TrustIoT Framework for Industry 4.0

"Post-Incident Analysis"

|  |  |
| --- | --- |
| Document Classification: | Internal |
| Document Ref. | *TrustIoT Framework for Industry 4.0* |
| Version: | *1* |
| Document Author: | *Jibran Saleem* |
| Document Owner: |  |

**Revision History**

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date** | **Revision Author** | **Summary of Changes** |
|  |  |  |  |
|  |  |  |  |

**Distribution**

|  |  |
| --- | --- |
| **Name** | **Title** |
|  |  |
|  |  |
|  |  |

**Approval**

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Position** | **Signature** | **Date** |
|  |  |  |  |

Table of Contents

[1. Introduction 4](#_Toc176333658)

[2. Purpose 4](#_Toc176333659)

[3. Scope 4](#_Toc176333660)

[4. Policy Statement 4](#_Toc176333661)

[4.1. Incident Documentation 4](#_Toc176333662)

[4.2. Root Cause Analysis 4](#_Toc176333663)

[4.3. Impact Assessment 4](#_Toc176333664)

[4.4. Lessons Learned and Improvement 5](#_Toc176333665)

[5. Responsibilities 5](#_Toc176333666)

[6. Breaches of Policy 5](#_Toc176333667)

[7. Document Management 5](#_Toc176333668)

# Introduction

The Internet of Things (IoT) ecosystem, with its interconnected devices and vast data flows, presents a complex and dynamic attack surface. Security incidents, while undesirable, are a reality in today's threat landscape. A robust post-incident analysis process is crucial for understanding the root causes of incidents, assessing their impact, and implementing corrective measures to prevent future occurrences. This policy outlines the procedures and responsibilities for conducting thorough and effective post-incident analyses within the IoT environment.

# Purpose

The purpose of this policy is to establish a framework for conducting comprehensive post-incident analyses following security incidents related to IoT devices and systems within the organisation. This policy aims to:

* Identify the root causes and contributing factors of security incidents.
* Assess the impact of incidents on the organisation's operations, data, and reputation.
* Develop and implement corrective actions to prevent similar incidents from recurring.
* Continuously improve the organisation's security posture and incident response capabilities.

# Scope

This policy applies to all security incidents that affect or involve IoT devices and systems connected to the organisation's network, regardless of their location or function.

# Policy Statement

## Incident Documentation

* **Detailed Records:** Comprehensive documentation of the incident shall be maintained, including:
  + Timeline of events
  + Affected devices and systems
  + Actions taken during incident response
  + Evidence collected
  + Communication logs

## Root Cause Analysis

* **Thorough Investigation:** A root cause analysis (RCA) shall be conducted to identify the underlying causes and contributing factors that led to the security incident.
* **Analysis Techniques:** Various analysis techniques, such as 5 Whys, fishbone diagrams, or fault tree analysis, may be employed to identify root causes.
* **Documentation:** The findings of the RCA shall be documented, including identified root causes, contributing factors, and recommendations for corrective actions.

## Impact Assessment

* **Impact Analysis:** The impact of the security incident on the organisation's operations, data, and reputation shall be assessed.
* **Financial Impact:** The financial costs associated with the incident, including recovery costs, lost productivity, and potential fines or penalties, shall be evaluated.
* **Reputational Impact:** The potential impact on the organisation's reputation and customer trust shall be considered.

## Lessons Learned and Improvement

* **Lessons Learned:** Key lessons learned from the incident and the RCA shall be identified and documented.
* **Corrective Actions:** Specific and actionable corrective actions shall be developed and implemented to address the identified root causes and prevent similar incidents from recurring.
* **Continuous Improvement:** The incident response plan and related procedures shall be updated based on the lessons learned to enhance the organisation's overall security posture.

# Responsibilities

* **Information Security Officer:** Responsible for overseeing the post-incident analysis process and ensuring that lessons learned are incorporated into security policies and procedures.
* **Incident Response Team:** Responsible for conducting the root cause analysis and impact assessment, and for developing and implementing corrective actions.
* **Management:** Responsible for reviewing and approving corrective actions and providing necessary resources for their implementation.

# Breaches of Policy

Failure to conduct a thorough post-incident analysis or to implement appropriate corrective actions may result in disciplinary action, up to and including termination of employment or contractual relationships.

# Document Management

This document is valid as of [dd/mm/yyyy].

This document is reviewed periodically and at least annually to ensure compliance with the following prescribed criteria.

* Compliant with the Internet of Things (IoT) Security Framework for Industry 4.0.
* Legislative requirements defined by law, where appropriate.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

[Name 1]

Manager