Internet of Things (IoT) Security Framework for Industry 4.0

"Data Privacy in AI Applications"

|  |  |
| --- | --- |
| 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](#_Toc190905693)

[2. Purpose 4](#_Toc190905694)

[3. Scope 4](#_Toc190905695)

[4. Policy Statement 4](#_Toc190905696)

[4.1. Lawful and Transparent Processing 4](#_Toc190905697)

[4.2. Data Minimisation 4](#_Toc190905698)

[4.3. Purpose Limitation 5](#_Toc190905699)

[4.4. Data Subject Rights 5](#_Toc190905700)

[4.5. Security of AI Data 5](#_Toc190905701)

[5. Responsibilities 5](#_Toc190905702)

[6. Breaches of Policy 5](#_Toc190905703)

[7. Document Management 6](#_Toc190905704)

# Introduction

The convergence of the Internet of Things (IoT) and Artificial Intelligence (AI) presents unique challenges and opportunities in the realm of data privacy. IoT devices generate vast amounts of data, which, when used for AI applications, can lead to insights and automation but also raise concerns about the collection, storage, and processing of personal and sensitive information. This policy outlines the organisation's commitment to ensuring data privacy compliance when leveraging IoT data for AI applications, particularly in industrial settings.

# Purpose

The purpose of this policy is to establish a framework for protecting the privacy of individuals and ensuring compliance with applicable data privacy regulations when collecting, storing, and processing data for AI applications in industrial settings. This policy aims to:

* Establish transparent and ethical data handling practices.
* Obtain and manage user consent for data collection and processing.
* Respect and uphold the rights of individuals regarding their personal data.
* Implement appropriate security measures to protect personal data.
* Ensure accountability and compliance with privacy regulations.

# Scope

This policy applies to all IoT devices and systems within the organisation that collect, process, or transmit data used for AI applications in industrial settings. This includes, but is not limited to:

* Sensors and actuators collecting data on employee behaviour or movements
* Cameras and surveillance systems capturing images or videos of individuals
* Biometric devices collecting fingerprint or facial recognition data
* Any other IoT system that handles personal data in an industrial context

# Policy Statement

## Lawful and Transparent Processing

* **Legal Basis:** Personal data shall only be collected and processed when there is a lawful basis for doing so under applicable data protection regulations, such as:
  + Explicit consent
  + Contractual necessity
  + Legal obligation
  + Legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject
* **Transparency:** Individuals shall be informed in a clear and concise manner 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 Minimisation

* **Minimal Collection:** Only the minimum necessary personal data shall be collected to fulfil the specified purposes of the AI application.
* **Data Retention:** Personal data shall not be retained longer than necessary for the purposes for which it was collected or as required by law.
* **Secure Disposal:** Personal data shall be securely disposed of when no longer needed, in accordance with the organisation's data destruction policies.

## Purpose Limitation

* **Specific Purposes:** Personal data shall be collected and processed only for specified, explicit, and legitimate purposes related to the AI application and not further processed in a manner that is incompatible with those purposes.
* **Secondary Use:** Any secondary use of personal data for purposes other than those originally specified shall require a new legal basis and, where necessary, additional consent from the data subjects.

## Data Subject Rights

* **Access and Rectification:** Individuals shall have the right to access their personal data and request corrections or updates if the data is inaccurate or incomplete.
* **Erasure:** Individuals shall have the right to request the erasure of their personal data under certain circumstances, such as when the data is no longer necessary for the purposes for which it was collected or when consent is withdrawn.
* **Objection:** Individuals shall have the right to object to the processing of their personal data for certain purposes, such as direct marketing or profiling.

## Security of AI Data

* **Appropriate Security Measures:** Appropriate technical and organisational measures shall be implemented to protect personal data against unauthorised access, loss, alteration, or destruction. This includes:
  + Access controls and authentication mechanisms
  + Encryption of data at rest and in transit
  + Regular security assessments and vulnerability management
* **Data Breach Notification:** In the event of a personal data breach, the relevant supervisory authority and affected individuals shall be notified within the timeframes stipulated by applicable regulations.

# Responsibilities

* **Data Protection Officer (DPO):** Responsible for overseeing the organisation's compliance with data privacy regulations and this policy.
* **IT Department:** Responsible for implementing technical measures to protect personal data and ensure privacy compliance.
* **AI Development Teams:** Responsible for designing and developing AI applications in a privacy-preserving manner, incorporating data minimisation and anonymisation techniques where possible.
* **Legal Department:** Responsible for providing legal advice and guidance on privacy matters.
* **Employees:** Responsible for handling personal data in accordance with this policy and reporting any privacy concerns or breaches.

# 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