Internet of Things (IoT) Security Framework for Industry 4.0

"Ongoing Maintenance and Updates"

|  |  |
| --- | --- |
| 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](#_Toc176333501)

[2. Purpose 4](#_Toc176333502)

[3. Scope 4](#_Toc176333503)

[4. Policy Statement 4](#_Toc176333504)

[4.1. Routine Maintenance 4](#_Toc176333505)

[4.2. Firmware and Software Updates 4](#_Toc176333506)

[4.3. Vulnerability Management and Patching 4](#_Toc176333507)

[4.4. End-of-Life and Decommissioning 5](#_Toc176333508)

[5. Responsibilities 5](#_Toc176333509)

[6. Breaches of Policy 5](#_Toc176333510)

[7. Document Management 5](#_Toc176333511)

# Introduction

The Internet of Things (IoT) ecosystem is characterised by a rapid pace of technological advancement and the constant emergence of new security threats. To ensure the continued security, functionality, and performance of IoT devices and systems, ongoing maintenance and updates are essential. This policy outlines the procedures and guidelines for maintaining and updating IoT devices throughout their lifecycle.

# Purpose

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

* Ensure that IoT devices remain secure and protected against emerging threats.
* Address vulnerabilities and bugs through timely updates and patches.
* Optimise device performance and functionality.
* Manage the lifecycle of IoT devices, including decommissioning and secure disposal.

# 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

## Routine Maintenance

* **Regular Inspections:** IoT devices shall be subject to regular inspections to identify any physical damage, wear and tear, or signs of tampering.
* **Cleaning and Calibration:** Devices shall be cleaned and calibrated as per manufacturer recommendations to ensure optimal performance and accuracy.
* **Battery Replacement:** Batteries in IoT devices shall be replaced or recharged as needed to prevent power-related disruptions or failures.

## Firmware and Software Updates

* **Regular Updates:** Firmware and software updates shall be applied to IoT devices in a timely manner to address security vulnerabilities, improve functionality, and enhance performance.
* **Secure Update Mechanisms:** Updates shall be delivered through secure channels and verified for authenticity and integrity before installation.
* **Testing and Validation:** Updates shall be tested in a controlled environment before deployment to production devices to ensure compatibility and minimise disruption.

## Vulnerability Management and Patching

* **Vulnerability Scanning:** IoT devices shall be regularly scanned for known vulnerabilities using automated tools and manual assessments.
* **Patch Prioritisation:** Identified vulnerabilities shall be assessed and prioritised based on their severity and potential impact.
* **Timely Patching:** Security patches shall be applied promptly to address identified vulnerabilities.
* **Zero-Day Vulnerabilities:** Procedures shall be in place to respond to and mitigate the risks associated with zero-day vulnerabilities.

## End-of-Life and Decommissioning

* **End-of-Life Management:** IoT devices that have reached their end-of-life or are no longer supported by the manufacturer shall be identified and scheduled for decommissioning.
* **Secure Decommissioning:** Decommissioned devices shall be securely removed from the network and any sensitive data stored on the devices shall be erased or destroyed in accordance with data destruction policies.

# Responsibilities

* **Information Security Officer:** Responsible for overseeing the implementation and enforcement of this policy.
* **IT Department:** Responsible for managing the maintenance and update process for IoT devices, including vulnerability management, patch deployment, and secure decommissioning.
* **Device Owners:** Responsible for ensuring that their IoT devices are included in the maintenance and update program and that updates are applied in a timely manner.

# 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