TrustIoT Framework for Industry 4.0

"Data at Rest and in Transit: Encryption standards & key management"

|  |  |
| --- | --- |
| 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](#_Toc176332848)

[2. Purpose 4](#_Toc176332849)

[3. Scope 4](#_Toc176332850)

[4. Policy Statement 4](#_Toc176332851)

[4.1. Data at Rest 4](#_Toc176332852)

[4.2. Data in Transit 4](#_Toc176332853)

[4.3. Key Management 5](#_Toc176332854)

[5. Responsibilities 5](#_Toc176332855)

[6. Breaches of Policy 5](#_Toc176332856)

[7. Document Management 5](#_Toc176332857)

# Introduction

The Internet of Things (IoT) ecosystem generates, transmits, and stores vast amounts of data, often of a sensitive nature, including personally identifiable information (PII), operational data, and intellectual property. Protecting the confidentiality and integrity of this data, both when it is stored (at rest) and when it is being transmitted (in transit), is of paramount importance to maintain the trust of stakeholders and comply with data protection regulations. Encryption serves as a fundamental safeguard against unauthorised access and data breaches.

# Purpose

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

* Ensure the confidentiality of sensitive data generated, transmitted, or stored by IoT devices.
* Protect data integrity by preventing unauthorised modification or tampering.
* Comply with industry best practices and regulatory requirements regarding data protection.

# 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 at Rest

* **Sensitive Data Identification and Classification:** All data stored on IoT devices, edge gateways, or in associated storage systems shall be classified based on its sensitivity. Sensitive data shall be identified and appropriately marked.
* **Encryption of Sensitive Data:** All sensitive data at rest shall be encrypted using strong, industry-standard encryption algorithms.
* **Encryption Policy:** Encryption shall be implemented using approved algorithms, such as AES (Advanced Encryption Standard), with appropriate key lengths.
* **Key Protection:** Encryption keys shall be securely managed and protected against unauthorised access, utilising key management systems or hardware security modules (HSMs) where appropriate.

## Data in Transit

* **Network Communication:** All data transmitted between IoT devices and other network entities shall be encrypted using secure protocols, such as TLS (Transport Layer Security) or its datagram counterpart DTLS.
* **Strong Cipher Suites:** Communication protocols shall be configured with strong cipher suites and authentication mechanisms to ensure confidentiality and integrity.
* **Wireless Networks:** Wireless communication shall employ robust encryption protocols, such as WPA3, to protect against eavesdropping and unauthorised access.

## Key Management

* **Key Generation and Distribution:** Secure mechanisms shall be implemented for the generation, distribution, and storage of encryption keys.
* **Key Rotation:** Encryption keys shall be periodically rotated to minimise the impact of potential key compromise.
* **Key Revocation:** Procedures shall be in place to revoke compromised keys and re-encrypt data as necessary.

# Responsibilities

* **Information Security Officer:** Responsible for overseeing the implementation and enforcement of this policy.
* **IT Department:** Responsible for configuring and maintaining encryption mechanisms, key management systems, and secure communication protocols.
* **Data Owners:** Responsible for classifying data based on sensitivity and ensuring that appropriate encryption measures are applied.
* **System Owners:** Responsible for ensuring that their systems support and enforce data encryption 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