Internet of Things (IoT) Security Framework for Industry 4.0

"Data Integrity and Provenance"

|  |  |
| --- | --- |
| 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](#_Toc176332879)

[2. Purpose 4](#_Toc176332880)

[3. Scope 4](#_Toc176332881)

[4. Policy Statement 4](#_Toc176332882)

[4.1. Data Integrity Mechanisms 4](#_Toc176332883)

[4.2. Data Provenance Tracking 4](#_Toc176332884)

[5. Responsibilities 5](#_Toc176332885)

[6. Breaches of Policy 5](#_Toc176332886)

[7. Document Management 5](#_Toc176332887)

# 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 integrity guarantees that data remains accurate, complete, and unaltered during transmission and storage, while data provenance tracks the origin and history of data, enabling traceability and verification. This document outlines the policies and procedures for maintaining data integrity and establishing clear data provenance within the IoT ecosystem.

# Purpose

The purpose of this policy is to establish clear guidelines and requirements for ensuring the integrity and traceability of data generated, transmitted, or stored by IoT devices and systems within the organisation. This policy aims to:

* Ensure the accuracy and completeness of data throughout its lifecycle.
* Detect any unauthorised modification or tampering of data.
* Provide mechanisms for verifying the authenticity and origin of data.
* Maintain the trustworthiness of IoT-generated data for decision-making and operations.
* Enable traceability and accountability for data actions and modifications.

# 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

## Data Integrity Mechanisms

* **Hashing Algorithms:** Hashing algorithms shall be used to generate unique fingerprints (hashes) of data to verify its integrity.
* **Approved Algorithms:** Only strong and approved hashing algorithms, such as SHA-256 or SHA-3, shall be used.
* **Storage of Hashes:** Hashes shall be securely stored and protected against unauthorised modification.
* **Integrity Checks:** Regular integrity checks shall be performed to compare data hashes and detect any alterations.
* **Digital Signatures:** Digital signatures shall be used to authenticate the origin of data and ensure non-repudiation.
* **Key Management:** Robust key management practices shall be implemented to protect the private keys used for generating digital signatures.
* **Signature Verification:** Digital signatures shall be verified using the corresponding public keys to ensure the authenticity and integrity of data.

## Data Provenance Tracking

* **Logging and Auditing:** Detailed logs shall be maintained to track the origin, movement, and modifications of data within the IoT ecosystem.
* **Metadata:** Relevant metadata, such as timestamps, user identities, and device identifiers, shall be associated with data to provide context and traceability.
* **Immutable Storage:** Critical data or logs may be stored in immutable storage solutions to prevent unauthorised modification or deletion.
* **Blockchain Technology:** Where appropriate, blockchain technology may be leveraged to create a tamper-proof and auditable record of data provenance.

# Responsibilities

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