TrustIoT Framework for Industry 4.0

"Regular Assessments: Vulnerability scanning & penetration testing"

|  |  |
| --- | --- |
| 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](#_Toc176333296)

[2. Purpose 4](#_Toc176333297)

[3. Scope 4](#_Toc176333298)

[4. Policy Statement 4](#_Toc176333299)

[4.1. Vulnerability Identification 4](#_Toc176333300)

[4.2. Vulnerability Assessment 4](#_Toc176333301)

[4.3. Remediation and Mitigation 4](#_Toc176333302)

[4.4. Vulnerability Reporting and Communication 5](#_Toc176333303)

[5. Responsibilities 5](#_Toc176333304)

[6. Breaches of Policy 5](#_Toc176333305)

[7. Document Management 5](#_Toc176333306)

# Introduction

The Internet of Things (IoT) ecosystem comprises a vast and diverse array of interconnected devices, each with its own potential vulnerabilities. These vulnerabilities, if exploited, can lead to unauthorised access, data breaches, service disruptions, and even physical harm. A proactive and systematic approach to vulnerability management is essential to identify, assess, and mitigate these risks, ensuring the continued security and resilience of the IoT infrastructure.

# Purpose

The purpose of this policy is to establish a framework for identifying, assessing, and remediating vulnerabilities in IoT devices and systems 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

## Vulnerability Identification

* **Asset Inventory:** A comprehensive inventory of all IoT devices and systems shall be maintained, including details such as make, model, firmware version, and location.
* **Vulnerability Scanning:** Regular vulnerability scans shall be conducted using automated tools and manual assessments to identify known vulnerabilities in IoT devices and systems.
* **Threat Intelligence:** Threat intelligence feeds and security advisories shall be monitored to stay informed about emerging threats and vulnerabilities.
* **Penetration Testing:** Periodic penetration testing may be conducted to simulate real-world attacks and identify potential weaknesses in the IoT infrastructure.

## Vulnerability Assessment

* **Risk-Based Prioritisation:** Identified vulnerabilities shall be assessed and prioritised based on their severity, potential impact, and exploitability.
* **Vulnerability Scoring:** A standardised vulnerability scoring system, such as the Common Vulnerability Scoring System (CVSS), may be used to quantify the risk associated with each vulnerability.

## Remediation and Mitigation

* **Timely Patching:** Security patches and updates from trusted sources shall be applied promptly to address identified vulnerabilities.
* **Compensating Controls:** Where patching is not immediately feasible, compensating controls, such as network segmentation or access restrictions, shall be implemented to mitigate the risks associated with vulnerabilities.
* **Zero-Day Vulnerabilities:** Procedures shall be in place to respond to and mitigate the risks associated with zero-day vulnerabilities, including temporary workarounds or isolation of affected devices.

## Vulnerability Reporting and Communication

* **Centralised Reporting:** A centralised system or process shall be established for reporting and tracking identified vulnerabilities.
* **Communication:** Relevant stakeholders, including device owners and system administrators, shall be promptly notified of identified vulnerabilities and required remediation actions.
* **Documentation:** All vulnerability assessments, remediation actions, and related communications shall be documented for audit and compliance purposes.

# Responsibilities

* **Information Security Officer:** Responsible for overseeing the implementation and enforcement of this policy.
* **IT Department:** Responsible for conducting vulnerability scans, assessments, and remediation activities.
* **Device Owners:** Responsible for ensuring that their IoT devices are included in vulnerability management processes and that identified vulnerabilities are addressed in a timely manner.
* **Software Developers/Vendors:** Responsible for providing timely security patches and updates for their products.

# 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