TrustIoT Framework for Industry 4.0

"Framework for continuous improvement based on 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](#_Toc176333703)

[2. Purpose 4](#_Toc176333704)

[3. Scope 4](#_Toc176333705)

[4. Policy Statement 4](#_Toc176333706)

[4.1. Incident Analysis and Documentation 4](#_Toc176333707)

[4.2. Root Cause Analysis 4](#_Toc176333708)

[4.3. Corrective and Preventive Actions 4](#_Toc176333709)

[4.4. Policy and Procedure Review 4](#_Toc176333710)

[4.5. Communication and Awareness 5](#_Toc176333711)

[5. Responsibilities 5](#_Toc176333712)

[6. Breaches of Policy 5](#_Toc176333713)

[7. Document Management 5](#_Toc176333714)

# Introduction

The dynamic nature of the Internet of Things (IoT) ecosystem, coupled with the evolving threat landscape, necessitates a proactive and adaptive approach to security. Security incidents, while undesirable, provide valuable opportunities for learning and improvement. This policy establishes a framework for leveraging incident analysis to drive continuous improvement in the organization's IoT security posture.

# Purpose

The purpose of this policy is to outline the procedures and guidelines for conducting thorough post-incident analyses and utilising the insights gained to enhance the security and resilience of the organization's IoT infrastructure. This policy aims to:

* Foster a culture of continuous improvement in IoT security.
* Identify and address root causes of security incidents.
* Implement corrective and preventive actions to prevent recurrence.
* Enhance the effectiveness of incident response and security controls.

# Scope

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

# Policy Statement

## Incident Analysis and Documentation

* **Thorough Investigation:** A comprehensive analysis shall be conducted following every security incident, documenting the timeline of events, affected systems, and actions taken during the incident response.
* **Evidence Collection and Preservation:** Relevant evidence shall be collected and preserved in a manner that maintains its integrity and chain of custody.
* **Incident Classification:** Incidents shall be classified based on their severity, impact, and root cause to facilitate trend analysis and identify areas for improvement.

## Root Cause Analysis

* **Systematic Approach:** A systematic root cause analysis (RCA) methodology shall be employed to identify the underlying causes and contributing factors that led to the security incident.
* **Documentation:** The findings of the RCA shall be documented, including identified root causes, contributing factors, and recommendations for corrective actions.

## Corrective and Preventive Actions

* **Action Plan:** Based on the findings of the incident analysis and RCA, a corrective and preventive action (CAPA) plan shall be developed, outlining specific actions to address the identified root causes and prevent similar incidents from recurring.
* **Implementation and Tracking:** The CAPA plan shall be implemented in a timely manner, and its progress shall be tracked and monitored to ensure its effectiveness.

## Policy and Procedure Review

* **Regular Reviews:** Existing security policies, procedures, and controls shall be periodically reviewed and updated based on lessons learned from incident analyses.
* **Gap Analysis:** Incident analysis findings shall be used to identify gaps in existing security measures and inform the development of new or improved controls.

## Communication and Awareness

* **Information Sharing:** Lessons learned from incident analyses shall be shared with relevant stakeholders, including IT staff, system owners, and management, to raise awareness and promote a culture of security.
* **Training and Education:** Incident analysis findings may be incorporated into security awareness training programs to educate employees about potential threats and best practices.

# Responsibilities

* **Information Security Officer:** Responsible for overseeing the incident analysis and continuous improvement process.
* **Incident Response Team:** Responsible for conducting incident analyses, root cause analyses, and developing CAPA plans.
* **IT Department:** Responsible for implementing corrective actions and updating security policies and procedures.
* **Management:** Responsible for reviewing and approving CAPA plans and providing necessary resources for their implementation.

# Breaches of Policy

Failure to conduct thorough incident analyses 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