Internet of Things (IoT) Security Framework for Industry 4.0

"Data Access and Sharing"

|  |  |
| --- | --- |
| 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](#_Toc176333007)

[2. Purpose 4](#_Toc176333008)

[3. Scope 4](#_Toc176333009)

[4. Policy Statement 4](#_Toc176333010)

[4.1. Data Classification and Access Levels 4](#_Toc176333011)

[4.2. Data Sharing and Transfer 4](#_Toc176333012)

[4.3. Third-Party Access 4](#_Toc176333013)

[4.4. Data Retention and Disposal 5](#_Toc176333014)

[5. Responsibilities 5](#_Toc176333015)

[6. Breaches of Policy 5](#_Toc176333016)

[7. Document Management 5](#_Toc176333017)

# Introduction

The Internet of Things (IoT) ecosystem generates and manages vast amounts of data, varying in sensitivity and criticality. Ensuring appropriate access and controlled sharing of this data is essential to protect confidentiality, maintain integrity, and comply with relevant regulations. This policy establishes a framework for governing data access and sharing practices within the organisation's IoT environment.

# Purpose

The purpose of this policy is to define guidelines and procedures for controlling access to and sharing of IoT data within the organisation. This policy aims to:

* Ensure that only authorised individuals and systems have access to IoT data based on their roles and responsibilities.
* Safeguard the confidentiality and integrity of IoT data by implementing appropriate access controls and data sharing mechanisms.
* Comply with relevant data protection regulations and industry standards.
* Facilitate secure and controlled data sharing with internal and external parties when necessary.

# Scope

This policy applies to all data generated, transmitted, or stored by IoT devices and systems within the organisation's network. 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

## Data Classification and Access Levels

* **Data Classification:** IoT data shall be classified based on its sensitivity and the potential impact of unauthorised access or disclosure.
* **Access Levels:** Access levels shall be defined for each data classification, specifying which roles or individuals are authorised to access, modify, or share the data.
* **Access Control Mechanisms:** Appropriate access control mechanisms, such as role-based access control (RBAC) or attribute-based access control (ABAC), shall be implemented to enforce access restrictions.

## Data Sharing and Transfer

* **Internal Sharing:** Data sharing within the organisation shall be conducted through secure channels and in accordance with defined access control policies.
* **External Sharing:** Sharing of IoT data with external parties shall be subject to prior authorisation and shall comply with relevant contractual agreements and data protection regulations.
* **Secure Transfer:** Data transfers shall be conducted using secure protocols and encryption mechanisms to protect data confidentiality and integrity.

## Third-Party Access

* **Due Diligence:** Third-party organisations requiring access to IoT data shall undergo a due diligence process to assess their security practices and data handling capabilities.
* **Data Processing Agreements:** Data processing agreements shall be established with third parties, outlining their responsibilities and obligations regarding data protection and confidentiality.
* **Access Monitoring:** Access by third parties shall be monitored and logged to ensure compliance with this policy and contractual agreements.

## Data Retention and Disposal

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

# 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 access control mechanisms and secure data transfer protocols.
* **Legal Department:** Responsible for providing legal advice and guidance on data protection regulations and contractual agreements.
* **Users:** Responsible for adhering to this policy and handling IoT data in accordance with defined access controls.

# 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