TrustIoT Framework for Industry 4.0

"Reporting Procedures: Incident reporting protocols"

|  |  |
| --- | --- |
| 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](#_Toc176333584)

[2. Purpose 4](#_Toc176333585)

[3. Scope 4](#_Toc176333586)

[4. Policy Statement 4](#_Toc176333587)

[4.1. Incident Identification 4](#_Toc176333588)

[4.2. Incident Reporting 4](#_Toc176333589)

[4.3. Incident Response 5](#_Toc176333590)

[4.4. Post-Incident Review 5](#_Toc176333591)

[5. Responsibilities 5](#_Toc176333592)

[6. Breaches of Policy 5](#_Toc176333593)

[7. Document Management 5](#_Toc176333594)

# 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. Timely detection and reporting of such incidents are crucial for effective response and mitigation. This policy outlines the procedures and responsibilities for identifying, reporting, and responding to security incidents within the IoT environment.

# Purpose

The purpose of this policy is to establish a framework for the detection, reporting, and response to security incidents related to IoT devices and systems within the organisation. This policy aims to:

* Enable prompt identification and reporting of security incidents.
* Facilitate efficient and coordinated incident response.
* Minimise the impact of security breaches and disruptions.
* Learn from incidents and continuously improve the organisation's security posture.

# 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 Identification

* **Monitoring and Logging:** IoT devices, network infrastructure, and security solutions shall be continuously monitored and logged to detect signs of suspicious or malicious activity. This includes but is not limited to:
  + Unauthorised access attempts
  + Unusual network traffic patterns
  + Unexplained changes in device configurations
  + System or application errors and crashes
* **Anomaly Detection:** Behavioural analytics and machine learning techniques shall be employed to identify deviations from normal patterns that may indicate security incidents.
* **User Reporting:** All employees, contractors, and third-party vendors shall be encouraged to report any suspected security incidents or unusual activity involving IoT devices.

## Incident Reporting

* **Reporting Channels:** Clear and accessible channels shall be established for reporting security incidents, such as:
  + A dedicated hotline or phone number
  + A designated email address
  + An online incident reporting system
* **Timely Reporting:** Security incidents shall be reported promptly to the designated incident response team or security personnel. Delays in reporting can significantly impact the effectiveness of incident response and may exacerbate the damage caused.
* **Incident Information:** Incident reports shall include all relevant details, such as:
  + The nature of the incident (e.g., unauthorised access, data breach, malware infection)
  + Affected devices or systems
  + Date and time of the incident
  + Potential impact on the organisation
  + Any observed indicators of compromise (IOCs)

## Incident Response

* **Incident Response Team:** A dedicated incident response team shall be established with clearly defined roles and responsibilities for handling security incidents.
* **Incident Response Plan:** A comprehensive incident response plan shall be developed and maintained, outlining the procedures for:
  + Incident triage and assessment
  + Containment and eradication of the threat
  + Recovery of affected systems and data
  + Post-incident analysis and lessons learned
* **Escalation:** Incidents shall be escalated to appropriate personnel or management based on their severity and potential impact.
* **Communication:** Timely and effective communication shall be maintained with relevant stakeholders throughout the incident response process.

## Post-Incident Review

* **Root Cause Analysis:** A thorough post-incident review shall be conducted to identify the root cause of the incident, assess the effectiveness of the response, and identify areas for improvement.
* **Lessons Learned:** Lessons learned from the incident shall be documented and incorporated into updated incident response procedures and security controls.
* **Documentation:** Detailed documentation of the incident, response actions, and lessons learned shall be maintained for future reference and compliance purposes.

# Responsibilities

* **Information Security Officer:** Responsible for overseeing the implementation and enforcement of this policy.
* **Security Operations Centre (SOC):** Responsible for monitoring security events, analysing threats, and coordinating incident response.
* **Incident Response Team:** Responsible for investigating and responding to security incidents.
* **All Employees:** Responsible for reporting suspected security incidents promptly and cooperating with incident response efforts.

# Breaches of Policy

Failure to report a security incident or comply with incident response procedures 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