TrustIoT Framework for Industry 4.0

"Data Integrity Checks: Checksums & 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](#_Toc176332907)

[2. Purpose 4](#_Toc176332908)

[3. Scope 4](#_Toc176332909)

[4. Policy Statement 4](#_Toc176332910)

[4.1. Checksums 4](#_Toc176332911)

[4.2. Digital Signatures 4](#_Toc176332912)

[5. Responsibilities 5](#_Toc176332913)

[6. Breaches of Policy 5](#_Toc176332914)

[7. Document Management 5](#_Toc176332915)

# Introduction

The Internet of Things (IoT) ecosystem 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, safeguarding against accidental corruption or malicious tampering. This document outlines the policies and procedures for utilising checksums 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 checks 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

## Checksums

* **Data Verification:** Checksum algorithms shall be used to generate a unique representation (checksum) of data to verify its integrity.
* **Approved Algorithms:** Only strong and approved checksum algorithms, such as CRC32, MD5, or SHA-256, shall be used, depending on the sensitivity and criticality of the data.
* **Calculation and Transmission:** Checksums shall be calculated before data transmission and included with the transmitted data.
* **Verification:** Upon receipt, the checksum shall be recalculated and compared to the transmitted checksum to verify data integrity.
* **Error Handling:** In case of checksum mismatch, appropriate error handling procedures shall be initiated, such as retransmission or notification of relevant personnel.

## Digital Signatures

* **Authentication and Non-Repudiation:** Digital signatures shall be used to authenticate the origin of data and ensure non-repudiation, providing evidence that the data has not been tampered with and originates from a trusted source.
* **Key Management:** Robust key management practices shall be implemented to protect the private keys used for generating digital signatures.
* **Signature Generation and Verification:** Digital signatures shall be generated using the sender's private key and verified using the corresponding public key.
* **Implementation:** Digital signatures shall be implemented using industry-standard algorithms and protocols, such as RSA or ECDSA.

# 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, including checksum generation and verification, and digital signature implementation.
* **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 using checksums or digital signatures.

# 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