Internet of Things (IoT) Security Framework for Industry 4.0

" Asset Management Policy"

|  |  |
| --- | --- |
| 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 3](#_Toc177470192)

[2. Policy 3](#_Toc177470193)

[3. Responsibilities 3](#_Toc177470194)

[4. Breaches of Policy 3](#_Toc177470195)

[5. Document Management 3](#_Toc177470196)

# Introduction

The organisation is committed to maximising the value and security of its IoT assets while ensuring compliance with all relevant legislative and regulatory requirements. This policy outlines the principles and guidelines for effective asset management within the context of the IoT ecosystem.

# Policy

To achieve the above commitment, the organisation will:

* **Asset Identification and Inventory:** Maintain a comprehensive and up-to-date inventory of all IoT assets, including hardware, software, and data.
* **Asset Classification:** Classify IoT assets based on their criticality, sensitivity, and business value.
* **Risk Management:** Conduct regular risk assessments to identify and mitigate risks associated with IoT assets throughout their lifecycle.
* **Security Controls:** Implement appropriate security controls to protect the confidentiality, integrity, and availability of IoT assets.
* **Lifecycle Management:** Manage the entire lifecycle of IoT assets, from procurement and deployment to maintenance, upgrades, and secure disposal.
* **Performance Monitoring:** Monitor the performance and utilisation of IoT assets to optimise their value and identify potential issues.
* **Cost Optimisation:** Implement strategies to minimise the total cost of ownership of IoT assets.
* **Compliance:** Ensure compliance with all relevant laws, regulations, and industry standards related to IoT asset management.
* **Continuous Improvement:** Regularly review and improve asset management processes to enhance efficiency and effectiveness.

# Responsibilities

* **Information Security Officer:** Responsible for overseeing the certification process and ensuring compliance with this policy.
* **IT Department:** Responsible for conducting technical evaluations and security testing.
* **Data Protection Officer (if applicable):** Responsible for conducting privacy impact assessments.
* **Department Heads:** Responsible for submitting certification requests and ensuring that their departments adhere to the requirements of this policy.

# Breaches of Policy

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

# 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