TrustIoT Framework for Industry 4.0

"Endpoint Detection: Anti-malware & endpoint protection platforms"

|  |  |
| --- | --- |
| 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](#_Toc176332419)

[2. Purpose 4](#_Toc176332420)

[3. Scope 4](#_Toc176332421)

[4. Policy Statement 4](#_Toc176332422)

[4.1. Anti-Malware Protection 4](#_Toc176332423)

[4.2. Endpoint Protection Platforms (EPP) 4](#_Toc176332424)

[4.3. Intrusion Detection and Prevention Systems (IDPS) 4](#_Toc176332425)

[4.4. Security Information and Event Management (SIEM) 5](#_Toc176332426)

[4.5. Continuous Monitoring and Response 5](#_Toc176332427)

[5. Responsibilities 5](#_Toc176332428)

[6. Breaches of Policy 5](#_Toc176332429)

[7. Document Management 5](#_Toc176332430)

# Introduction

The proliferation of Internet of Things (IoT) devices has expanded the attack surface of organisational networks, introducing new and evolving threats. IoT devices, often with limited security capabilities, can be exploited to gain unauthorised access, exfiltrate data, or disrupt operations. A robust endpoint detection and protection strategy is essential to identify, prevent, and respond to threats targeting these devices.

# Purpose

The purpose of this policy is to establish a comprehensive framework for detecting and protecting against threats to IoT endpoints within the organisation. This policy aims to:

* Prevent and detect malware infections on IoT devices.
* Monitor and analyse IoT endpoint activity for suspicious behaviour.
* Enable rapid response to security incidents involving IoT devices.
* Safeguard the confidentiality, integrity, and availability of data and systems connected to IoT endpoints.

# Scope

This policy applies to all IoT devices connected to the organisation's network, regardless of their function or manufacturer. This includes, but is not limited to:

* Sensors, actuators, and controllers
* Gateways and edge devices
* Industrial control systems (ICS)
* Wearable and embedded devices

# Policy Statement

## Anti-Malware Protection

* **Deployment:** Anti-malware software or agents, specifically designed for IoT devices, shall be deployed on all applicable endpoints.
* **Regular Updates:** Anti-malware signatures and software shall be updated regularly to ensure protection against the latest threats.
* **Scanning:** Regular scans shall be conducted on IoT devices to detect and remove any malware infections.

## Endpoint Protection Platforms (EPP)

* **Deployment:** Where feasible, EPP solutions shall be implemented to provide comprehensive endpoint protection capabilities, including:
  + Anti-malware and anti-virus
  + Firewall and intrusion prevention
  + Application control and whitelisting
  + Data loss prevention (DLP)
* **Centralised Management:** EPP solutions shall be centrally managed to enable consistent policy enforcement and monitoring across all IoT endpoints.

## Intrusion Detection and Prevention Systems (IDPS)

* **Network-Based IDPS:** Network-based IDPS shall be deployed to monitor network traffic for signs of malicious activity targeting IoT devices.
* **Host-Based IDPS:** Where appropriate, host-based IDPS may be installed on IoT devices to detect and prevent intrusions at the endpoint level.

## Security Information and Event Management (SIEM)

* **Log Collection and Correlation:** Logs from IoT devices, endpoint security solutions, and IDPS shall be collected and correlated using a SIEM system to identify potential threats and security incidents.
* **Alerting:** Automated alerts shall be generated for suspicious activity or potential security breaches, triggering timely investigation and response.

## Continuous Monitoring and Response

* **Real-Time Monitoring:** IoT endpoints shall be continuously monitored for signs of compromise or anomalous behaviour.
* **Incident Response:** A well-defined incident response plan shall be in place to address security incidents involving IoT devices, including containment, eradication, and recovery procedures.

# Responsibilities

* **Information Security Officer:** Responsible for overseeing the implementation and enforcement of this policy.
* **IT Department:** Responsible for deploying and managing endpoint security solutions, IDPS, and SIEM systems.
* **Device Owners:** Responsible for ensuring that their IoT devices are protected and monitored in accordance with this policy.
* **Incident Response Team:** Responsible for investigating and responding to security incidents involving IoT endpoints.

# 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