TrustIoT Framework for Industry 4.0

"Secure Network 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](#_Toc176333243)

[2. Purpose 4](#_Toc176333244)

[3. Scope 4](#_Toc176333245)

[4. Policy Statement 4](#_Toc176333246)

[4.1. Protocol Selection and Configuration 4](#_Toc176333247)

[4.2. Encryption and Authentication 4](#_Toc176333248)

[4.3. Secure Key Exchange and Management 4](#_Toc176333249)

[4.4. Vulnerability Management and Patching 5](#_Toc176333250)

[5. Responsibilities 5](#_Toc176333251)

[6. Breaches of Policy 5](#_Toc176333252)

[7. Document Management 5](#_Toc176333253)

# Introduction

The proliferation of Internet of Things (IoT) devices has led to an exponential increase in network traffic and data exchange. Ensuring the security and integrity of this communication is paramount to protect sensitive information, maintain operational continuity, and prevent unauthorised access. This document outlines the policies and procedures for selecting, configuring, and managing secure network protocols for IoT devices within the organisation.

# Purpose

The purpose of this policy is to establish guidelines and requirements for the use of secure network protocols in the context of IoT communication. This policy aims to:

* Protect the confidentiality of data transmitted between IoT devices and other network entities.
* Ensure the integrity of data by preventing unauthorised modification or tampering during transmission.
* Provide authentication mechanisms to verify the identity of communicating parties.
* Mitigate the risk of unauthorised access, eavesdropping, and man-in-the-middle attacks.

# 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

## Protocol Selection and Configuration

* **Secure Protocols:** Only secure network protocols that provide confidentiality, integrity, and authentication shall be used for IoT communication. Examples include:
  + Transport Layer Security (TLS) 1.2 or later
  + Datagram Transport Layer Security (DTLS) 1.2 or later
  + Secure Shell (SSH)
  + HTTPS (HTTP over TLS)
* **Protocol Configuration:** Secure protocols shall be configured with strong cipher suites, appropriate key exchange mechanisms, and mutual authentication where feasible.
* **Legacy Protocols:** The use of legacy or insecure protocols, such as Telnet or FTP, shall be prohibited for IoT communication.

## Encryption and Authentication

* **Data Encryption:** All sensitive data transmitted between IoT devices and other network entities shall be encrypted using strong encryption algorithms and protocols.
* **Device and Server Authentication:** Both IoT devices and servers shall be authenticated using digital certificates or other robust authentication mechanisms.
* **Mutual Authentication:** Where applicable, mutual authentication shall be implemented to ensure both the IoT device and the server verify each other's identity.

## Secure Key Exchange and Management

* **Key Exchange Protocols:** Secure key exchange protocols, such as Diffie-Hellman or Elliptic Curve Diffie-Hellman (ECDH), shall be used to establish secure communication channels.
* **Key Management:** Robust key management practices shall be implemented, including:
  + Secure generation and storage of keys
  + Periodic key rotation
  + Revocation of compromised keys

## Vulnerability Management and Patching

* **Regular Assessments:** Network protocols and their implementations shall be regularly assessed for vulnerabilities using automated tools and manual reviews.
* **Timely Patching:** Identified vulnerabilities shall be addressed promptly by applying patches or updates from trusted sources.
* **Zero-Day Vulnerabilities:** Procedures shall be in place to respond to and mitigate the risks associated with zero-day vulnerabilities in network protocols.

# Responsibilities

* **Information Security Officer:** Responsible for overseeing the implementation and enforcement of this policy.
* **Network Administrators:** Responsible for configuring and managing network protocols and security devices.
* **Device Owners:** Responsible for ensuring that their IoT devices utilise secure network protocols and are configured in compliance with this policy.
* **IT Security Team:** Responsible for conducting vulnerability assessments and implementing security patches.

# 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