Internet of Things (IoT) Security Framework for Industry 4.0

"Certification for new technologies and practices"

|  |  |
| --- | --- |
| 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](#_Toc176333741)

[2. Purpose 4](#_Toc176333742)

[3. Scope 4](#_Toc176333743)

[4. Policy Statement 4](#_Toc176333744)

[4.1. Certification Requirements 4](#_Toc176333745)

[4.2. Evaluation Criteria 4](#_Toc176333746)

[4.3. Certification Process 5](#_Toc176333747)

[4.4. Ongoing Compliance 5](#_Toc176333748)

[5. Responsibilities 5](#_Toc176333749)

[6. Breaches of Policy 5](#_Toc176333750)

[7. Document Management 5](#_Toc176333751)

# Introduction

The rapid evolution of the Internet of Things (IoT) landscape introduces new technologies and practices 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 new IoT technologies and practices before their adoption or deployment within the organisation.

# Purpose

The purpose of this policy is to ensure that new IoT technologies and practices are thoroughly assessed for security, privacy, and compliance risks before being integrated into the organisation's environment. This policy aims to:

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

# Scope

This policy applies to all new IoT technologies and practices considered for adoption or deployment within the organisation, including but not limited to:

* New IoT devices and sensors
* Communication protocols and platforms
* Data storage and processing solutions
* Cloud services and applications
* Operational procedures and workflows

# Policy Statement

## Certification Requirements

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

## Evaluation Criteria

* **Security Testing:** The technology or practice shall undergo rigorous security testing, including vulnerability scanning, penetration testing, and code review, to identify and address potential weaknesses.
* **Privacy Impact Assessment:** A privacy impact assessment (PIA) shall be conducted to evaluate the potential impact on the privacy of individuals and ensure compliance with relevant regulations.
* **Performance and Scalability:** The technology or practice 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 or promoting the practice shall be assessed.

## Certification Process

* **Formal Request:** A formal request for certification shall be submitted, including detailed information about the technology or practice, its intended use, and the results of the risk assessment and evaluation.
* **Review and Approval:** The request shall be reviewed by a designated committee or team, comprising representatives from IT, security, legal, and relevant business units.
* **Certification Decision:** A decision shall be made to approve or deny the certification based on the evaluation criteria and risk assessment.
* **Documentation:** The certification process and decision shall be documented, including any conditions or limitations imposed on the use of the technology or practice.

## Ongoing Compliance

* **Monitoring and Review:** Certified technologies and practices 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 technology or practice is found to be non-compliant or poses an unacceptable risk to the organisation.

# 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 (DPO):** 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