Internet of Things (IoT) Security Framework for Industry 4.0

"Data Minimisation - Principles for limiting data collection"

|  |  |
| --- | --- |
| 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](#_Toc190895746)

[2. Purpose 4](#_Toc190895747)

[3. Scope 4](#_Toc190895748)

[4. Policy Statement 4](#_Toc190895749)

[4.1. Data Collection Limitation 4](#_Toc190895750)

[4.2. Data Retention 4](#_Toc190895751)

[4.3. Data Anonymisation and Pseudonymisation 4](#_Toc190895752)

[5. Responsibilities 5](#_Toc190895753)

[6. Breaches of Policy 5](#_Toc190895754)

[7. Document Management 5](#_Toc190895755)

# Introduction

The Internet of Things (IoT) ecosystem is characterised by the pervasive collection and processing of data. While this data can provide valuable insights and enable innovative services, it is crucial to ensure that data collection is conducted in a responsible and privacy-conscious manner. The principle of data minimisation emphasises the collection of only the data that is necessary and relevant for the specified purposes, thereby reducing the risk of unauthorised access, data breaches, and privacy violations.

# Purpose

The purpose of this policy is to establish clear guidelines and requirements for implementing data minimisation principles in the context of IoT devices and systems within the organisation. This policy aims to:

* Limit the collection of personal and sensitive data to only what is strictly necessary for the intended purposes.
* Reduce the risk of data breaches and privacy violations by minimising the amount of data stored and processed.
* Promote transparency and accountability in data collection practices.
* Ensure compliance with relevant privacy regulations and data protection laws.

# Scope

This policy applies to all IoT devices and systems within the organisation that collect, process, or transmit data, regardless of their location or function. This includes, but is not limited to:

* Sensors and actuators
* Wearable devices
* Smart home devices
* Industrial control systems

# Policy Statement

## Data Collection Limitation

* **Necessity and Relevance:** Data collected by IoT devices shall be limited to only what is strictly necessary and relevant for the specified purposes.
* **Purpose Specification:** The purposes for which data is collected shall be clearly defined and documented prior to collection.
* **Data Collection Review:** Data collection practices shall be periodically reviewed to ensure that they remain aligned with the stated purposes and comply with data minimisation principles.

## Data Retention

* **Retention Periods:** Personal and sensitive data shall not be retained longer than necessary for the purposes for which it was collected, unless required by law or other legitimate reasons.
* **Data Retention Schedule:** A data retention schedule shall be established and maintained, specifying the retention periods for different types of data.
* **Secure Disposal:** Data shall be securely disposed of when no longer needed, in accordance with the organisation's data destruction policies.

## Data Anonymisation and Pseudonymisation

* **Privacy Enhancement:** Where possible, data anonymisation or pseudonymisation techniques shall be employed to reduce the risk of identifying individuals from collected data.
* **Anonymisation:** Anonymisation involves removing or modifying personally identifiable information (PII) in a way that makes it impossible to re-identify individuals.
* **Pseudonymisation:** Pseudonymisation involves replacing PII with artificial identifiers or pseudonyms, allowing for data analysis while protecting individual privacy.

# Responsibilities

* **Data Protection Officer (DPO):** Responsible for overseeing the organisation's compliance with data minimisation principles and this policy.
* **IT Department:** Responsible for implementing technical measures to support data minimisation, such as data anonymisation and pseudonymisation tools.
* **System Owners:** Responsible for defining and documenting the purposes of data collection for their respective systems and ensuring compliance with this policy.
* **Data Processors:** Responsible for handling data in accordance with this policy and minimising the collection and retention of unnecessary data.

# 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