Internet of Things (IoT) Security Framework for Industry 4.0

"Secure Data Sharing for AI Collaboration"

|  |  |
| --- | --- |
| 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](#_Toc190905766)

[2. Purpose 4](#_Toc190905767)

[3. Scope 4](#_Toc190905768)

[4. Policy Statement 4](#_Toc190905769)

[4.1. Data Sharing Agreements 4](#_Toc190905770)

[4.2. Data Minimisation and Anonymisation 4](#_Toc190905771)

[4.3. Secure Data Transfer Mechanisms 4](#_Toc190905772)

[4.4. Access Control and Monitoring 5](#_Toc190905773)

[5. Responsibilities 5](#_Toc190905774)

[6. Breaches of Policy 5](#_Toc190905775)

[7. Document Management 5](#_Toc190905776)

# Introduction

Collaboration in the development and deployment of Artificial Intelligence (AI) often necessitates the sharing of data between organisations. However, this data sharing must be conducted securely to protect sensitive information, maintain data ownership, and comply with relevant privacy regulations. This policy outlines the procedures and controls to ensure the secure and controlled sharing of data for AI collaboration purposes.

# Purpose

The purpose of this policy is to establish a framework for secure and compliant data sharing practices for AI collaboration within the organisation. This policy aims to:

* Facilitate collaborative AI development while safeguarding data confidentiality, integrity, and ownership.
* Protect the privacy of individuals by minimising the exposure of personally identifiable information (PII).
* Ensure compliance with relevant data protection regulations and contractual obligations.
* Establish clear guidelines and procedures for data sharing with external partners.

# Scope

This policy applies to all data sharing activities related to AI collaboration, involving the exchange of data between the organisation and external partners, including but not limited to:

* Sharing of datasets for model training and validation
* Exchange of model outputs and insights
* Collaborative development and testing of AI algorithms

# Policy Statement

## Data Sharing Agreements

* **Formal Agreements:** Data sharing for AI collaboration shall be governed by formal agreements that clearly define the terms and conditions of data sharing, including:
  + Purpose and scope of data sharing
  + Data ownership and usage restrictions
  + Data protection and security requirements
  + Confidentiality and non-disclosure obligations
  + Data retention and destruction guidelines
* **Legal Review:** Data sharing agreements shall be reviewed and approved by the legal department to ensure compliance with applicable laws and regulations.

## Data Minimisation and Anonymisation

* **Need-to-Know Basis:** Only the minimum necessary data required for the specific AI collaboration purpose shall be shared.
* **Anonymisation and Pseudonymisation:** Where feasible, data anonymisation or pseudonymisation techniques shall be employed to minimise the risk of identifying individuals from shared data.
* **Re-identification Risk Assessment:** The risk of re-identification shall be assessed before sharing anonymised or pseudonymised data, and appropriate safeguards shall be implemented to mitigate this risk.

## Secure Data Transfer Mechanisms

* **Secure Channels:** Data sharing shall be conducted through secure and encrypted channels, utilising industry-standard protocols such as HTTPS, SFTP, or dedicated secure file transfer solutions.
* **Access Controls:** Access to shared data shall be restricted to authorised personnel and systems at both the sending and receiving organisations, utilising strong authentication and authorisation mechanisms.

## Access Control and Monitoring

* **Data Access Agreements:** Data access agreements shall be established with external partners, outlining their responsibilities and obligations regarding data protection and confidentiality.
* **Access Monitoring and Logging:** Access to and usage of shared data shall be monitored and logged to ensure compliance with data sharing agreements and detect any unauthorised activity.

# 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 for AI collaboration purposes.
* **IT Department:** Responsible for implementing and maintaining secure data transfer mechanisms and access control systems.
* **Legal Department:** Responsible for reviewing and approving data sharing agreements and providing legal advice on data protection and privacy matters.
* **Project Managers:** Responsible for ensuring that AI collaboration projects adhere to this policy and data sharing agreements.

# Breaches of Policy

Non-compliance with this policy may result in disciplinary action, up to and including termination of employment or contractual relationships. Additionally, unauthorised sharing or misuse of data 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