TrustIoT Framework for Industry 4.0

"Emerging Threats"

|  |  |
| --- | --- |
| 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](#_Toc176333797)

[2. Purpose 4](#_Toc176333798)

[3. Scope 4](#_Toc176333799)

[4. Policy Statement 4](#_Toc176333800)

[4.1. Threat Intelligence and Monitoring 4](#_Toc176333801)

[4.2. Vulnerability Management and Patching 4](#_Toc176333802)

[4.3. Security Awareness and Training 4](#_Toc176333803)

[4.4. Incident Response and Recovery 5](#_Toc176333804)

[5. Responsibilities 5](#_Toc176333805)

[6. Breaches of Policy 5](#_Toc176333806)

[7. Document Management 5](#_Toc176333807)

# Introduction

The rapid evolution of the Internet of Things (IoT) ecosystem brings forth new and sophisticated threats that can compromise the confidentiality, integrity, and availability of connected devices and the data they handle. These emerging threats may exploit vulnerabilities in IoT devices, communication protocols, or cloud platforms, leading to data breaches, service disruptions, or even physical harm. This policy outlines the organisation's commitment to proactively addressing emerging threats through continuous monitoring, vulnerability management, and incident response preparedness.

# Purpose

The purpose of this policy is to establish a framework for identifying, assessing, and mitigating emerging threats to the organisation's IoT infrastructure. This policy aims to:

* Stay abreast of the latest developments in the threat landscape and proactively address potential risks.
* Implement effective security controls and countermeasures to protect against emerging threats.
* Ensure that IoT devices and systems are resilient to new and evolving attack vectors.
* Minimise the impact of security incidents through timely detection and response.

# Scope

This policy applies to all IoT devices, systems, and data within the organisation's network, regardless of their location or function.

# Policy Statement

## Threat Intelligence and Monitoring

* **Threat Intelligence Gathering:** The organisation shall actively gather and analyse threat intelligence from reputable sources, including security vendors, industry forums, and government agencies, to stay informed about emerging threats and vulnerabilities relevant to the IoT ecosystem.
* **Real-time Monitoring:** IoT devices, network traffic, and security solutions shall be continuously monitored for signs of suspicious or malicious activity, utilising intrusion detection systems, behavioural analytics, and other security tools.
* **Anomaly Detection:** Advanced analytics and machine learning techniques shall be employed to identify deviations from normal patterns that may indicate potential threats or attacks.

## Vulnerability Management and Patching

* **Regular Scanning:** IoT devices and systems shall be regularly scanned for vulnerabilities using automated tools and manual assessments.
* **Timely Patching:** Identified vulnerabilities shall be addressed promptly by applying patches or updates from trusted sources.
* **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.

## Security Awareness and Training

* **Employee Education:** Employees shall receive regular security awareness training to educate them about emerging threats, social engineering techniques, and best practices for protecting IoT devices and data.
* **Phishing and Social Engineering:** Employees shall be trained to recognise and report phishing attempts and other social engineering tactics that may be used to target IoT devices.

## Incident Response and Recovery

* **Incident Response Plan:** A comprehensive incident response plan shall be developed and maintained, outlining the procedures for responding to and recovering from security incidents involving IoT devices.
* **Incident Response Team:** A dedicated incident response team shall be established with clearly defined roles and responsibilities.
* **Tabletop Exercises:** Regular tabletop exercises shall be conducted to test and refine the incident response plan and ensure preparedness for emerging threats.

# Responsibilities

* **Information Security Officer:** Responsible for overseeing the implementation and enforcement of this policy.
* **Security Operations Centre (SOC):** Responsible for monitoring security events, analysing threats, and coordinating incident response.
* **IT Department:** Responsible for implementing and maintaining security controls, conducting vulnerability assessments, and applying patches.
* **All Employees:** Responsible for adhering to security best practices and reporting any suspected security incidents or vulnerabilities.

# 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