TrustIoT Framework for Industry 4.0

"Vulnerability Management"

|  |  |
| --- | --- |
| 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](#_Toc176333280)

[2. Purpose 4](#_Toc176333281)

[3. Scope 4](#_Toc176333282)

[4. Policy Statement 4](#_Toc176333283)

[4.1. Secure OTA Update Process 4](#_Toc176333284)

[4.2. Firmware/Software Verification and Validation 4](#_Toc176333285)

[4.3. Rollback Capabilities 4](#_Toc176333286)

[4.4. Update Scheduling and Notification 5](#_Toc176333287)

[5. Responsibilities 5](#_Toc176333288)

[6. Breaches of Policy 5](#_Toc176333289)

[7. Document Management 5](#_Toc176333290)

# Introduction

The dynamic nature of the Internet of Things (IoT) landscape necessitates frequent updates to firmware and software components to address security vulnerabilities, enhance functionality, and improve performance. Over-the-Air (OTA) updates provide a convenient and efficient mechanism for delivering these updates to deployed IoT devices. However, OTA updates also introduce potential risks, such as the installation of malicious or faulty code. This document outlines the policies and procedures for implementing secure OTA updates with rollback capabilities to ensure the integrity and reliability of IoT devices.

# Purpose

The purpose of this policy is to establish a framework for secure and controlled OTA updates for IoT devices within the organisation. This policy aims to:

* Enable efficient and timely updates to IoT devices without requiring physical access.
* Ensure the authenticity and integrity of firmware and software updates.
* Provide a mechanism to revert to a previous stable state in case of failed or problematic updates.
* Minimise downtime and disruption to operations during the update process.

# Scope

This policy applies to all IoT devices within the organisation that are capable of receiving OTA updates, including but not limited to:

* Sensors, actuators, and controllers
* Gateways and edge devices
* Industrial control systems (ICS)
* Wearable and embedded devices

# Policy Statement

## Secure OTA Update Process

* **Secure Communication Channels:** OTA updates shall be delivered over secure communication channels, utilising encryption and authentication mechanisms to protect against unauthorised interception or modification.
* **Firmware/Software Verification:** Prior to installation, updates shall be cryptographically verified using digital signatures or similar mechanisms to ensure their authenticity and integrity.
* **Access Control:** Access to the OTA update process shall be restricted to authorised personnel and systems.
* **Logging and Auditing:** All OTA update activities, including successful and failed attempts, shall be logged and audited for traceability and accountability.

## Firmware/Software Verification and Validation

* **Testing and Validation:** Firmware and software updates shall undergo rigorous testing and validation in a controlled environment before deployment to production devices.
* **Staging Environments:** Staged rollouts shall be conducted to gradually deploy updates to a subset of devices, allowing for monitoring and validation before wider deployment.

## Rollback Capabilities

* **Rollback Mechanism:** IoT devices shall have the capability to revert to a previous known-good firmware or software version in case of failed or problematic updates.
* **Rollback Triggers:** Rollback procedures shall be initiated automatically or manually based on predefined criteria, such as device instability, communication failures, or security breaches.

## Update Scheduling and Notification

* **Scheduled Updates:** OTA updates shall be scheduled during non-critical periods to minimise disruption to operations.
* **User Notification:** Users shall be notified in advance of upcoming updates, providing information about the changes and potential impact.

# Responsibilities

* **Information Security Officer:** Responsible for overseeing the implementation and enforcement of this policy.
* **IT Department:** Responsible for managing the OTA update infrastructure, including secure communication channels, firmware/software repositories, and rollback mechanisms.
* **Device Owners:** Responsible for ensuring that their IoT devices are configured to receive OTA updates and that updates are applied in a timely manner.
* **Software Developers/Vendors:** Responsible for developing and delivering secure and reliable firmware and software updates.

# 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