TrustIoT Framework for Industry 4.0

"Security guidelines for emerging 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](#_Toc176333257)

[2. Purpose 4](#_Toc176333258)

[3. Scope 4](#_Toc176333259)

[4. Policy Statement 4](#_Toc176333260)

[4.1. Risk Assessment and Evaluation 4](#_Toc176333261)

[4.2. Security Requirements and Controls 4](#_Toc176333262)

[4.3. Protocol Testing and Validation 4](#_Toc176333263)

[4.4. Vendor Due Diligence 5](#_Toc176333264)

[4.5. Monitoring and Incident Response 5](#_Toc176333265)

[5. Responsibilities 5](#_Toc176333266)

[6. Breaches of Policy 5](#_Toc176333267)

[7. Document Management 5](#_Toc176333268)

# Introduction

The rapid evolution of the Internet of Things (IoT) ecosystem often necessitates the adoption of emerging network protocols to support new functionalities, improve performance, or address specific use cases. However, these emerging protocols may introduce novel security challenges and vulnerabilities. This policy outlines the guidelines and procedures for evaluating and securely integrating emerging network protocols into the organisation's IoT infrastructure.

# Purpose

The purpose of this policy is to establish a framework for assessing and managing the security risks associated with the adoption of emerging network protocols for IoT devices and systems. This policy aims to:

* Ensure that emerging network protocols are thoroughly evaluated for security risks before deployment.
* Implement appropriate security controls to mitigate identified risks.
* Maintain the confidentiality, integrity, and availability of data transmitted over emerging protocols.
* Enable the secure and controlled adoption of new technologies while minimising potential security vulnerabilities.

# Scope

This policy applies to all emerging network protocols considered for adoption or deployment within the organisation's IoT infrastructure. This includes, but is not limited to:

* New or experimental protocols not yet widely adopted or standardised.
* Protocols undergoing significant revisions or updates.
* Protocols designed for specific IoT use cases or industries.

# Policy Statement

## Risk Assessment and Evaluation

* **Thorough Evaluation:** Prior to adoption, emerging network protocols shall undergo a comprehensive security assessment, considering factors such as:
  + Encryption and authentication mechanisms
  + Key management practices
  + Vulnerability to known attack vectors
  + Compatibility with existing security infrastructure
* **Proof of Concept:** A proof of concept (POC) may be conducted in a controlled environment to evaluate the protocol's security and performance in real-world scenarios.

## Security Requirements and Controls

* **Minimum Security Standards:** Emerging protocols must meet or exceed the organisation's minimum-security standards for data confidentiality, integrity, and availability.
* **Compensating Controls:** If a protocol does not fully meet the security standards, compensating controls shall be implemented to mitigate the identified risks.
* **Secure Configuration:** Protocols shall be configured securely, following vendor recommendations and industry best practices.

## Protocol Testing and Validation

* **Security Testing:** Emerging protocols shall undergo rigorous security testing, including vulnerability scanning, penetration testing, and fuzzing, to identify and address potential weaknesses.
* **Performance Testing:** Performance testing shall be conducted to ensure that the protocol can handle the expected data volumes and traffic patterns without impacting the overall system performance.

## Vendor Due Diligence

* **Vendor Assessment:** The security posture and track record of vendors providing emerging protocols shall be evaluated before adoption.
* **Support and Updates:** Vendors shall demonstrate a commitment to providing ongoing support and security updates for their protocols.

## Monitoring and Incident Response

* **Network Monitoring:** Traffic utilising emerging protocols shall be monitored for suspicious activity or anomalies.
* **Incident Response:** Procedures shall be in place to respond to and investigate security incidents involving emerging protocols.

# Responsibilities

* **Information Security Officer:** Responsible for overseeing the implementation and enforcement of this policy.
* **IT Department:** Responsible for evaluating, testing, and deploying emerging network protocols.
* **Network Administrators:** Responsible for configuring and managing network infrastructure to support secure protocol implementation.
* **Security Operations Centre (SOC):** Responsible for monitoring network traffic and responding to security incidents.

# 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