TrustIoT Framework for Industry 4.0

"Patch Management: Procedures for timely patch application"

|  |  |
| --- | --- |
| 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](#_Toc176333308)

[2. Purpose 4](#_Toc176333309)

[3. Scope 4](#_Toc176333310)

[4. Policy Statement 4](#_Toc176333311)

[4.1. Patch Identification and Assessment 4](#_Toc176333312)

[4.2. Patch Testing and Validation 4](#_Toc176333313)

[4.3. Patch Deployment and Installation 4](#_Toc176333314)

[4.4. Rollback and Contingency Plans 5](#_Toc176333315)

[5. Responsibilities 5](#_Toc176333316)

[6. Breaches of Policy 5](#_Toc176333317)

[7. Document Management 5](#_Toc176333318)

# Introduction

The Internet of Things (IoT) ecosystem comprises a vast array of interconnected devices, each running firmware and software that may contain vulnerabilities. These vulnerabilities, if left unaddressed, can be exploited by malicious actors to gain unauthorised access, disrupt operations, or steal sensitive data. Patch management, the process of identifying, evaluating, and applying software updates or patches, is crucial to mitigate these risks and ensure the continued security and integrity of IoT devices and systems.

# Purpose

The purpose of this policy is to establish a framework for the timely and effective application of patches to IoT devices within the organisation. This policy aims to:

* Minimise the risk of exploitation of vulnerabilities in IoT devices.
* Ensure that IoT devices are maintained in a secure and hardened state.
* Establish a process for continuous monitoring and improvement of the IoT security posture.

# Scope

This policy applies to all IoT devices and systems connected to the organisation's network, regardless of their function or manufacturer. This includes, but is not limited to:

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

# Policy Statement

## Patch Identification and Assessment

* **Vulnerability Monitoring:** IoT devices and systems shall be continuously monitored for known vulnerabilities using automated tools, vendor notifications, and security advisories.
* **Patch Availability:** The availability of patches or updates from trusted sources shall be promptly identified and assessed for applicability and potential impact.
* **Risk Assessment:** A risk-based approach shall be adopted to prioritise the deployment of patches based on the severity of the vulnerability, potential impact, and exploitability.

## Patch Testing and Validation

* **Testing Environment:** Patches shall be thoroughly tested in a controlled environment before deployment to production devices to ensure compatibility and identify any potential issues.
* **Regression Testing:** Regression testing shall be performed to verify that existing functionalities are not adversely affected by the patch.
* **Performance Testing:** Performance testing may be conducted to assess the impact of the patch on device performance and resource utilisation.

## Patch Deployment and Installation

* **Change Management:** Patch deployment and installation shall be subject to a formal change management process to ensure proper authorisation, testing, and documentation.
* **Secure Delivery:** Patches shall be delivered through secure channels, utilising encryption and authentication mechanisms to protect against tampering or unauthorised modification.
* **Installation Verification:** The successful installation of patches shall be verified through appropriate mechanisms, such as version checks or checksum validation.

## Rollback and Contingency Plans

* **Rollback Capability:** Where feasible, IoT devices shall have the capability to roll back to a previous known-good state in case of failed or problematic patch installations.
* **Contingency Plans:** Contingency plans shall be developed to address potential issues during patch deployment, including communication outages, device failures, or unexpected behaviour.

# Responsibilities

* **Information Security Officer:** Responsible for overseeing the implementation and enforcement of this policy.
* **IT Department:** Responsible for managing the patch management process, including vulnerability monitoring, patch testing, deployment, and incident response.
* **Device Owners:** Responsible for ensuring that their IoT devices are included in the patch management program and that patches are applied in a timely manner.
* **Change Management Team:** Responsible for reviewing and approving patch deployment plans.

# 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