TrustIoT Framework for Industry 4.0

"Gap Analysis"

|  |  |
| --- | --- |
| 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](#_Toc190890082)

[2. Purpose 4](#_Toc190890083)

[3. Scope 4](#_Toc190890084)

[4. Policy Statement 4](#_Toc190890085)

[4.1. Regular Gap Assessments 4](#_Toc190890086)

[4.2. Scope of Assessments 4](#_Toc190890087)

[4.3. Remediation and Improvement 4](#_Toc190890088)

[5. Responsibilities 5](#_Toc190890089)

[6. Breaches of Policy 5](#_Toc190890090)

[7. Document Management 5](#_Toc190890091)

# Introduction

The Internet of Things (IoT) landscape is characterised by rapid technological advancements and evolving security threats. To ensure the ongoing effectiveness of the organisation's IoT security posture, it is essential to conduct regular gap analyses to identify and address any weaknesses or shortcomings in existing controls and processes. This policy outlines the framework for performing gap analyses within the IoT environment.

# Purpose

The purpose of this policy is to establish a systematic approach for identifying and addressing gaps between the organisation's current IoT security practices and the desired level of security, as defined by industry best practices, regulatory requirements, and internal security policies. This policy aims to:

* Proactively identify and assess security weaknesses and vulnerabilities in the IoT infrastructure
* Facilitate continuous improvement of the organisation's IoT security posture
* Ensure compliance with relevant regulations and standards
* Minimise the risk of security breaches and data compromise

# Scope

This policy applies to all IoT devices, systems, and data within the organisation's network, as well as the processes and controls associated with their security and management.

# Policy Statement

## Regular Gap Assessments

* **Frequency:** Gap assessments shall be conducted on a regular basis, at least annually or more frequently as dictated by changes in the threat landscape, technology advancements, or regulatory requirements.
* **Scope:** Assessments shall cover all aspects of IoT security, including device security, network security, data security, access control, incident response, and compliance.
* **Methodology:** A standardised methodology shall be adopted for conducting gap assessments, including the use of questionnaires, interviews, vulnerability scans, and other relevant tools and techniques.

## Scope of Assessments

* **Security Controls:** The effectiveness of existing security controls shall be evaluated against industry best practices, regulatory requirements, and internal security standards.
* **Risk Assessment:** The organisation's risk assessment methodology shall be reviewed to ensure it adequately addresses IoT-specific risks and vulnerabilities.
* **Incident Response:** The incident response plan and procedures shall be assessed for their adequacy in handling IoT-related security incidents.
* **Third-Party Management:** The security practices of third-party vendors and service providers involved in the IoT ecosystem shall be evaluated.

## Remediation and Improvement

* **Gap Identification:** Identified gaps and areas for improvement shall be documented and prioritised based on their risk level and potential impact.
* **Corrective Action Plans:** Action plans shall be developed to address identified gaps, including the implementation of new or enhanced security controls, process improvements, or technology upgrades.
* **Implementation and Monitoring:** Corrective actions shall be implemented in a timely manner, and their effectiveness shall be monitored to ensure that gaps are closed and risks are mitigated.

# Responsibilities

* **Information Security Officer:** Responsible for overseeing the gap analysis process and ensuring that identified gaps are addressed.
* **IT Department:** Responsible for conducting gap assessments, developing corrective action plans, and implementing necessary changes.
* **Internal Audit Department:** May be involved in conducting independent gap assessments to provide an objective evaluation of the organisation's IoT security posture.
* **Department Heads:** Responsible for cooperating with gap assessment activities and implementing corrective actions within their respective areas.

# Breaches of Policy

Failure to conduct regular gap assessments or to address identified gaps in a timely manner may result in increased security risks, non-compliance with regulations, and potential financial or reputational damage to the organisation.

# 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