TrustIoT Framework for Industry 4.0

"Device Onboarding and Provisioning"

|  |  |
| --- | --- |
| 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](#_Toc190904418)

[2. Purpose 4](#_Toc190904419)

[3. Scope 4](#_Toc190904420)

[4. Policy Statement 4](#_Toc190904421)

[4.1. Device Identification and Registration 4](#_Toc190904422)

[4.2. Secure Provisioning 4](#_Toc190904423)

[4.3. Authentication and Authorisation 4](#_Toc190904424)

[4.4. Configuration Management 5](#_Toc190904425)

[4.5. Decommissioning and Removal 5](#_Toc190904426)

[5. Responsibilities 5](#_Toc190904427)

[6. Breaches of Policy 5](#_Toc190904428)

[7. Document Management 5](#_Toc190904429)

# Introduction

The proliferation of Internet of Things (IoT) devices necessitates a structured and secure approach to onboarding and provisioning these devices onto the network. Improper onboarding can lead to unauthorised access, misconfigurations, and potential security breaches. This policy outlines the procedures and controls to ensure the secure and controlled introduction of IoT devices into the organisation's environment.

# Purpose

The purpose of this policy is to establish a framework for the secure onboarding and provisioning of IoT devices within the organisation's network. This policy aims to:

* Establish a standardised process for introducing new IoT devices into the network.
* Ensure that IoT devices are properly configured and secured before being granted access.
* Manage device identities and credentials throughout their lifecycle.
* Prevent unauthorised devices from connecting to the network.

# Scope

This policy applies to all IoT devices that are connected or intended to be connected to the organisation's network, regardless of their function or manufacturer.

# Policy Statement

## Device Identification and Registration

* **Unique Identifiers:** Each IoT device shall be assigned a unique and tamper-proof identifier, such as a hardware-based identifier or a digitally signed certificate.
* **Centralised Inventory:** A centralised inventory of all IoT devices shall be maintained, including details such as device type, manufacturer, model, serial number, location, and assigned owner.
* **Registration Process:** A formal registration process shall be followed for all new IoT devices, requiring approval from authorised personnel and capturing relevant device information in the inventory.

## Secure Provisioning

* **Secure Configuration:** IoT devices shall be provisioned with secure configurations, including strong passwords, disabled default accounts, and appropriate network settings.
* **Firmware Updates:** Devices shall be updated to the latest available firmware version before deployment to ensure they are protected against known vulnerabilities.
* **Secure Boot:** Where supported, secure boot mechanisms shall be enabled to prevent the execution of unauthorised or modified firmware.

## Authentication and Authorisation

* **Strong Authentication:** IoT devices shall be authenticated using strong authentication mechanisms, such as digital certificates or pre-shared keys.
* **Network Access Control (NAC):** NAC solutions may be employed to enforce authentication and authorisation policies before granting network access to IoT devices.
* **Least Privilege:** IoT devices shall be granted only the minimum necessary network access and permissions required for their intended functions.

## Configuration Management

* **Configuration Baselines:** Secure configuration baselines shall be established for different types of IoT devices, and deviations from these baselines shall be monitored and addressed.
* **Change Management:** Changes to device configurations shall be subject to a formal change management process to ensure proper authorisation, testing, and documentation.

## Decommissioning and Removal

* **Secure Decommissioning:** When an IoT device is decommissioned or removed from the network, its access credentials and any sensitive data stored on the device shall be securely erased or destroyed.
* **Inventory Update:** The centralised inventory shall be updated to reflect the decommissioning or removal of the device.

# Responsibilities

* **Information Security Officer:** Responsible for overseeing the implementation and enforcement of this policy.
* **IT Department:** Responsible for managing the device onboarding and provisioning process, maintaining the device inventory, and enforcing security configurations.
* **Device Owners:** Responsible for initiating the onboarding process for new devices and ensuring compliance with 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