TrustIoT Framework for Industry 4.0

"Encryption Protocols "

|  |  |
| --- | --- |
| 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](#_Toc176332109)

[2. Purpose 4](#_Toc176332110)

[3. Scope 4](#_Toc176332111)

[4. Policy Statement 4](#_Toc176332112)

[4.1. Transport Layer Security (TLS) 4](#_Toc176332113)

[4.2. End-to-End Encryption (E2EE) 4](#_Toc176332114)

[5. Responsibilities 5](#_Toc176332115)

[6. Breaches of Policy 5](#_Toc176332116)

[7. Document Management 5](#_Toc176332117)

# Introduction

The Internet of Things (IoT) ecosystem involves the transmission of vast amounts of data between devices, often across public networks. This data can include sensitive information such as personally identifiable information (PII), operational data, and intellectual property. To safeguard this data from unauthorised access, interception, and tampering, robust encryption protocols must be employed. This document outlines the policies and procedures for utilising Transport Layer Security (TLS) and End-to-End Encryption (E2EE) to ensure the confidentiality and integrity of IoT communications.

# Purpose

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

* Protect the confidentiality of sensitive data transmitted by IoT devices.
* Maintain the integrity of data to prevent unauthorised modification or tampering.
* Ensure compliance with industry best practices and regulatory requirements regarding data protection.

# Scope

This policy applies to all communication channels used by IoT devices within the organisation's network, including but not limited to:

* Wired and wireless networks
* Local area networks (LANs) and wide area networks (WANs)
* Cloud-based communication platforms
* Application programming interfaces (APIs)

# Policy Statement

## Transport Layer Security (TLS)

* **Mandatory Use:** TLS shall be the default protocol for securing communication between IoT devices and other network entities.
* **Latest Version:** The latest version of TLS (currently TLS 1.3) or a similarly secure protocol shall be used.
* **Strong Cipher Suites:** TLS connections shall be configured with strong cipher suites that provide adequate protection against known attacks.
* **Certificate Management:** Valid and trusted digital certificates shall be used for server authentication and, where applicable, client authentication.
* **Regular Updates:** TLS implementations shall be regularly updated to address any newly discovered vulnerabilities.

## End-to-End Encryption (E2EE)

* **Sensitive Data:** E2EE shall be employed for protecting sensitive data transmitted between IoT devices and authorised endpoints.
* **Key Management:** Robust key management practices shall be implemented to ensure the secure generation, distribution, and storage of encryption keys.
* **Data Integrity:** E2EE implementations shall include mechanisms to ensure the integrity of data and detect any tampering attempts.

# 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 secure communication for IoT devices.
* **Device Owners:** Responsible for ensuring that their IoT devices comply with this policy.
* **Users:** Responsible for adhering to this policy and reporting any security incidents or concerns.

# 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