scope of insider threat incident	CISO	Email, Phone, Text Message
	Information Security Manager	Email, Phone, Text Message
	IT Manager/Director	Email, Phone, Text Message
	IH&R Team	Email, Phone, Text Message
Analyze the insider threat incident and report potentially compromised data	Information Security Manager	Email, Phone, Text Message
	IH&R Team	Email, Phone, Text Message
	Resilience Lead	Email, Phone, Text Message
	Business Continuity Lead	Email, Phone, Text Message
	Policy Area Lead	Email, Phone, Text Message

5.4 Additional Information (if any)

Note: Refer to the following documents to fill the necessary details:

- m. Insider Threats Analysis Template.docx
- n. Evidence Gathering and Forensic Analysis Form.docx

6. Eradication

6.1 Objectives

The main objective of this phase is to take appropriate measures to eradicate the incident and prevent recurrence in future.

6.2 Eradication Steps/Activities

[Activities may differ according to organizational policies, but they are not limited to the following.]

- Perform the following activities to eradicate the insider threat:
 - Create rules to minimize the outbound transfer of files to an authorized set of users and systems
 - Scan all outgoing and incoming emails for sensitive information and malicious codes
 - Enforce a strict password policy with MFA
 - Enforce account management policies and procedures
 - Employ proper system administration safeguards for critical servers
 - Enable access privileges to employees based on their job roles
 - Use modification alert tools on all systems that flag attempts to change system settings
 - Audit the access rights of employees regularly and revoke unnecessary access
 - Employ strict policies for accessing critical information
 - Disable the access of all employees after termination, including access to premises, applications, accounts, and network devices
 - Regularly change the passwords of wireless networks
 - Limit concurrent logins to prevent repudiation issues
 - Disable default administrative accounts to ensure accountability
 - Monitor the activities of system administrators and privileged users who can access critical information
 - Implement control over the access permissions of administrators and privileged users
 - Regularly monitor the online activities of employees
 - Enforce account and password policies and procedures to ensure that employees regularly change their passwords using password management tools and active directory configurations

- Regularly assess the logging, monitoring, and auditing processes to identify and investigate suspicious insider actions
- Implement intrusion detection and file integrity tools to detect and monitor suspicious activities on sensitive data
- Deploy security guards to investigate unauthorized entry or stop employees from taking unauthorized personnel inside organizational premises
- Implement proper logging devices with ID and biometric scanning abilities at all entry and exit points
- Enforce a system security policy wherein the systems are automatically locked after a certain period of inactivity
- Strictly prohibit the entry of portable media by placing metal detectors at all entry points
- Implement physical security for server rooms, databases, and other critical data resources via dual authentication
- Use cable locks for portable devices such as laptops and smartphones
- Install surveillance cameras in all important areas across organizational premises
- Ensure that all meeting rooms are soundproof to avoid eavesdropping and espionage attempts
- Wipe all hard disks and other media before discarding old computers and laptops
- Ensure strict access policies for third-party staff and vendors

6.3 Stakeholders Involved/Communication Established

The stakeholders involved in the aforementioned activities and their communication modes are listed below:

Activities	Stakeholders Involved	Communication Mode/Channel
Develop an eradication plan ○ Perform technical and business analyses and create a prioritized eradication plan ○ Establish a communication strategy based on the eradication plan	Information Security Manager	Email, Phone, Text Message
	IH&R Team	Email, Phone, Text Message
	IT Manager/Director	Email, Phone, Text Message
	Internal/External Communications Team	Email, Phone, Text Message
	Resilience Lead	Email, Phone, Text Message
	Business Continuity Lead	Email, Phone, Text Message
	Policy Area Lead	Email, Phone, Text Message

Eradication activities	Information Security Manager	Email, Phone, Text Message
	IH&R Team	Email, Phone, Text Message

6.4 Additional Information (if any)

Note: Refer to the following documents to fill the necessary details:

- o. Eradication of Insider Threats Checklist.docx
- p. Incident Eradication Template.docx
- q. Incident Eradication Checklist.docx

7. Recovery

7.1 Objectives

The main objective of this phase is to recover organizational resources from the impact of insider threat incident and maintain business continuity.

7.2 Recovery Steps/Activities

[Activities may differ according to organizational policies, but they are not limited to the following.]

- Activities to recovery from insider attack incident:
 - Implement recovery processes to restore normal work functionality and business operations using trusted devices and backups
 - Create alerting systems from associated user accounts in case of abnormal activity
 - Preserve the evidence required for legal proceedings obtained from forensic analysis
 - File a complaint with the cybercrime department
 - Contact law enforcement and brief them about the incident
 - Change the passwords of all accounts and employ two-factor authentication
 - Remove malicious artifacts and recover data from clean and trusted backups if the attacker damaged any data or installed malware
 - Secure backup media and its content from alteration, theft, or destruction
 - Implement cloud-to-cloud backup solutions
 - Store administrator keys in a secure location
 - Apply patches for the identified vulnerabilities to prevent similar incidents

7.3 Stakeholders Involved/Communication Established

The stakeholders involved in the aforementioned activities and their communication modes are listed below:

Activities	Stakeholders Involved	Communication Mode/Channel
Recovery activities	Information Security Manager	Email, Phone, Text Message
	IH&R Team	Email, Phone, Text Message

7.4 Additional Information (if any)

Note: Refer to the following documents to fill the necessary details:

- r. Recovery from Insider Threats Checklist.docx
- s. Incident Recovery Procedure Template.docx
- t. Incident Recovery Checklist.docx

8. Post-incident Activities

8.1 Objectives

The main objective of this phase is to create the necessary insider threat incident reports such as incident post-mortem, after-action report (AAR), incident documentation, lessons learned, and incident impact assessment. Another objective of this phase is to close the insider threat investigation and disclose its details to respective stakeholders through proper channels.

8.2 Activities

[Activities may differ according to organizational policies, but they are not limited to the following.]

- Perform insider threat incident post-mortem or incident review to understand the root causes
- Create an AAR that includes information such as what worked effectively, areas of improvement, and strategies for enhancing the response in case of similar insider incidents
- Conduct a lessons learned meeting to document incident details; additionally, ensure that the following questions are answered in this meeting:
 - When and who detected the insider threat?
 - What happened exactly?
 - What caused the insider incident?
 - To whom was the insider incident reported?

- Was the organization adequately prepared to handle insider threats?
- How was the insider threat incident contained?
- How were the impacted accounts sanitized?
- What procedures were followed during recovery?
- Were the documented procedures followed by the response team?
- How efficiently did the incident response team and management resolve the insider threat incident?
- How should the incident response team and management respond to mitigate similar insider threat incidents in future?
- Were there any gaps in communication during incident response?
- Was the right amount of information shared with the right personnel?
- What are the tools and resources required to detect, analyze, and prevent similar insider incidents in future?
- Create concise and clear insider threat incident documentation in a standard format and get it reviewed by editors
- Create an incident impact assessment report to determine all types of losses caused by the insider threat incident; this report must address the following, if required:
 - Financial losses caused by the leakage of confidential information
 - Legal costs for investigating the case, lawyer's fees, etc.
 - Costs pertaining to analyzing the insider threat, recovering from the incident, and installing software and hardware
 - Implementation costs
 - Costs related to the damage of goodwill as well as the loss of customer trust and reputation
- Officially close the insider threat investigation by informing the management and securely retain investigation reports considering the retention policy of the organization
- Disclose incident details to the respective stakeholders through proper channels after consulting with the legal department of the organization

8.3 Stakeholders Involved/Communication Established

The stakeholders involved in the aforementioned activities and their communication modes are listed below:

Activities	Stakeholders Involved	Communication Mode/Channel
Create incident post-mortem report	Information Security Manager	Email, Phone, Text Message
	IH&R Team	Email, Phone, Text Message
Create AAR	Information Security Manager	Email, Phone, Text Message
	IH&R Team	Email, Phone, Text Message
Conduct lessons learned meeting	Information Security Manager	Email, Phone, Text Message
	IH&R Team	Email, Phone, Text Message
Create incident documentation	Information Security Manager	Email, Phone, Text Message
	IH&R Team	Email, Phone, Text Message
Create incident impact assessment report	Information Security Manager	Email, Phone, Text Message
	IH&R Team	Email, Phone, Text Message
Close the investigation officially	Information Security Manager	Email, Phone, Text Message
	IH&R Team	Email, Phone, Text Message
	Management	Email, Phone, Text Message
Disclose incident details to the respective stakeholders	Information Security Manager	Email, Phone, Text Message
	IT Manager/ Director	Email, Phone, Text Message
	CISO	Email, Phone, Text Message
	IH&R Team	Email, Phone, Text Message
	Legal Team	Email, Phone, Text Message
	HR Manager	Email, Phone, Text Message
	Media	Email, Phone, Text Message

	Vendors	Email, Phone, Text Message
	Customers & General Public	Email, Phone, Text Message
	Business Partners	Email, Phone, Text Message
	Resilience Lead	Email, Phone, Text Message
	Business Continuity Lead	Email, Phone, Text Message
	Policy Area Lead	Email, Phone, Text Message

8.4 Additional Information (if any)

Note: Refer to the following documents to fill the necessary details:

- u. Incident Postmortem Template.docx
- v. After Action Report Form Template.docx
- w. Incident Documentation Template.docx
- x. Incident Impact Assessment Report Template.docx
- y. Incident Closure Letter.docx
- z. Incident Disclosure Form.docx
- aa. Incident Reporting Template.docx

9. Appendix