TrustIoT Framework for Industry 4.0

" Supplier Security Policy"

|  |  |
| --- | --- |
| Document Classification: | Internal |
| Document Ref. | *TrustIoT 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](#_Toc190890432)

[2. Policy Statement 4](#_Toc190890433)

[2.1. Information Security 4](#_Toc190890434)

[2.2. Objectives 4](#_Toc190890435)

[2.3. Information Risk Assessment and Management 4](#_Toc190890436)

[2.4. Legislative, Regulatory, and Contractual Requirements 4](#_Toc190890437)

[2.5. Access to Information, Assets, and Systems 4](#_Toc190890438)

[2.6. Information Security Management System (ISMS) Controls 5](#_Toc190890439)

[3. Supplier Responsibilities 5](#_Toc190890440)

[4. Contractual Obligations 5](#_Toc190890441)

[5. Responsibilities 5](#_Toc190890442)

[6. Breaches of Policy 5](#_Toc190890443)

[7. Conclusion 5](#_Toc190890444)

[8. Document Management 6](#_Toc190890445)

# Introduction

This document outlines the security requirements that suppliers and vendors must adhere to when interacting with the organisation's IoT ecosystem. It aims to ensure the confidentiality, integrity, and availability of information and assets associated with IoT devices, systems, and data.

# Policy Statement

## Information Security

Information security encompasses the preservation of confidentiality, integrity, and availability of all information related to the organisation's IoT ecosystem. This includes data generated, collected, processed, stored, and transmitted by IoT devices, as well as any associated metadata or supporting information.

## Objectives

* Ensure that suppliers maintain the security of the organisation's IoT-related information to support business needs and meet legal, regulatory, and contractual obligations.
* Establish a framework for assessing and managing information security risks associated with supplier relationships.
* Define the security controls and requirements that suppliers must implement to protect the organisation's IoT ecosystem.

## Information Risk Assessment and Management

* The organisation employs a risk-based approach to assess and manage information security risks associated with suppliers.
* Suppliers are expected to cooperate in risk assessments and implement appropriate risk mitigation measures.
* Residual risks will be evaluated and accepted only up to a defined tolerance level.

## Legislative, Regulatory, and Contractual Requirements

* Suppliers must comply with all applicable laws, regulations, and contractual obligations related to data protection, privacy, and information security.
* Any processing of personal data must adhere to relevant data protection regulations and obtain necessary consents.
* Suppliers handling sensitive or confidential information may be subject to additional security requirements.

## Access to Information, Assets, and Systems

* Supplier access to the organisation's IoT information, assets, and systems will be granted on a need-to-know basis and subject to appropriate authorisation and authentication.
* Suppliers must implement access controls to restrict access to authorised personnel only.
* Upon termination of the contract, suppliers must return all organisation-owned equipment and cease access to information and systems.
* The organisation reserves the right to monitor supplier activities within its IoT ecosystem for security and compliance purposes.

## Information Security Management System (ISMS) Controls

* Suppliers handling sensitive IoT data or providing critical services must have an ISMS in place that aligns with recognised security standards (e.g., ISO/IEC 27001).
* Suppliers must agree to periodic audits of their ISMS by the organisation or its authorised representatives.
* Communication between the organisation and suppliers must be secured using appropriate encryption and security protocols.
* Live or production data must not be used for testing or development purposes. Suppliers must use sanitised or anonymised data for such activities.

# Supplier Responsibilities

* Implement and maintain appropriate security controls to protect the confidentiality, integrity, and availability of the organisation's IoT-related information.
* Promptly report any security incidents or breaches involving the organisation's data or systems.
* Cooperate with the organisation in conducting risk assessments and implementing necessary security measures.
* Ensure that their personnel handling the organisation's IoT data receive adequate security awareness training.
* Maintain appropriate insurance coverage to address potential liabilities arising from security incidents.

# Contractual Obligations

* Security requirements and obligations will be incorporated into supplier contracts and agreements.
* The organisation reserves the right to terminate contracts with suppliers who fail to comply with the security policy or demonstrate inadequate security practices.

# 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.

# Conclusion

This Supplier Security Policy establishes a framework for ensuring that suppliers and vendors maintain the security and integrity of the organisation's IoT ecosystem. By adhering to these requirements, suppliers contribute to the overall protection of sensitive data and critical infrastructure.

**Note:** This policy is subject to periodic review and updates to reflect changes in the threat landscape, technology advancements, and regulatory requirements.

# 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