TrustIoT Framework for Industry 4.0

"Data Security for AI"

|  |  |
| --- | --- |
| 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](#_Toc190905495)

[2. Purpose 4](#_Toc190905496)

[3. Scope 4](#_Toc190905497)

[4. Policy Statement 4](#_Toc190905498)

[4.1. Data Classification and Protection 4](#_Toc190905499)

[4.2. Data Access Control 4](#_Toc190905500)

[4.3. Data Encryption 4](#_Toc190905501)

[4.4. Data Minimisation and Anonymisation 5](#_Toc190905502)

[4.5. Secure Data Sharing and Transfer 5](#_Toc190905503)

[5. Responsibilities 5](#_Toc190905504)

[6. Breaches of Policy 5](#_Toc190905505)

[7. Document Management 5](#_Toc190905506)

# Introduction

Artificial Intelligence (AI) and Machine Learning (ML) models rely heavily on data for training, inference, and continuous improvement. This data, often collected and processed by IoT devices, can include sensitive information such as personally identifiable information (PII), operational data, and intellectual property. Ensuring the security and privacy of this data is paramount to maintaining trust, complying with regulations, and protecting the organisation's assets. This policy outlines the measures to be taken to safeguard IoT data used for AI purposes.

# Purpose

The purpose of this policy is to establish a framework for protecting the confidentiality, integrity, and availability of IoT data used for AI and ML purposes within the organisation. This policy aims to:

* Ensure that IoT data used for AI is classified, handled, and protected in accordance with its sensitivity and applicable regulations.
* Restrict access to IoT data to authorised personnel and systems only.
* Implement appropriate security measures to protect data at rest and in transit.
* Minimise the collection and retention of unnecessary data.
* Facilitate secure and controlled data sharing and transfer.

# Scope

This policy applies to all data generated, collected, processed, or stored by IoT devices and systems within the organisation that is used for AI and ML purposes. This includes, but is not limited to:

* Training data used to develop and train AI models
* Input data used for real-time inference and decision-making
* Output data generated by AI models
* Any other data relevant to the development, deployment, or operation of AI models in the IoT environment

# Policy Statement

## Data Classification and Protection

* **Data Classification:** IoT data shall be classified based on its sensitivity and the potential impact of unauthorised access or disclosure. Appropriate data protection measures shall be applied based on the data classification.
* **Sensitive Data:** Sensitive data, such as PII, shall be subject to stricter access controls and encryption requirements.

## Data Access Control

* **Role-Based Access Control (RBAC):** Access to IoT data shall be granted based on user roles and responsibilities within the organisation, utilising RBAC or similar mechanisms.
* **Need-to-Know Basis:** Access shall be granted on a need-to-know basis, limiting exposure to sensitive data.
* **Data Sharing Agreements:** Data sharing with external parties shall be governed by formal agreements that outline data protection and confidentiality requirements.

## Data Encryption

* **Data at Rest:** Sensitive data stored on IoT devices, edge gateways, or in associated storage systems shall be encrypted using strong encryption algorithms.
* **Data in Transit:** Data transmitted between IoT devices and other systems shall be encrypted using secure protocols, such as TLS (Transport Layer Security).

## Data Minimisation and Anonymisation

* **Data Minimisation:** The collection and retention of IoT data shall be limited to only what is necessary for the specified AI purposes.
* **Anonymisation and Pseudonymisation:** Where feasible, data anonymisation or pseudonymisation techniques shall be employed to minimise the risk of identifying individuals from collected data.

## Secure Data Sharing and Transfer

* **Secure Channels:** Data sharing and transfer shall be conducted through secure channels, utilising encryption and authentication mechanisms.
* **Data Transfer Agreements:** Data transfers to third parties shall be governed by formal agreements that outline data protection and confidentiality requirements.

# Responsibilities

* **Information Security Officer:** Responsible for overseeing the implementation and enforcement of this policy.
* **Data Scientists and AI Developers:** Responsible for handling IoT data in accordance with this policy and implementing appropriate data protection measures.
* **IT Department:** Responsible for providing secure infrastructure and tools for data storage, transmission, and access control.
* **Data Owners:** Responsible for classifying data and defining access control policies.

# 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