TrustIoT Framework for Industry 4.0

"Proactive threat modelling and scenario planning"

|  |  |
| --- | --- |
| 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](#_Toc176333831)

[2. Purpose 4](#_Toc176333832)

[3. Scope 4](#_Toc176333833)

[4. Policy Statement 4](#_Toc176333834)

[4.1. Threat Modelling 4](#_Toc176333835)

[4.2. Scenario Planning 4](#_Toc176333836)

[4.3. Risk Assessment and Mitigation 5](#_Toc176333837)

[4.4. Continuous Improvement 5](#_Toc176333838)

[5. Responsibilities 5](#_Toc176333839)

[6. Breaches of Policy 5](#_Toc176333840)

[7. Document Management 5](#_Toc176333841)

# Introduction

The ever-evolving threat landscape necessitates a proactive approach to security, anticipating and preparing for potential attacks. Threat modelling and scenario planning are essential components of a robust security strategy, enabling organisations to identify vulnerabilities, assess potential impacts, and develop effective mitigation strategies. This policy outlines the procedures and guidelines for conducting proactive threat modelling and scenario planning within the organisation's IoT environment.

# Purpose

The purpose of this policy is to establish a framework for proactively identifying, assessing, and mitigating security risks through threat modelling and scenario planning exercises. This policy aims to:

* Anticipate and understand potential threats and attack vectors targeting the organisation's IoT infrastructure.
* Identify vulnerabilities and weaknesses in IoT devices, systems, and processes.
* Develop and implement effective mitigation strategies to reduce the risk of exploitation.
* Enhance the organisation's preparedness and resilience to security incidents.

# 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 Modelling

* **Regular Threat Modelling Exercises:** Threat modelling exercises shall be conducted on a regular basis, considering new and emerging threats, changes in the IoT environment, and lessons learned from previous incidents.
* **Systematic Approach:** A structured threat modelling methodology shall be adopted, such as STRIDE (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege) or DREAD (Damage, Reproducibility, Exploitability, Affected Users, Discoverability).
* **Asset Identification:** Critical IoT assets, including devices, data, and communication channels, shall be identified and prioritised based on their value and potential impact of compromise.
* **Threat Identification:** Potential threats and attack vectors targeting the identified assets shall be identified, considering both internal and external threats.
* **Vulnerability Assessment:** Vulnerabilities in IoT devices, systems, and processes that could be exploited by identified threats shall be assessed.
* **Impact Analysis:** The potential impact of successful attacks on the organisation's operations, data, and reputation shall be evaluated.

## Scenario Planning

* **Scenario Development:** Based on the threat modelling results, realistic scenarios shall be developed to simulate potential attack sequences and their impact on the organisation.
* **Incident Response Playbooks:** Incident response playbooks shall be created or updated to address the identified scenarios, outlining specific actions to be taken in case of an attack.
* **Tabletop Exercises:** Tabletop exercises shall be conducted to test the effectiveness of incident response playbooks and identify areas for improvement.

## Risk Assessment and Mitigation

* **Risk Assessment:** The risks associated with identified threats and vulnerabilities shall be assessed, considering their likelihood and potential impact.
* **Mitigation Strategies:** Appropriate mitigation strategies shall be developed and implemented to reduce the identified risks to an acceptable level. These strategies may include:
  + Technical controls (e.g., encryption, access control, intrusion detection)
  + Operational controls (e.g., security awareness training, incident response procedures)
  + Physical controls (e.g., secure device placement, tamper-evident seals)

## Continuous Improvement

* **Lessons Learned:** Lessons learned from threat modelling exercises, scenario planning, and actual security incidents shall be incorporated into future security assessments and improvement efforts.
* **Regular Reviews:** Threat models and incident response playbooks shall be reviewed and updated periodically to reflect changes in the threat landscape and the organisation's IoT environment.

# Responsibilities

* **Information Security Officer:** Responsible for overseeing the threat modelling and scenario planning process and ensuring that identified risks are addressed.
* **Security Operations Centre (SOC):** Responsible for conducting threat modelling exercises, developing scenarios, and updating incident response playbooks.
* **IT Department:** Responsible for implementing and maintaining security controls and mitigation strategies.
* **Department Heads:** Responsible for participating in threat modelling exercises and scenario planning activities related to their respective areas.

# Breaches of Policy

Failure to comply with this policy or to adequately address identified security risks 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