Internet of Things (IoT) Security Framework for Industry 4.0

"Industry-specific privacy requirements for industrial data"

|  |  |
| --- | --- |
| 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](#_Toc190895829)

[2. Purpose 4](#_Toc190895830)

[3. Scope 4](#_Toc190895831)

[4. Policy Statement 4](#_Toc190895832)

[4.1. Data Classification and Handling 4](#_Toc190895833)

[4.2. Consent and Transparency 4](#_Toc190895834)

[4.3. Data Security and Access Control 5](#_Toc190895835)

[4.4. Anonymisation and De-identification 5](#_Toc190895836)

[4.5. Data Retention and Disposal 5](#_Toc190895837)

[5. Responsibilities 5](#_Toc190895838)

[6. Breaches of Policy 5](#_Toc190895839)

[7. Document Management 5](#_Toc190895840)

# Introduction

Industrial data, while crucial for operational efficiency and innovation, often encompasses sensitive information related to individuals, processes, and intellectual property. Ensuring the privacy and protection of this data is paramount to maintaining trust, complying with regulations, and safeguarding competitive advantage. This policy outlines the specific privacy requirements and considerations for handling industrial data within the context of the organisation's operations.

# Purpose

The purpose of this policy is to establish a framework for protecting the privacy and confidentiality of industrial data, including any personally identifiable information (PII) it may contain, and ensuring compliance with relevant industry-specific regulations and data protection laws. This policy aims to:

* Establish clear guidelines for the collection, processing, storage, and sharing of industrial data.
* Implement appropriate technical and organisational measures to safeguard industrial data against unauthorised access, disclosure, or misuse.
* Promote transparency and accountability in data handling practices.
* Ensure compliance with industry-specific regulations and maintain the trust of stakeholders.

# Scope

This policy applies to all industrial data generated, collected, processed, or stored by the organisation, regardless of the format or medium. This includes, but is not limited to:

* Sensor data and machine logs
* Production and manufacturing data
* Employee and customer information related to industrial processes
* Research and development data
* Any other data generated or used in the context of industrial operations

# Policy Statement

## Data Classification and Handling

* **Data Classification:** Industrial data shall be classified based on its sensitivity and the potential impact of its unauthorised disclosure. Appropriate handling procedures shall be defined for each data classification level.
* **Data Minimisation:** The collection and processing of industrial data shall be limited to only what is necessary for specific, explicit, and legitimate purposes.
* **Purpose Limitation:** Industrial data shall not be further processed in a manner that is incompatible with the original purposes for which it was collected.
* **Storage and Retention:** Industrial data shall be stored securely and retained only for as long as necessary to fulfil the specified purposes or as required by law.

## Consent and Transparency

* **Informed Consent:** Where applicable, explicit and informed consent shall be obtained from individuals before collecting or processing their personal data in the context of industrial operations.
* **Transparency:** Clear and concise information shall be provided to individuals about the purposes of data collection and processing, the types of data collected, and any third parties with whom the data may be shared.
* **Data Subject Access Requests:** Procedures shall be in place to handle data subject access requests, allowing individuals to access, rectify, or erase their personal data in accordance with applicable regulations.

## Data Security and Access Control

* **Security Measures:** Appropriate technical and organisational measures shall be implemented to protect industrial data against unauthorised access, loss, alteration, or destruction.
* **Access Control:** Access to industrial data shall be restricted to authorised personnel on a need-to-know basis, utilising role-based access control (RBAC) or similar mechanisms.
* **Encryption:** Sensitive industrial data, especially when transmitted over networks or stored in cloud environments, shall be encrypted using strong encryption algorithms and protocols.

## Anonymisation and De-identification

* **Privacy Enhancement:** Where feasible, data anonymisation or pseudonymisation techniques shall be employed to minimise the risk of identifying individuals from industrial data.
* **Aggregation and Statistical Analysis:** Aggregated or statistical data that does not allow for the identification of individuals may be used for research, analysis, or reporting purposes.

## Data Retention and Disposal

* **Data Retention Schedule:** A data retention schedule shall be established and maintained, specifying the retention periods for different types of industrial data based on legal, regulatory, and business requirements.
* **Secure Disposal:** Industrial data shall be securely disposed of when no longer needed, using appropriate data destruction methods to prevent unauthorised access or recovery.

# Responsibilities

* **Data Protection Officer (DPO):** Responsible for overseeing the organisation's compliance with privacy regulations and this policy.
* **IT Department:** Responsible for implementing technical measures to protect industrial data and ensure privacy compliance.
* **Legal Department:** Responsible for providing legal advice and guidance on industry-specific privacy regulations.
* **Department Heads:** Responsible for ensuring that their departments comply with this policy and handle industrial data in a privacy-conscious manner.

# 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 privacy 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