TrustIoT Framework for Industry 4.0

"Firewalls and Intrusion Detection Systems (IDS)"

|  |  |
| --- | --- |
| 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](#_Toc176333181)

[2. Purpose 4](#_Toc176333182)

[3. Scope 4](#_Toc176333183)

[4. Policy Statement 4](#_Toc176333184)

[4.1. Firewall Deployment and Configuration 4](#_Toc176333185)

[4.2. Intrusion Detection Systems (IDS) 4](#_Toc176333186)

[4.3. Rule Management and Updates 4](#_Toc176333187)

[4.4. Monitoring and Logging 5](#_Toc176333188)

[5. Responsibilities 5](#_Toc176333189)

[6. Breaches of Policy 5](#_Toc176333190)

[7. Document Management 5](#_Toc176333191)

# Introduction

The proliferation of Internet of Things (IoT) devices has significantly expanded the attack surface of organisational networks. These devices, often with diverse functionalities and varying levels of security maturity, can be exploited to gain unauthorised access, propagate malware, or disrupt critical operations. Firewalls and Intrusion Detection Systems (IDS) play a crucial role in safeguarding the network perimeter and internal segments, detecting and preventing unauthorised access and malicious activity.

# Purpose

The purpose of this policy is to establish guidelines and requirements for the deployment, configuration, and management of firewalls and IDS within the organisation's IoT infrastructure. This policy aims to:

* Control and monitor network traffic to and from IoT devices.
* Detect and prevent unauthorised access and malicious activity.
* Protect the confidentiality, integrity, and availability of data and systems connected to the IoT network.
* Ensure compliance with industry best practices and regulatory requirements.

# Scope

This policy applies to all firewalls and IDS deployed within the organisation's network, including those specifically dedicated to protecting IoT devices and segments.

# Policy Statement

## Firewall Deployment and Configuration

* **Network Perimeter:** Firewalls shall be deployed at the network perimeter to control inbound and outbound traffic, allowing only authorised communication.
* **Segmentation:** Firewalls shall be used to segment the network into distinct zones based on security requirements and device types, isolating critical systems and sensitive data from less trusted segments.
* **Rule Management:** Firewall rules shall be configured to explicitly permit or deny traffic based on source/destination IP addresses, ports, protocols, and other relevant criteria.
* **Default Deny:** A default deny policy shall be implemented, meaning that all traffic not explicitly permitted by firewall rules shall be blocked.

## Intrusion Detection Systems (IDS)

* **Network-based IDS:** Network-based IDS shall be deployed to monitor network traffic for signs of malicious activity, such as intrusion attempts, malware propagation, or data exfiltration.
* **Host-based IDS:** Where appropriate, host-based IDS may be installed on critical IoT devices or servers to detect and alert on suspicious activity at the endpoint level.
* **Signature-Based and Anomaly-Based Detection:** IDS shall utilise both signature-based and anomaly-based detection techniques to identify known attack patterns and deviations from normal behaviour.

## Rule Management and Updates

* **Regular Reviews:** Firewall rules and IDS signatures shall be regularly reviewed and updated to address new threats and vulnerabilities.
* **Change Management:** Changes to firewall rules or IDS configurations shall be subject to a formal change management process to ensure proper authorisation and testing.

## Monitoring and Logging

* **Log Collection:** Logs from firewalls and IDS shall be collected and stored securely for analysis and incident response.
* **Real-time Monitoring:** Security information and event management (SIEM) systems or equivalent tools shall be utilised to monitor firewall and IDS logs in real-time, enabling the detection and response to security events.
* **Alerting:** Automated alerts shall be generated for suspicious activity or policy violations, triggering timely investigation and remediation.

# Responsibilities

* **Information Security Officer:** Responsible for overseeing the implementation and enforcement of this policy.
* **Network Administrators:** Responsible for configuring and managing firewalls and IDS.
* **Security Operations Centre (SOC):** Responsible for monitoring security events, analysing threats, and responding to incidents.

# 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