Internet of Things (IoT) Security Framework for Industry 4.0

"Analysis: Root cause analysis & forensic investigations"

|  |  |
| --- | --- |
| Document Classification: | Internal |
| Document Ref. | *Internet of Things (IoT) Security 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](#_Toc176333670)

[2. Purpose 4](#_Toc176333671)

[3. Scope 4](#_Toc176333672)

[4. Policy Statement 4](#_Toc176333673)

[4.1. Root Cause Analysis 4](#_Toc176333674)

[4.2. Forensic Investigations 4](#_Toc176333675)

[5. Responsibilities 5](#_Toc176333676)

[6. Breaches of Policy 5](#_Toc176333677)

[7. Document Management 5](#_Toc176333678)

# Introduction

The Internet of Things (IoT) ecosystem, with its interconnected devices and vast data flows, presents a complex and dynamic attack surface. Security incidents, such as unauthorised access, data breaches, or service disruptions, can have significant consequences for the organisation. A robust process for analysing these incidents is crucial for understanding their root causes, assessing their impact, and implementing corrective measures to prevent future occurrences. This policy outlines the procedures and responsibilities for conducting thorough and effective analyses, including root cause analysis and forensic investigations, within the IoT environment.

# Purpose

The purpose of this policy is to establish a framework for conducting comprehensive 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

## Root Cause Analysis

* **Thorough Investigation:** A root cause analysis (RCA) shall be conducted following every security incident to identify the underlying causes and contributing factors that led to the incident.
* **Analysis Techniques:** Various analysis techniques, such as 5 Whys, fishbone diagrams, or fault tree analysis, may be employed to systematically identify root causes.
* **Documentation:** The findings of the RCA shall be documented, including identified root causes, contributing factors, and recommendations for corrective actions.
* **Corrective Actions:** Specific and actionable corrective actions shall be developed and implemented to address the identified root causes and prevent similar incidents from recurring.

## Forensic Investigations

* **Evidence Collection and Preservation:** In the event of a security incident, forensic evidence shall be collected and preserved in a manner that maintains its integrity and chain of custody. This may involve:
  + Imaging or capturing affected devices and systems
  + Collecting network logs and traffic data
  + Preserving relevant files and artifacts
* **Forensic Analysis:** Qualified personnel or external experts shall conduct forensic investigations to analyse the collected evidence, identify the attack vectors, and determine the extent of the compromise.
* **Legal and Regulatory Compliance:** Forensic investigations shall be conducted in compliance with applicable legal and regulatory requirements, including data privacy and chain of custody considerations.

# Responsibilities

* **Information Security Officer:** Responsible for overseeing the incident analysis process and ensuring that lessons learned are incorporated into security policies and procedures.
* **Incident Response Team:** Responsible for conducting root cause analyses and coordinating forensic investigations.
* **IT Department:** Responsible for providing technical support and expertise during incident analysis and forensic investigations.
* **Legal Department:** Responsible for providing legal advice and guidance on evidence collection, preservation, and handling.
* **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