Internet of Things (IoT) Security Framework for Industry 4.0

"Criteria: Device and system certification standards"

|  |  |
| --- | --- |
| 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](#_Toc176333768)

[2. Purpose 4](#_Toc176333769)

[3. Scope 4](#_Toc176333770)

[4. Policy Statement 4](#_Toc176333771)

[4.1. Certification Requirements 4](#_Toc176333772)

[4.2. Evaluation Criteria 4](#_Toc176333773)

[4.3. Certification Process 5](#_Toc176333774)

[4.4. Ongoing Compliance 5](#_Toc176333775)

[5. Responsibilities 5](#_Toc176333776)

[6. Breaches of Policy 5](#_Toc176333777)

[7. Document Management 5](#_Toc176333778)

# Introduction

The rapid evolution of the Internet of Things (IoT) introduces new technologies and devices at an unprecedented pace. While these innovations offer significant benefits, they also bring potential security and privacy risks. This policy establishes a framework for evaluating and certifying IoT devices and systems before their adoption or deployment within the organization.

# Purpose

The purpose of this policy is to ensure that all IoT devices and systems meet stringent security and privacy standards before being integrated into the organization's environment. This policy aims to:

* Minimise the risk of introducing vulnerabilities or disruptions through the adoption of new IoT technologies.
* Ensure that new devices and systems align with the organization's security and privacy standards.
* Establish a process for ongoing monitoring and evaluation of certified technologies.

# Scope

This policy applies to all IoT devices and systems considered for adoption or deployment within the organization, including but not limited to:

* Sensors, actuators, and controllers
* Gateways and edge devices
* Industrial control systems (ICS)
* Wearable and embedded devices
* Any other device with network connectivity capabilities

# Policy Statement

## Certification Requirements

* **Mandatory Certification:** All IoT devices and systems shall undergo a formal certification process before being adopted or deployed within the organization.
* **Risk Assessment:** A comprehensive risk assessment shall be conducted to evaluate the potential security, privacy, and compliance risks associated with each device or system.
* **Security and Privacy Standards:** Devices and systems must meet or exceed the organization's security and privacy standards, including data protection, access control, and encryption requirements.
* **Compatibility and Interoperability:** The technology must be compatible with the organization's existing infrastructure and demonstrate interoperability with other IoT components.

## Evaluation Criteria

* **Security Testing:** Devices and systems shall undergo rigorous security testing, including vulnerability scanning and penetration testing, to identify and address potential weaknesses.
* **Privacy Impact Assessment:** If the device or system involves the processing of personal data, a privacy impact assessment (PIA) shall be conducted to evaluate its compliance with data protection regulations.
* **Performance and Scalability:** The technology shall be evaluated for its performance, scalability, and ability to handle the expected data volumes and traffic patterns.
* **Vendor Due Diligence:** The security posture and track record of vendors providing the technology shall be assessed.

## Certification Process

* **Formal Request:** A formal request for certification shall be submitted, including detailed information about the device or system, its intended use, and the results of the risk assessment.
* **Evaluation and Testing:** The IT department, in conjunction with relevant stakeholders, shall conduct a thorough evaluation of the device or system, including security testing and privacy impact assessments where necessary.
* **Approval or Denial:** A decision shall be made to approve or deny the certification based on the evaluation results and risk assessment.
* **Documentation:** The certification process and decision shall be documented, including any conditions or limitations imposed on the use of the device or system.

## Ongoing Compliance

* **Monitoring and Review:** Certified devices and systems shall be subject to ongoing monitoring and periodic reviews to ensure their continued compliance with security and privacy standards.
* **Revocation:** Certification may be revoked if the device or system is found to be non-compliant or poses an unacceptable risk to the organization.

# 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