TrustIoT Framework for Industry 4.0

" Industry specific incident response playbooks"

|  |  |
| --- | --- |
| 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](#_Toc176333645)

[2. Purpose 4](#_Toc176333646)

[3. Scope 4](#_Toc176333647)

[4. Policy Statement 4](#_Toc176333648)

[4.1. Playbook Development 4](#_Toc176333649)

[4.2. Playbook Content 4](#_Toc176333650)

[4.3. Playbook Maintenance and Review 5](#_Toc176333651)

[4.4. Training and Awareness 5](#_Toc176333652)

[5. Responsibilities 5](#_Toc176333653)

[6. Breaches of Policy 5](#_Toc176333654)

[7. Document Management 5](#_Toc176333655)

# Introduction

The Internet of Things (IoT) has revolutionised various industries, but it has also introduced unique security challenges and threats. Incident response in the IoT landscape requires specialised knowledge and tailored procedures to address the specific vulnerabilities and risks associated with different industrial sectors. This policy outlines the development, maintenance, and utilisation of industry-specific incident response playbooks to ensure effective and efficient response to security incidents affecting IoT devices and systems.

# Purpose

The purpose of this policy is to establish a framework for creating and maintaining industry-specific incident response playbooks that provide clear and actionable guidance for handling security incidents within the organisation's IoT environment. This policy aims to:

* Enable a rapid and coordinated response to security incidents, minimising their impact on critical operations and sensitive data.
* Tailor incident response procedures to the specific threats and vulnerabilities prevalent in the organisation's industry sector.
* Ensure that incident response personnel have access to clear and concise guidance for handling various types of IoT security incidents.
* Facilitate continuous improvement of incident response capabilities through regular reviews and updates of playbooks.

# Scope

This policy applies to all IoT devices, systems, and data within the organisation, across all industry sectors in which the organisation operates.

# Policy Statement

## Playbook Development

* **Industry-Specific Focus:** Incident response playbooks shall be developed for each industry sector in which the organisation operates, addressing the unique threats, vulnerabilities, and regulatory requirements associated with that sector.
* **Collaboration and Expertise:** Playbooks shall be developed in collaboration with subject matter experts from relevant departments, including IT, security, operations, and legal.
* **Threat Modelling:** Threat modelling exercises shall be conducted to identify potential attack scenarios and develop corresponding response procedures.
* **Clear and Actionable Steps:** Playbooks shall provide clear, step-by-step instructions for incident responders, including checklists, decision trees, and escalation procedures.

## Playbook Content

* **Incident Identification and Classification:** Playbooks shall define criteria for identifying and classifying different types of IoT security incidents.
* **Containment and Eradication:** Procedures shall be outlined for containing and eradicating threats, including isolation of affected devices, network segmentation, and removal of malicious code.
* **Data Recovery and Restoration:** Guidelines shall be provided for recovering and restoring affected systems and data from clean backups or other reliable sources.
* **Communication and Notification:** Protocols shall be established for communicating with internal and external stakeholders during and after an incident, including notification of regulatory bodies or law enforcement when required.
* **Lessons Learned:** Playbooks shall include a section for documenting lessons learned from each incident and incorporating them into future updates.

## Playbook Maintenance and Review

* **Regular Reviews:** Playbooks shall be reviewed and updated regularly to reflect changes in the threat landscape, technology advancements, and lessons learned from previous incidents.
* **Version Control:** Version control shall be maintained for playbooks to ensure that the latest version is always used during incident response.
* **Testing and Drills:** Incident response playbooks shall be tested through tabletop exercises and drills to validate their effectiveness and identify areas for improvement.

## Training and Awareness

* **Incident Response Training:** All incident response personnel shall receive training on the use of industry-specific playbooks and their roles and responsibilities during an incident.
* **Security Awareness:** General security awareness training shall be provided to all employees to help them identify and report potential security incidents.

# Responsibilities

* **Information Security Officer:** Responsible for overseeing the development, maintenance, and implementation of incident response playbooks.
* **Incident Response Team:** Responsible for executing the playbooks and managing all aspects of incident response.
* **Department Heads:** Responsible for ensuring that their departments are aware of and comply with the incident response procedures outlined in the playbooks.

# Breaches of Policy

Failure to comply with this policy or to follow the procedures outlined in the incident response playbooks 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