Internet of Things (IoT) Security Framework for Industry 4.0

"Automated provisioning and configuration management systems"

|  |  |
| --- | --- |
| 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](#_Toc176333489)

[2. Purpose 4](#_Toc176333490)

[3. Scope 4](#_Toc176333491)

[4. Policy Statement 4](#_Toc176333492)

[4.1. Automated Provisioning 4](#_Toc176333493)

[4.2. Configuration Management 4](#_Toc176333494)

[4.3. Security and Access Control 5](#_Toc176333495)

[4.4. Monitoring and Logging 5](#_Toc176333496)

[5. Responsibilities 5](#_Toc176333497)

[6. Breaches of Policy 5](#_Toc176333498)

[7. Document Management 5](#_Toc176333499)

# Introduction

The rapid proliferation of Internet of Things (IoT) devices in modern enterprises necessitates efficient and secure mechanisms for provisioning and managing their configurations. Manual configuration processes are prone to errors, inconsistencies, and security vulnerabilities. Automated provisioning and configuration management systems address these challenges by streamlining the deployment and configuration of IoT devices, ensuring consistency, security, and scalability.

# Purpose

The purpose of this policy is to establish guidelines and requirements for the implementation and use of automated provisioning and configuration management systems for IoT devices within the organization. This policy aims to:

* Streamline the deployment and configuration of IoT devices, reducing manual effort and errors.
* Ensure consistent and secure configurations across all IoT devices.
* Enable efficient management and control of device configurations throughout their lifecycle.
* Facilitate scalability and adaptability to accommodate the growing number and diversity of IoT devices.

# Scope

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

# Policy Statement

## Automated Provisioning

* **Centralised Provisioning:** A centralised system or platform shall be utilised for the automated provisioning of IoT devices, including:
  + Initial configuration and setup
  + Assignment of unique identifiers and credentials
  + Deployment of firmware and software updates
  + Network configuration and security settings
* **Secure Communication:** Communication between the provisioning system and IoT devices shall be secured using appropriate encryption and authentication mechanisms.
* **Zero-Touch Provisioning:** Where feasible, zero-touch provisioning mechanisms shall be employed to minimise manual intervention and reduce the risk of misconfigurations.

## Configuration Management

* **Configuration Baselines:** Secure configuration baselines shall be established for different types of IoT devices, defining the required settings and parameters.
* **Configuration Enforcement:** Automated configuration management tools shall be used to enforce compliance with defined baselines and detect any deviations.
* **Change Management:** Changes to device configurations shall be subject to a formal change management process to ensure proper authorization, testing, and documentation.

## Security and Access Control

* **Secure Access:** Access to the provisioning and configuration management systems shall be restricted to authorised personnel only, utilising strong authentication and authorization mechanisms.
* **Credential Management:** Credentials used for device provisioning and configuration shall be securely managed and protected against unauthorised access.
* **Least Privilege:** The principle of least privilege shall be applied, granting users and systems only the minimum necessary access required to perform their functions.

## Monitoring and Logging

* **Comprehensive Logging:** All provisioning and configuration activities, including successful and failed attempts, shall be logged in a centralised and secure manner.
* **Real-time Monitoring:** Automated tools shall be used to monitor device configurations and detect any unauthorised changes or deviations from baselines.
* **Alerting:** Automated alerts shall be generated for configuration changes or security events, triggering timely investigation and response.

# Responsibilities

* **Information Security Officer:** Responsible for overseeing the implementation and enforcement of this policy.
* **IT Department:** Responsible for selecting, deploying, and managing automated provisioning and configuration management systems.
* **Device Owners:** Responsible for ensuring that their IoT devices are provisioned and configured in compliance with this policy.
* **Security Operations Centre (SOC):** Responsible for monitoring security events and responding to incidents related to device provisioning and configuration.

# 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