TrustIoT Framework for Industry 4.0

"Data Integrity Mechanisms: Hashing algorithms & digital signatures"

|  |  |
| --- | --- |
| 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](#_Toc176332130)

[2. Purpose 4](#_Toc176332131)

[3. Scope 4](#_Toc176332132)

[4. Policy Statement 4](#_Toc176332133)

[4.1. Hashing Algorithms 4](#_Toc176332134)

[4.2. Digital Signatures 4](#_Toc176332135)

[5. Responsibilities 4](#_Toc176332136)

[6. Breaches of Policy 5](#_Toc176332137)

[7. Document Management 5](#_Toc176332138)

# Introduction

The Internet of Things (IoT) generates and transmits vast amounts of data, the integrity of which is crucial for ensuring the reliability and trustworthiness of IoT systems. Data integrity ensures that data remains accurate, complete, and unaltered during transmission and storage. This document outlines the policies and procedures for utilising hashing algorithms and digital signatures to maintain the integrity of data within the IoT ecosystem.

# Purpose

The purpose of this policy is to establish clear guidelines and requirements for the implementation and management of data integrity mechanisms for 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.

# 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

## Hashing Algorithms

* **Data Verification:** 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

* **Authentication and Non-Repudiation:** 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.

# Responsibilities

* **Information Security Officer:** Responsible for overseeing the implementation and enforcement of this policy.
* **IT Department:** Responsible for configuring and maintaining the technical infrastructure to support data integrity mechanisms.
* **Device Owners:** Responsible for ensuring that their IoT devices implement appropriate data integrity mechanisms.
* **System Owners:** Responsible for ensuring that their systems validate the integrity of 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