TrustIoT Framework for Industry 4.0

"Response Procedures: Incident handling, containment & eradication"

|  |  |
| --- | --- |
| 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](#_Toc190891643)

[2. Purpose 4](#_Toc190891644)

[3. Scope 4](#_Toc190891645)

[4. Policy Statement 4](#_Toc190891646)

[4.1. Incident Response Team 4](#_Toc190891647)

[4.2. Incident Identification and Reporting 4](#_Toc190891648)

[4.3. Incident Assessment and Prioritisation 5](#_Toc190891649)

[4.4. Containment and Eradication 5](#_Toc190891650)

[4.5. Recovery and Restoration 5](#_Toc190891651)

[4.6. Post-Incident Review 5](#_Toc190891652)

[5. Responsibilities 6](#_Toc190891653)

[6. Breaches of Policy 6](#_Toc190891654)

[7. Document Management 6](#_Toc190891655)

# Introduction

The Internet of Things (IoT) ecosystem, with its interconnected devices and vast data flows, presents a complex and dynamic attack surface. Security incidents, such as unauthorised access, data breaches, or service disruptions, can have significant consequences for the organisation. A well-defined and practiced incident response plan is crucial for effectively managing and mitigating the impact of such incidents. This policy outlines the procedures and responsibilities for responding to security incidents within the IoT environment.

# Purpose

The purpose of this policy is to establish a framework for the efficient and coordinated response to security incidents related to IoT devices and systems within the organisation. This policy aims to:

* Minimise the impact of security breaches and disruptions.
* Ensure a swift and organised response to security incidents.
* Facilitate effective communication and collaboration among incident response personnel.
* Enable the recovery of affected systems and data.
* Learn from incidents and continuously improve the organisation's security posture.

# Scope

This policy applies to all security incidents that affect or involve IoT devices and systems connected to the organisation's network, regardless of their location or function.

# Policy Statement

## Incident Response Team

* **Establishment:** A dedicated incident response team shall be established, comprising individuals with the necessary skills and expertise to handle security incidents effectively. The team should include representatives from IT, security, legal, and relevant business units.
* **Roles and Responsibilities:** Clear roles and responsibilities shall be defined for each member of the incident response team, including:
  + Incident Manager: Overall coordination and management of the incident response process
  + Technical Lead: Technical analysis and containment of the incident
  + Communication Lead: Internal and external communication regarding the incident
  + Other relevant roles as needed
* **Training and Awareness:** Incident response team members shall receive regular training and awareness updates to ensure their skills and knowledge remain current.
* **On-call Availability:** The incident response team shall maintain on-call availability to respond to incidents outside of normal business hours.

## Incident Identification and Reporting

* **Incident Detection:** Security incidents shall be identified through various mechanisms, including:
  + Monitoring and logging of IoT devices, network infrastructure, and security solutions
  + Anomaly detection and behavioural analytics
  + User reporting of suspicious activity
* **Incident Reporting:** Security incidents shall be reported promptly to the designated incident response team or security personnel through established channels, such as:
  + A dedicated hotline or phone number
  + A designated email address
  + An online incident reporting system
* **Incident Information:** Incident reports shall include all relevant details, such as:
  + The nature of the incident (e.g., unauthorised access, data breach, malware infection)
  + Affected devices or systems
  + Date and time of the incident
  + Potential impact on the organisation
  + Any observed indicators of compromise (IOCs)

## Incident Assessment and Prioritisation

* **Triage:** Reported incidents shall be triaged to assess their severity, potential impact, and urgency.
* **Prioritisation:** Incidents shall be prioritised based on their assessed impact and urgency, ensuring that critical incidents receive immediate attention.
* **Severity Levels:** A clear classification system shall be used to categorise incidents based on their severity, guiding the allocation of resources and response efforts.

## Containment and Eradication

* **Containment:** Immediate action shall be taken to contain the incident and prevent further damage or spread. This may involve:
  + Isolating affected devices or network segments
  + Blocking malicious traffic
  + Disabling compromised accounts
  + Applying security patches or updates
* **Eradication:** The root cause of the incident shall be identified and eradicated, ensuring that the threat is completely removed from the environment. This may involve:
  + Removing malware or malicious code
  + Remediating vulnerabilities
  + Strengthening security controls
* **Evidence Collection:** Forensic evidence shall be collected and preserved in a manner that maintains its integrity and chain of custody, following legal and regulatory requirements.

## Recovery and Restoration

* **System Restoration:** Affected systems and data shall be restored to their normal operating state from clean backups or other reliable sources.
* **Validation:** Restored systems and data shall be thoroughly validated to ensure their integrity and functionality.
* **Communication:** Affected users and stakeholders shall be informed of the incident and recovery efforts.

## Post-Incident Review

* **Lessons Learned:** A comprehensive post-incident review shall be conducted to:
  + Identify the root cause of the incident
  + Assess the effectiveness of the response
  + Identify areas for improvement in incident response procedures and security controls
* **Documentation:** Detailed documentation of the incident, response actions, and lessons learned shall be maintained for future reference and compliance purposes.

# Responsibilities

* **Information Security Officer:** Responsible for overseeing the development, implementation, and maintenance of the incident response plan.
* **Incident Response Team:** Responsible for executing the incident response plan and managing all aspects of incident response.
* **IT Department:** Responsible for providing technical support and expertise during incident response.
* **Management:** Responsible for providing necessary resources and support to the incident response team.
* **All Employees:** Responsible for reporting suspected security incidents promptly and cooperating with incident response efforts.

# Breaches of Policy

Failure to report a security incident or comply with incident response procedures 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