TrustIoT Framework for Industry 4.0

"Detection Mechanisms: Anomaly detection & logging"

|  |  |
| --- | --- |
| 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](#_Toc176333569)

[2. Purpose 4](#_Toc176333570)

[3. Scope 4](#_Toc176333571)

[4. Policy Statement 4](#_Toc176333572)

[4.1. Anomaly Detection 4](#_Toc176333573)

[4.2. Logging 4](#_Toc176333574)

[5. Responsibilities 5](#_Toc176333575)

[6. Breaches of Policy 5](#_Toc176333576)

[7. Document Management 5](#_Toc176333577)

# Introduction

The Internet of Things (IoT) ecosystem presents a complex and dynamic environment where numerous devices generate and exchange vast amounts of data. Ensuring the security and integrity of this ecosystem requires proactive measures to detect anomalies and potential threats. This policy outlines the implementation and utilisation of anomaly detection mechanisms and comprehensive logging practices to identify and respond to security incidents and operational issues within the IoT infrastructure.

# Purpose

The purpose of this policy is to establish guidelines and requirements for the deployment and operation of anomaly detection mechanisms and logging practices within the organisation's IoT environment. This policy aims to:

* Enable the timely detection of suspicious or anomalous activity that may indicate security breaches, unauthorised access, or system malfunctions.
* Facilitate the investigation and analysis of security incidents and operational issues through comprehensive logging.
* Enhance the overall security posture and resilience of the IoT ecosystem.

# Scope

This policy applies to all IoT devices, systems, and data within the organisation's network. This includes, but is not limited to:

* Sensors, actuators, and controllers
* Gateways and edge devices
* Industrial control systems (ICS)
* Data storage and processing systems

# Policy Statement

## Anomaly Detection

* **Behavioural Baselining:** Baseline profiles of normal behaviour shall be established for IoT devices and systems, considering factors such as network traffic patterns, data transmission volumes, and resource utilisation.
* **Anomaly Detection Mechanisms:** Automated tools and techniques, such as machine learning algorithms and statistical analysis, shall be employed to identify deviations from established baselines that may indicate potential threats or anomalies.
* **Real-time Monitoring:** Anomaly detection shall be performed in real-time to enable prompt identification and response to security incidents or operational issues.
* **Alerting and Escalation:** Automated alerts shall be generated for detected anomalies, triggering timely investigation and escalation to appropriate personnel or systems.

## Logging

* **Comprehensive Logging:** Detailed logs shall be maintained for all IoT devices and systems, capturing events such as:
  + Device authentication and authorisation attempts
  + Data access and modification activities
  + Network traffic patterns and communication logs
  + System and application events
* **Secure Log Storage:** Logs shall be stored securely and protected against unauthorised access or modification, utilising encryption and access controls.
* **Log Retention:** Logs shall be retained for a period defined by the organisation's data retention policy and any applicable regulatory requirements.
* **Log Analysis:** Logs shall be regularly analysed to identify trends, patterns, and potential security or operational issues.

# Responsibilities

* **Information Security Officer:** Responsible for overseeing the implementation and enforcement of this policy.
* **IT Department:** Responsible for deploying and managing anomaly detection tools and logging infrastructure.
* **Device Owners:** Responsible for ensuring that their IoT devices generate appropriate logs and that these logs are forwarded to the centralised logging system.
* **Security Operations Centre (SOC):** Responsible for monitoring alerts, investigating anomalies, and responding to security incidents.

# Breaches of Policy

Non-compliance with this policy 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