TrustIoT Framework for Industry 4.0

"Comprehensive vulnerability management for legacy systems"

|  |  |
| --- | --- |
| 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](#_Toc190897259)

[2. Purpose 4](#_Toc190897260)

[3. Scope 4](#_Toc190897261)

[4. Policy Statement 4](#_Toc190897262)

[4.1. Legacy System Identification and Inventory 4](#_Toc190897263)

[4.2. Risk Assessment and Prioritisation 4](#_Toc190897264)

[4.3. Mitigation and Remediation Strategies 4](#_Toc190897265)

[4.4. Change Management and Monitoring 5](#_Toc190897266)

[5. Responsibilities 5](#_Toc190897267)

[6. Breaches of Policy 5](#_Toc190897268)

[7. Document Management 5](#_Toc190897269)

# Introduction

Legacy systems, while often critical to business operations, can pose significant security risks due to outdated technologies, lack of vendor support, and inherent vulnerabilities. These systems may not be easily patched or upgraded, making them attractive targets for cyberattacks. A comprehensive vulnerability management approach is essential to identify, assess, and mitigate risks associated with legacy systems, ensuring their continued operation while minimising potential security breaches.

# Purpose

The purpose of this policy is to establish a framework for managing vulnerabilities in legacy systems within the organisation. This policy aims to:

* Identify and inventory all legacy systems within the organisation's IT infrastructure
* Assess and prioritise vulnerabilities based on their potential impact and exploitability
* Implement appropriate mitigation and remediation strategies to address identified vulnerabilities
* Establish a process for continuous monitoring and improvement of the security posture of legacy systems

# Scope

This policy applies to all legacy systems within the organisation, defined as systems that are no longer supported by the vendor or have reached their end-of-life. This includes, but is not limited to:

* Operating systems
* Applications
* Hardware devices
* Network infrastructure components

# Policy Statement

## Legacy System Identification and Inventory

* **Comprehensive Inventory:** A detailed inventory of all legacy systems shall be maintained, including information such as system name, version, location, and criticality to business operations.
* **Regular Reviews:** The inventory shall be reviewed periodically to identify new legacy systems and ensure its accuracy.

## Risk Assessment and Prioritisation

* **Vulnerability Assessment:** Legacy systems shall be assessed for vulnerabilities using a combination of automated tools, manual reviews, and penetration testing.
* **Risk Prioritisation:** Identified vulnerabilities shall be prioritised based on their severity, potential impact, and exploitability, considering the criticality of the affected systems.

## Mitigation and Remediation Strategies

* **Patching and Upgrades:** Where possible, security patches and upgrades shall be applied to legacy systems to address known vulnerabilities.
* **Compensating Controls:** When patching or upgrading is not feasible, compensating controls shall be implemented to mitigate the risks associated with vulnerabilities. These controls may include:
  + Network segmentation and isolation
  + Access restrictions and strong authentication
  + Intrusion detection and prevention systems (IDPS)
  + Application whitelisting
  + Regular backups and data recovery procedures
* **System Replacement:** In cases where the risks associated with legacy systems cannot be adequately mitigated, plans shall be developed for their replacement with modern, supported systems.

## Change Management and Monitoring

* **Change Control:** Any changes to legacy systems, including configuration changes, software installations, or hardware replacements, shall be subject to a formal change management process to ensure proper authorisation, testing, and documentation.
* **Continuous Monitoring:** Legacy systems shall be continuously monitored for signs of compromise or suspicious activity, utilising intrusion detection systems, log analysis, and other security tools.

# Responsibilities

* **Information Security Officer:** Responsible for overseeing the implementation and enforcement of this policy.
* **IT Department:** Responsible for conducting vulnerability assessments, implementing mitigation strategies, and managing the change control process for legacy systems.
* **System Owners:** Responsible for identifying and inventorying legacy systems within their areas of responsibility and collaborating with the IT department on vulnerability management efforts.

# 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