TrustIoT Framework for Industry 4.0

" Third Party Connection 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](#_Toc190890559)

[2. Purpose 4](#_Toc190890560)

[3. Scope 4](#_Toc190890561)

[4. Policy Statement 4](#_Toc190890562)

[5. Procedures 4](#_Toc190890563)

[5.1. Connection Request 4](#_Toc190890564)

[5.2. Risk Assessment 5](#_Toc190890565)

[5.3. Connection Approval 5](#_Toc190890566)

[5.4. Contractual Agreement 5](#_Toc190890567)

[5.5. Implementation and Monitoring 5](#_Toc190890568)

[5.6. Termination 5](#_Toc190890569)

[6. Incident Management 5](#_Toc190890570)

[7. Review and Updates 5](#_Toc190890571)

[8. Responsibilities 5](#_Toc190890572)

[9. Breaches of Policy 6](#_Toc190890573)

[10. Summary 6](#_Toc190890574)

[11. Document Management 6](#_Toc190890575)

# Introduction

This policy outlines the requirements and procedures for establishing and managing connections between the organisation's IoT ecosystem and external third-party organisations or service providers. It aims to ensure the confidentiality, integrity, and availability of information and assets while promoting secure and controlled collaboration.

# Purpose

The purpose of this policy is to:

* Define the process for initiating, evaluating, and approving third-party connections to the IoT ecosystem.
* Establish security controls and requirements for third-party connections to protect sensitive data and critical infrastructure.
* Ensure compliance with relevant legal, regulatory, and contractual obligations.
* Mitigate risks associated with third-party access to the organisation's IoT environment.

# Scope

This policy applies to all connections between the organisation's IoT ecosystem and external third parties, including but not limited to:

* Cloud service providers
* Data analytics platforms
* Device manufacturers
* Software vendors
* System integrators
* Consultants and contractors

# Policy Statement

* All third-party connections must be initiated through a formal request process and undergo a thorough risk assessment.
* Connections will only be approved if they serve a legitimate business purpose and the associated risks are deemed acceptable.
* Third parties must demonstrate compliance with the organisation's security policies and standards.
* Access to the organisation's IoT ecosystem will be granted on a need-to-know basis and subject to appropriate authorisation and authentication.
* The organisation reserves the right to monitor and audit third-party activities within its IoT environment.

# Procedures

## Connection Request

* Business units submit a formal request for a third-party connection, outlining the purpose, scope, and data involved.
* The request is reviewed by the Information Security Officer and relevant data owners.
* A risk assessment is conducted to evaluate the potential security risks associated with the connection.

## Risk Assessment

* The risk assessment considers factors such as:
  + Sensitivity of data to be accessed or shared
  + Third-party's security posture and track record
  + Technical controls and safeguards in place
  + Potential impact of a security breach
* The risk assessment results are documented and reviewed by the Information Security Officer.

## Connection Approval

* The Information Security Officer makes a recommendation on whether to approve or deny the connection request based on the risk assessment.
* Final approval is granted by senior management.

## Contractual Agreement

* A formal contract or agreement is established with the third party, outlining security requirements, data protection obligations, and incident response procedures.
* The contract is reviewed and approved by the Legal Department.

## Implementation and Monitoring

* The IT Department implements the necessary technical controls to establish the connection securely.
* Ongoing monitoring and auditing are conducted to ensure compliance with security policies and contractual obligations.

## Termination

* Upon termination of the contract or relationship, access to the organisation's IoT ecosystem is revoked.
* The third party is required to return or destroy any sensitive data in their possession.

# Incident Management

* Any security incidents or breaches involving third-party connections must be reported immediately to the Information Security Officer.
* The organisation's incident response procedures will be followed to contain and mitigate the impact of any incidents.

# Review and Updates

* This policy will be reviewed periodically and updated as needed to reflect changes in the threat landscape, technology, and regulatory requirements.

# Responsibilities

* **Information Security Officer:** Oversees the third-party connection process and ensures compliance with security policies.
* **Data Owners:** Responsible for classifying data and systems and determining appropriate access levels for third parties.
* **IT Department:** Implements and manages technical controls for third-party connections.
* **Legal Department:** Reviews and approves contractual agreements with third parties.
* **Business Units:** Initiate requests for third-party connections and provide justification for their business need.

# Breaches of Policy

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

# Summary

This Third-Party Connection Policy establishes a framework for secure and controlled collaboration with external organisations within the IoT ecosystem. By adhering to these guidelines, the organisation can leverage the benefits of third-party partnerships while minimising the associated security risks.

# 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