TrustIoT Framework for Industry 4.0

"Firmware and Software Integrity"

|  |  |
| --- | --- |
| 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](#_Toc176332182)

[2. Purpose 4](#_Toc176332183)

[3. Scope 4](#_Toc176332184)

[4. Policy Statement 4](#_Toc176332185)

[4.1. Secure Boot 4](#_Toc176332186)

[4.2. Secure Firmware and Software Updates 4](#_Toc176332187)

[4.3. Code Signing and Verification 4](#_Toc176332188)

[4.4. Vulnerability Management 5](#_Toc176332189)

[5. Responsibilities 5](#_Toc176332190)

[6. Breaches of Policy 5](#_Toc176332191)

[7. Document Management 5](#_Toc176332192)

# Introduction

The firmware and software running on IoT devices are critical components that govern their functionality, security, and overall performance. Maintaining the integrity of this firmware and software is essential to protect against unauthorised modifications, malware infections, and other cyber threats that can compromise the confidentiality, integrity, and availability of IoT systems and data. This document outlines the policies and procedures for ensuring the integrity of firmware and software throughout the lifecycle of IoT devices.

# Purpose

The purpose of this policy is to establish a framework for protecting the firmware and software integrity of IoT devices within the organisation. This policy aims to:

* Prevent unauthorised modifications or tampering with firmware and software.
* Ensure that only authorised and verified code is executed on IoT devices.
* Mitigate the risk of malware infections and other software-based attacks.
* Maintain the reliability and trustworthiness of IoT devices and systems.

# Scope

This policy applies to all firmware and software components of IoT devices connected to the organisation's network, including but not limited to:

* Bootloaders and operating systems
* Device drivers and firmware
* Application software and middleware
* Configuration files and scripts

# Policy Statement

## Secure Boot

* **Secure Boot Mechanisms:** IoT devices shall implement secure boot mechanisms to ensure that only authorised and verified firmware is loaded during startup.
* **Trusted Execution Environment:** Where feasible, a Trusted Execution Environment (TEE) shall be utilised to protect the integrity of the boot process and critical system components.

## Secure Firmware and Software Updates

* **Authenticated Updates:** Firmware and software updates shall be delivered through secure channels and authenticated using digital signatures or other cryptographic mechanisms.
* **Code Verification:** Prior to installation, updates shall be verified for integrity and authenticity to prevent the execution of unauthorised or malicious code.
* **Rollback Mechanisms:** Rollback mechanisms shall be implemented to revert to a previous known-good state in case of failed or compromised updates.

## Code Signing and Verification

* **Code Signing:** All firmware and software components shall be digitally signed by authorised developers or vendors.
* **Signature Verification:** IoT devices shall verify the digital signatures of firmware and software before execution or installation.
* **Key Management:** Robust key management practices shall be implemented to protect the private keys used for code signing.

## Vulnerability Management

* **Regular Scanning:** IoT devices shall be regularly scanned for known vulnerabilities using automated tools and manual assessments.
* **Prompt Patching:** Identified vulnerabilities shall be addressed promptly by applying patches or updates from trusted sources.
* **Zero-Day Vulnerabilities:** Procedures shall be in place to respond to and mitigate the risks associated with zero-day vulnerabilities.

# Responsibilities

* **Information Security Officer:** Responsible for overseeing the implementation and enforcement of this policy.
* **IT Department:** Responsible for managing the technical infrastructure and processes related to firmware and software updates, code signing, and vulnerability management.
* **Device Owners:** Responsible for ensuring that their IoT devices comply with this policy and receive timely updates.
* **Software Developers/Vendors:** Responsible for following secure coding practices and providing signed and verified 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