TrustIoT Framework for Industry 4.0

"Data Sharing Mechanisms - Secure APIs & data anonymisation"

|  |  |
| --- | --- |
| 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](#_Toc190896105)

[2. Purpose 4](#_Toc190896106)

[3. Scope 4](#_Toc190896107)

[4. Policy Statement 4](#_Toc190896108)

[4.1. Secure APIs 4](#_Toc190896109)

[4.2. Data Anonymisation and Pseudonymisation 4](#_Toc190896110)

[5. Responsibilities 5](#_Toc190896111)

[6. Breaches of Policy 5](#_Toc190896112)

[7. Document Management 5](#_Toc190896113)

# Introduction

The Internet of Things (IoT) ecosystem generates and manages vast amounts of data, which often needs to be shared internally and externally to enable various business functions and collaborations. However, the sensitive nature of some IoT data necessitates secure and controlled sharing mechanisms. This document outlines the policies and procedures for utilising secure APIs and data anonymisation techniques to facilitate safe and compliant data sharing practices within the organisation.

# Purpose

The purpose of this policy is to define guidelines and requirements for secure and controlled sharing of IoT data within and outside the organisation. This policy aims to:

* Facilitate secure data sharing while preserving confidentiality and integrity.
* Protect the privacy of individuals by minimising the exposure of personally identifiable information (PII).
* Ensure compliance with relevant data protection regulations and industry standards.
* Enable authorised access to IoT data for legitimate purposes.

# Scope

This policy applies to all data generated, transmitted, or stored by IoT devices and systems within the organisation's network, and intended for sharing with internal or external parties. This includes, but is not limited to:

* Sensor data
* Operational data
* Personally Identifiable Information (PII)
* Any other data collected or processed by IoT devices

# Policy Statement

## Secure APIs

* **API Access Control:** Access to APIs shall be restricted to authorised individuals and systems based on their roles and responsibilities.
* **Authentication and Authorisation:** Strong authentication and authorisation mechanisms, such as API keys, OAuth, or OpenID Connect, shall be implemented to verify the identity and permissions of API consumers.
* **Input Validation and Sanitisation:** All API inputs shall be rigorously validated and sanitised to prevent injection attacks and other vulnerabilities.
* **Encryption:** Sensitive data transmitted through APIs shall be encrypted using industry-standard encryption protocols, such as TLS 1.3.
* **Logging and Monitoring:** API access and usage shall be logged and monitored for suspicious activity or potential security breaches.

## Data Anonymisation and Pseudonymisation

* **Privacy Protection:** Before sharing IoT data, personally identifiable information (PII) shall be anonymised or pseudonymised to protect the privacy of individuals.
* **Anonymisation:** Anonymisation involves removing or modifying PII in a way that makes it impossible to re-identify individuals.
* **Pseudonymisation:** Pseudonymisation involves replacing PII with artificial identifiers or pseudonyms, allowing for data analysis while protecting individual privacy.
* **Re-identification Risk:** The risk of re-identification shall be assessed before sharing anonymised or pseudonymised data, and appropriate safeguards shall be implemented to minimise this risk.

# Responsibilities

* **Information Security Officer:** Responsible for overseeing the implementation and enforcement of this policy.
* **Data Owners:** Responsible for classifying data, defining access levels, and authorising data sharing.
* **IT Department:** Responsible for implementing and maintaining secure APIs and data anonymisation/pseudonymisation tools.
* **API Developers:** Responsible for designing and implementing APIs in accordance with security best practices.
* **Users:** Responsible for adhering to this policy and sharing IoT data only through authorised channels and with appropriate anonymisation or pseudonymisation.

# Breaches of Policy

Non-compliance with this policy may result in disciplinary action, up to and including termination of employment or contractual relationships. Additionally, breaches of data protection regulations may result in legal and financial penalties for the organisation.

# 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