Incident Response Policy on Form Filling

1. Introduction

1.1 Purpose

The purpose of this policy is to provide guidelines and procedures for accurately and consistently filling out incident response forms during the incident handling process. Proper form filling is essential for documenting incidents comprehensively and facilitating effective incident response.

1.2 Scope

This policy applies to all incident response team members and individuals involved in the documentation of security incidents within our organization.

2. Roles and Responsibilities

2.1 Form Filling Responsibilities

Incident responders are responsible for completing incident response forms accurately and comprehensively.

Incident coordinators are responsible for overseeing the form filling process and ensuring that all necessary information is captured.

All individuals involved in incident handling must cooperate with incident responders and provide accurate information for form filling.

3. Incident Response Forms

3.1 Form Structure

The incident response form consists of the following fields, each of which serves a specific purpose in documenting incidents:

**Reported by:** The individual or entity reporting the incident should provide their name or organization's name.

**Title/Role:** Specify the title or role of the person completing the form.

**Date of Report:** Enter the date when the incident is officially reported, following the format MM/DD/YYYY.

**Incident Number:** Assign incident number with year, month, day, and preparer initial to each incident for tracking and reference purposes. If the preparer has filled more than 1 form for the day, add v followed by number. For example, 20240122-TA-V2 for date, first and last name initial and V2 indicating 2nd form filled.

**Incident Type:** Indicate the type or category of the incident (e.g., data breach, malware infection).

**Date of Incident:** Record the date when the incident occurred (MM/DD/YYYY).

**Time of Incident:** Document the exact time of the incident (HH:MM AM/PM).

**Date of Detection:** Enter the date when the incident was first detected (MM/DD/YYYY).

**Status:** Describe the status of the incident (e.g., under investigation, resolved).

**Location:** Specify the location or context where the incident occurred.

**Name/Role/Contact of Parties Involved:** Provide the names, roles, and contact information of individuals involved in the incident.

**Source IP:** Capture the source IP address of the incident.

**Source Port:** Include the source port used in the incident.

**Destination IP:** Document the destination IP address affected by the incident or IP of breached system

**Destination Port:** Specify the destination port impacted by the incident.

**Timeline:** Create a chronological timeline of events related to the incident timeline of any unusual or noteworthy characteristics.

**Access Obtained:** Indicate whether unauthorized access was obtained during the incident.

**Password Compromised:** Specify if any passwords were compromised.

**Impact on Service:** Describe the impact of the incident on services or systems.

**Impact on Information:** Explain the impact on sensitive or confidential information.

**Asset Affected:** Identify the specific assets or resources affected by the incident.

**Follow-Up Actions:** Outline the follow-up actions taken in response to the incident, including containment, eradication, recovery, and mitigation measures.

**Additional Notes:** Include any additional notes, observations, or comments that may provide further context or insights into the incident.

4. Guidelines for Form Filling

4.1 Reporting and Form Completion

Incidents should be reported promptly to the incident response team.

Complete the incident response form accurately and comprehensively, providing **minimum of red above field** requested information.

Use N/A when a specific field is not applicable to the incident.

Follow the specified date and time formats when recording incident-related dates and times.

Ensure consistency and clarity in documenting incident details.

5. Documentation Standards

5.1 Consistency and Completeness

Maintain consistency in form filling across all incidents.

Ensure that the form is completed in its entirety and that no critical information is omitted.

6. Training and Awareness

6.1 Training Programs

Ensure that all incident response team members receive training on proper form filling procedures.

Promote awareness of the importance of accurate form completion for effective incident response.

7. Review and Revision

7.1 Form Review

Periodically review and update the incident response forms and associated form filling procedures to align with evolving organizational needs and best practices.

By adhering to this "Incident Response Policy on Form Filling," our organization aims to maintain consistent and thorough documentation of security incidents, ultimately enhancing our ability to respond effectively to incidents and protect our assets and information.