Internet of Things (IoT) Security Framework for Industry 4.0

"Standardised data schemas for industrial IoT data interoperability"

|  |  |
| --- | --- |
| Document Classification: | Internal |
| Document Ref. | *Internet of Things (IoT) Security 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](#_Toc190898029)

[2. Purpose 4](#_Toc190898030)

[3. Scope 4](#_Toc190898031)

[4. Policy Statement 4](#_Toc190898032)

[4.1. Adoption of Standardised Schemas 4](#_Toc190898033)

[4.2. Schema Design and Development 4](#_Toc190898034)

[4.3. Data Validation and Transformation 5](#_Toc190898035)

[4.4. Version Control and Management 5](#_Toc190898036)

[5. Responsibilities 5](#_Toc190898037)

[6. Breaches of Policy 5](#_Toc190898038)

[7. Document Management 5](#_Toc190898039)

# Introduction

The Industrial Internet of Things (IIoT) generates vast amounts of data from diverse sources, including sensors, machines, and control systems. Ensuring seamless interoperability and efficient data exchange between these disparate systems necessitates the adoption of standardised data schemas. These schemas provide a common structure and vocabulary for representing and interpreting data, facilitating integration and analysis across the IIoT landscape.

# Purpose

The purpose of this policy is to establish guidelines and requirements for the use of standardised data schemas to promote interoperability and data exchange within the organisation's industrial IoT environment. This policy aims to:

* Facilitate seamless communication and data sharing between different IIoT systems and applications.
* Ensure data consistency, accuracy, and meaningfulness across the IIoT ecosystem.
* Streamline data integration and analysis processes.
* Support the development of scalable and maintainable IIoT solutions.

# Scope

This policy applies to all data generated, transmitted, or stored by IIoT devices and systems within the organisation. This includes, but is not limited to:

* Sensor data and machine logs
* Production and manufacturing data
* Equipment and asset information
* Environmental and operational data

# Policy Statement

## Adoption of Standardised Schemas

* **Industry Standards:** The organisation shall prioritise the use of widely adopted and recognised industry standards for IIoT data schemas, such as those defined by:
  + OPC Unified Architecture (OPC UA)
  + Industrial Internet Consortium (IIC)
  + Platform Industries 4.0
* **Open Standards:** Open standards shall be preferred over proprietary schemas to promote interoperability and avoid vendor lock-in.
* **Consistency:** Consistent use of standardised schemas shall be enforced across all IIoT systems and applications to ensure seamless data exchange and integration.

## Schema Design and Development

* **Data Modelling:** Data schemas shall be designed based on a thorough understanding of the data requirements and use cases within the industrial IoT environment.
* **Semantic Clarity:** Schemas shall use clear and unambiguous terminology to define data elements and their relationships, ensuring consistent interpretation across systems.
* **Extensibility:** Schemas shall be designed to be extensible, allowing for future additions or modifications without disrupting existing integrations.

## Data Validation and Transformation

* **Schema Validation:** Data received from IIoT devices and systems shall be validated against the defined schemas to ensure its correctness and integrity.
* **Data Transformation:** Where necessary, data transformation tools or processes shall be implemented to convert data between different schemas or formats, ensuring compatibility and interoperability.

## Version Control and Management

* **Versioning:** Data schemas shall be versioned to track changes and maintain compatibility with existing systems and applications.
* **Schema Registry:** A centralised schema registry may be established to store and manage schema definitions, facilitating version control and access by authorised systems.

# Responsibilities

* **Information Security Officer:** Responsible for overseeing the implementation and enforcement of this policy.
* **IT Department:** Responsible for defining and promoting the use of standardised data schemas within the organisation.
* **System Architects and Developers:** Responsible for designing and implementing IIoT systems that adhere to the data schema standards outlined in this policy.
* **Data Analysts:** Responsible for ensuring that data received from IIoT devices is properly validated and transformed according to the defined schemas.

# 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