TrustIoT Framework for Industry 4.0

"Encrypted communication for low-power & resource-constrained devices"

|  |  |
| --- | --- |
| 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](#_Toc190893999)

[2. Purpose 4](#_Toc190894000)

[3. Scope 4](#_Toc190894001)

[4. Policy Statement 4](#_Toc190894002)

[4.1. Lightweight Cryptography 4](#_Toc190894003)

[4.2. Key Management 4](#_Toc190894004)

[4.3. Secure Protocols 4](#_Toc190894005)

[4.4. Data Minimisation 5](#_Toc190894006)

[5. Responsibilities 5](#_Toc190894007)

[6. Breaches of Policy 5](#_Toc190894008)

[7. Document Management 5](#_Toc190894009)

# Introduction

The proliferation of low-power, resource-constrained IoT devices presents unique challenges for ensuring secure communication. These devices often have limited processing power, memory, and battery life, making traditional encryption methods impractical. This document outlines the policies and procedures for implementing lightweight cryptography and other security measures to protect the confidentiality and integrity of data transmitted by such devices.

# Purpose

The purpose of this policy is to establish guidelines and requirements for securing communication channels used by low-power, resource-constrained IoT devices within the organisation. This policy aims to:

* Safeguard sensitive data transmitted by these devices, even with their inherent limitations.
* Maintain data integrity and prevent unauthorised modification or interception.
* Balance the need for security with the constraints of low-power, resource-constrained devices.
* Ensure compliance with industry best practices and regulatory requirements.

# Scope

This policy applies to all low-power, resource-constrained IoT devices connected to the organisation's network, including but not limited to:

* Sensors and actuators with limited processing capabilities
* Wearable devices with battery life constraints
* Embedded systems with minimal memory resources

# Policy Statement

## Lightweight Cryptography

* **Algorithm Selection:** Encryption algorithms specifically designed for low-power, resource-constrained devices shall be employed. Examples include:
  + Lightweight block ciphers (e.g., PRESENT, CLEFIA)
  + Stream ciphers (e.g., Grain, Trivium)
  + Elliptic Curve Cryptography (ECC) with optimised implementations
* **Key Sizes:** Appropriate key sizes shall be selected to balance security and performance, considering the constraints of the devices.

## Key Management

* **Secure Key Generation and Distribution:** Robust mechanisms shall be implemented for the secure generation and distribution of encryption keys to IoT devices.
* **Key Storage:** Keys shall be stored securely on the devices, utilising hardware-based security features where available.
* **Key Rotation:** Encryption keys shall be periodically rotated to minimise the impact of potential key compromise.

## Secure Protocols

* **Lightweight Protocols:** Communication protocols optimised for low-power, resource-constrained devices shall be utilised. Examples include:
  + Constrained Application Protocol (CoAP)
  + Message Queuing Telemetry Transport (MQTT) with TLS
* **Protocol Security:** Secure protocol versions and configurations shall be enforced, including the use of strong cipher suites and authentication mechanisms.

## Data Minimisation

* **Essential Data Only:** Only essential data necessary for the device's functionality shall be transmitted, reducing the amount of data that needs to be encrypted and transmitted.
* **Data Aggregation:** Where possible, data aggregation and processing shall be performed at edge gateways or in the cloud to reduce the communication overhead on constrained devices.

# Responsibilities

* **Information Security Officer:** Responsible for overseeing the implementation and enforcement of this policy.
* **IT Department:** Responsible for selecting and configuring appropriate encryption protocols and key management solutions.
* **Device Manufacturers/Vendors:** Responsible for implementing secure communication capabilities in their devices.
* **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