TrustIoT Framework for Industry 4.0

" Standardised procedures for verifying third-party software components"

|  |  |
| --- | --- |
| 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](#_Toc176332258)

[2. Purpose 4](#_Toc176332259)

[3. Scope 4](#_Toc176332260)

[4. Policy Statement 4](#_Toc176332261)

[4.1. Risk Assessment 4](#_Toc176332262)

[4.2. Source Code Review 4](#_Toc176332263)

[4.3. Vulnerability Scanning and Penetration Testing 4](#_Toc176332264)

[4.4. Security Testing 5](#_Toc176332265)

[4.5. Vendor Due Diligence 5](#_Toc176332266)

[4.6. Ongoing Monitoring 5](#_Toc176332267)

[5. Responsibilities 5](#_Toc176332268)

[6. Breaches of Policy 5](#_Toc176332269)

[7. Document Management 5](#_Toc176332270)

# Introduction

The integration of third-party software components into an organisation's IT infrastructure introduces potential security risks. These components may contain vulnerabilities or malicious code that can compromise the confidentiality, integrity, and availability of systems and data. To mitigate these risks, it is imperative to establish standardised procedures for verifying the security and trustworthiness of third-party software before its deployment.

# Purpose

The purpose of this policy is to define a systematic approach for evaluating and verifying the security of third-party software components before their integration into the organisation's environment. This policy aims to:

* Minimise the risk of introducing vulnerabilities or malicious code through third-party software.
* Ensure that third-party software components adhere to the organisation's security standards and requirements.
* Establish a process for ongoing monitoring and management of third-party software risks.

# Scope

This policy applies to all third-party software components that are integrated or utilised within the organisation's IT infrastructure, including but not limited to:

* Commercial off-the-shelf (COTS) software
* Open-source software
* Libraries and frameworks
* Software-as-a-Service (SaaS) applications

# Policy Statement

## Risk Assessment

* **Prior to Acquisition:** A comprehensive risk assessment shall be conducted before acquiring or integrating any third-party software component. This assessment shall consider factors such as:
  + The criticality of the software to business operations
  + The potential impact of a security breach or compromise
  + The vendor's reputation and security track record
  + The availability of security documentation and support

## Source Code Review

* **When Necessary:** For critical software components or when deemed necessary based on the risk assessment, a source code review shall be conducted to identify potential vulnerabilities or malicious code.
* **Qualified Personnel:** Source code reviews shall be performed by qualified personnel with expertise in secure coding practices and vulnerability analysis.

## Vulnerability Scanning and Penetration Testing

* **Regular Scanning:** Third-party software components shall be regularly scanned for known vulnerabilities using automated tools and manual assessments.
* **Penetration Testing:** Penetration testing may be conducted to simulate real-world attacks and identify potential weaknesses in the software.

## Security Testing

* **Functional and Security Testing:** Third-party software shall undergo functional and security testing to ensure it operates as intended and does not introduce security risks.
* **Test Environments:** Testing shall be performed in isolated environments to prevent any impact on production systems.

## Vendor Due Diligence

* **Vendor Assessment:** A thorough assessment of the vendor's security practices and policies shall be conducted before engaging their services or products.
* **Security Documentation:** Vendors shall provide adequate security documentation, including vulnerability disclosures, security advisories, and incident response plans.
* **Ongoing Communication:** Open communication channels shall be maintained with vendors to address security concerns and receive timely updates.

## Ongoing Monitoring

* **Vulnerability Monitoring:** Third-party software components shall be continuously monitored for newly discovered vulnerabilities.
* **Prompt Patching:** Security patches and updates shall be applied promptly to address identified vulnerabilities.
* **Software Updates:** Regular software updates from trusted sources shall be installed to ensure the software remains secure and up-to-date.

# Responsibilities

* **Information Security Officer:** Responsible for overseeing the implementation and enforcement of this policy.
* **IT Department:** Responsible for conducting risk assessments, security testing, and vulnerability management for third-party software.
* **Procurement Department:** Responsible for incorporating security requirements into vendor contracts and conducting vendor due diligence.
* **Users:** Responsible for reporting any security incidents or concerns related to third-party software.

# 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) Standards Framework for Industry 4.0.
* Legislative requirements defined by law, where appropriate.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

[Name 1]

Manager