Internet of Things (IoT) Security Framework for Industry 4.0

"Provenance Tracking: Tools for tracking data origin and changes"

|  |  |
| --- | --- |
| 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](#_Toc176332892)

[2. Purpose 4](#_Toc176332893)

[3. Scope 4](#_Toc176332894)

[4. Policy Statement 4](#_Toc176332895)

[4.1. Logging and Auditing 4](#_Toc176332896)

[4.2. Metadata Management 4](#_Toc176332897)

[4.3. Immutable Storage 5](#_Toc176332898)

[4.4. Blockchain Technology 5](#_Toc176332899)

[5. Responsibilities 5](#_Toc176332900)

[6. Breaches of Policy 5](#_Toc176332901)

[7. Document Management 5](#_Toc176332902)

# Introduction

The Internet of Things (IoT) ecosystem generates and transmits vast amounts of data, the integrity and origin of which are crucial for ensuring the reliability, trustworthiness, and accountability of IoT systems. Data provenance, the ability to track the origin and history of data, is essential for understanding how data is collected, processed, and modified throughout its lifecycle. This document outlines the policies and procedures for establishing and maintaining clear data provenance within the IoT ecosystem.

# Purpose

The purpose of this policy is to establish clear guidelines and requirements for implementing data provenance tracking mechanisms for IoT devices and systems within the organisation. This policy aims to:

* Enable traceability and accountability for data actions and modifications.
* Facilitate the identification and investigation of data breaches or anomalies.
* Support compliance with regulatory requirements and industry standards related to data handling and accountability.
* Enhance the overall trustworthiness and reliability of IoT-generated data.

# Scope

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

* Sensor data
* Control commands
* Firmware updates
* Configuration files
* Log files

# Policy Statement

## Logging and Auditing

* **Comprehensive Logging:** Detailed logs shall be maintained to track the origin, movement, and modifications of data within the IoT ecosystem. This includes capturing information such as:
  + Data source (device or system)
  + Timestamps of data creation, transmission, and modification
  + User or system identities associated with data actions
  + Details of any data transformations or modifications
* **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, ensuring compliance with regulatory and legal requirements.

## Metadata Management

* **Metadata Capture:** Relevant metadata, such as timestamps, user identities, device identifiers, and location information, shall be associated with data to provide context and traceability.
* **Metadata Standards:** Standardised metadata formats and schemas shall be used to ensure consistency and interoperability across different IoT systems and platforms.
* **Metadata Storage:** Metadata shall be stored securely alongside the associated data, ensuring its integrity and availability for provenance tracking.

## Immutable Storage

* **Critical Data:** Critical data or logs that require tamper-proof storage may be stored in immutable storage solutions, such as write-once-read-many (WORM) storage or blockchain-based systems.
* **Data Protection:** Immutable storage solutions shall be implemented with appropriate security controls to prevent unauthorised access or deletion of data.

## Blockchain Technology

* **Consideration for Provenance:** Where appropriate and feasible, blockchain technology may be leveraged to create a decentralised and tamper-proof ledger for recording data provenance information.
* **Secure Implementation:** Blockchain solutions shall be implemented with robust security measures to protect against unauthorised access, manipulation, or denial-of-service attacks.

# Responsibilities

* **Information Security Officer:** Responsible for overseeing the implementation and enforcement of this policy.
* **IT Department:** Responsible for configuring and maintaining logging and auditing systems, metadata management solutions, and any blockchain implementations.
* **Data Owners:** Responsible for ensuring that appropriate data provenance tracking mechanisms are implemented for the data they own.
* **System Owners:** Responsible for ensuring that their systems support and enforce data provenance tracking for IoT data.

# 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