Sample Outline for Incident Response Policy

I. Introduction
   A. Purpose and Scope
   B. Policy Objectives
   C. Definitions and Terminology

II. Incident Response Team
   A. Formation and Responsibilities
   B. Roles and Responsibilities of Team Members
   C. Contact Information

III. Incident Identification
   A. Procedures for Identifying Incidents
   B. Detection Tools and Mechanisms
   C. Reporting Mechanisms

IV. Incident Categorization and Classification
   A. Categories of Incidents
   B. Incident Classification Criteria

V. Incident Response Procedures
   A. Initial Response Steps
   B. Containment and Eradication Procedures
   C. Recovery Measures
   D. Documentation Requirements

VI. Communication and Notification
   A. Internal Communication Procedures
   B. External Communication Procedures
   C. Notification of Relevant Parties (Management, Legal, Law Enforcement)

VII. Post-Incident Review

I. Introduction

The purpose of this policy is to establish an incident response framework to effectively detect, respond to, and recover from cybersecurity incidents. This policy applies to all employees, contractors, and third-party service providers.

II. Incident Response Team

The incident response team is composed of designated individuals responsible for coordinating and executing incident response activities. The team' structure allows for team members to be flexible while working to respond to the various aspects of incident detection, response, and recovery.

Roles and Responsibilities of Team Members

(add brief description of responsibilities)

Role: Captain
Role: Linux Team
Role: Windows Team
Role: Firewall
Role: Threat Hunting
Role: Inject

Team Member Contact Information

Each team member's contact information, including primary and secondary contact details, will be maintained and updated on a regular basis. This will provide an efficient method of communication and collaboration of vital information during incident response.

III. Incident Identification

Employees Responsibilities:

1. Prompt Reporting

   All employees are responsible for promptly reporting any suspected security incidents to the Incident Response Team through designated reporting mechanisms. This includes but is not limited to unusual activity, potential security threats, emails from unknown senders, or suspicious behavior immediately upon detection. Employees should be made aware of how to utilize designated reporting channels, such as a dedicated incident reporting portal, email, or informing manager on duty.

2. Awareness and Training:

   Stay informed and participate in cybersecurity awareness training programs to recognize potential incidents. This can include but is not limited to attending regular training sessions to understand the latest threats and incident indicators. Be vigilant for signs of phishing, malware, unauthorized access, or any unusual system behavior.

3. Documentation

   Document and provide as much detailed information about the suspected incident as possible. The more information the better. Include relevant details such as the date, time, location, workstation, hostname, IP and a description of the incident. Capture any error messages, unusual system behavior, or suspicious emails.

4. Non-Retaliation Policy

1. We here at [Company A] always encourage a culture that promotes incident reporting without fear of retaliation. Upon submittal of an incident response, an employee may be contacted by a incident response team member and be presented with the organization's non-retaliation policy. An employee who submits and incident will be provided assurance that reporting incidents is an extremely beneficial contribution to the overall security of all members of the organization.

Incident Response Team Responsibilities

[insert small descript]

1. Designated Reporting Mechanisms
   The Incident Response Team will ensure that employees have clear and accessible reporting mechanisms. The IRT will maintain an incident reporting portal or email address for streamlined reporting of employee security concerns and incidents. The IRT will regularly communicate the available reporting channels to all employees.
2. Response Acknowledgement
   The IRT will acknowledge receipt of incident reports promptly. The IRT will establish a method of communication that will acknowledge the employee submitting the complaint, a confirmation of received.
3. The IRT wil conduct an initial assessment of reported incidents. This initial assessment shall include an evaluation of the severity and potential impact of reported incidents. The incidents will be assigned to the relevant Incident Response Team for further investigation.

4. Feedback and Communication

1. The IR Team will keep the organization's employees informed about the incident response actions and provide updates on the incident investigation progress. This includes communicating to the organization's employees any necessary steps employees should take in response to ongoing incidents.

Third-Party Vendors

1. Any third-party vendors whose services may be impacted as a result of an incident should be informed as soon as possible. Communication protocols should be established and procedures for collaboration with vendors to address and mitigate potential impacts of incidents.
2. Develop a system to communicate with third-party vendors. Each vendor will have an assigned point of contact. The assigned point of contact and the third-party vendor will establish a safe way to share important information and the frequency of communication between each other through meetings, emails, and updates.

Customers or Clients

1. Communication with customers or clients should be made If their data or services are potentially affected by an incident. This should be done by developing a communication plan to notify affected parties. In the event of an incident that has affected the customer or client, transparency should be timely and those affected should be updated on the incident resolution.

Regulatory Bodies

1. Regulatory bodies require compliance with reporting requirements. Establish procedures for reporting security incidents to regulatory authorities. To comply and meet legal obligations, ensure that reporting of incidents is completed in a timely and accurate manner

IV. Incident Response Procedures

Initial Response Steps
Identification
Quickly identify and confirm potential security incidents via monitoring and alert systems. Establishing indicators of compromise (IoCs) to recognize unusual patterns or behaviors is

Third-Party Vendor Plan

Customer and/or client plan

Regulatory Bodies Plan