TrustIoT Framework for Industry 4.0

"Automated tools for real-time data provenance and anomaly detection"

|  |  |
| --- | --- |
| 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](#_Toc176332925)

[2. Purpose 4](#_Toc176332926)

[3. Scope 4](#_Toc176332927)

[4. Policy Statement 4](#_Toc176332928)

[4.1. Data Provenance Tools 4](#_Toc176332929)

[4.2. Anomaly Detection Tools 4](#_Toc176332930)

[4.3. Integration and Correlation 4](#_Toc176332931)

[5. Responsibilities 5](#_Toc176332932)

[6. Breaches of Policy 5](#_Toc176332933)

[7. Document Management 5](#_Toc176332934)

# Introduction

The Internet of Things (IoT) generates vast amounts of data at high velocities, making manual tracking and analysis of data provenance and anomalies impractical. Automated tools are essential to establish and maintain a clear record of data origin, movement, and modifications, as well as to detect any deviations from expected patterns that may indicate security breaches or operational issues. This policy outlines the requirements for implementing and utilising such tools within the organisation's IoT ecosystem.

# Purpose

The purpose of this policy is to establish guidelines for the deployment and utilisation of automated tools for real-time data provenance tracking and anomaly detection within the IoT environment. This policy aims to:

* Enable efficient and comprehensive tracking of data origin, movement, and modifications.
* Facilitate the identification and investigation of data breaches, anomalies, and security incidents.
* Proactively detect and respond to potential threats and operational issues.
* Enhance the overall security and reliability 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

## Data Provenance Tools

* **Data Lineage Tracking:** Automated tools shall be employed to track the lineage of data, capturing information about its origin, transformations, and destinations throughout its lifecycle.
* **Metadata Capture and Management:** Tools shall capture and manage relevant metadata associated with data, such as timestamps, user identities, device identifiers, and location information.
* **Tamper-Proof Logging:** Data provenance information shall be securely logged in a tamper-proof manner, ensuring its integrity and authenticity.

## Anomaly Detection Tools

* **Behavioural Analytics:** Tools shall utilise behavioural analytics and machine learning techniques to establish baseline patterns of normal activity and identify deviations that may indicate anomalies or potential threats.
* **Real-time Monitoring:** Anomaly detection shall be performed in real-time to enable prompt identification and response to security incidents or operational issues.
* **Thresholds and Alerts:** Appropriate thresholds and alerting mechanisms shall be configured to notify relevant personnel of detected anomalies.

## Integration and Correlation

* **Centralised Platform:** Data provenance and anomaly detection tools shall be integrated into a centralised platform or security information and event management (SIEM) system to enable correlation and analysis of events from multiple sources.
* **Threat Intelligence:** Threat intelligence feeds shall be integrated to enhance the detection of known attack patterns and indicators of compromise.

# Responsibilities

* **Information Security Officer:** Responsible for overseeing the implementation and enforcement of this policy.
* **IT Department:** Responsible for selecting, deploying, and managing data provenance and anomaly detection tools.
* **Data Owners:** Responsible for defining data sensitivity levels and ensuring appropriate provenance tracking and anomaly detection measures are in place for the data they own.
* **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