TrustIoT Framework for Industry 4.0

"Segmentation Strategies: VLANs, subnetting & DMZs"

|  |  |
| --- | --- |
| 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](#_Toc176333079)

[2. Purpose 4](#_Toc176333080)

[3. Scope 4](#_Toc176333081)

[4. Policy Statement 4](#_Toc176333082)

[4.1. Segmentation Architecture 4](#_Toc176333083)

[4.2. Access Control between Segments 4](#_Toc176333084)

[4.3. Monitoring and Inspection 5](#_Toc176333085)

[5. Responsibilities 5](#_Toc176333086)

[6. Breaches of Policy 5](#_Toc176333087)

[7. Document Management 5](#_Toc176333088)

# Introduction

The proliferation of Internet of Things (IoT) devices introduces a significant expansion of the attack surface within organisational networks. These devices, often with varying levels of security maturity, can be exploited to gain unauthorised access, propagate malware, or disrupt critical operations. Network segmentation provides a crucial defence mechanism by dividing the network into isolated segments, limiting the lateral movement of threats and containing potential breaches.

# Purpose

The purpose of this policy is to establish guidelines and requirements for implementing network segmentation to enhance the security and resilience of the organisation's IoT infrastructure. This policy aims to:

* Isolate critical systems and sensitive data from less sensitive or potentially compromised IoT devices.
* Restrict the lateral movement of threats within the network.
* Contain the impact of security breaches and limit their propagation.
* Improve network performance and manageability by reducing broadcast domains.

# Scope

This policy applies to all IoT devices and systems 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

## Segmentation Architecture

* **Segmentation Strategy:** A well-defined network segmentation strategy shall be developed, considering the organisation's risk profile, business requirements, and IoT device characteristics.
* **Logical or Physical Segmentation:** Network segmentation may be implemented using logical constructs, such as VLANs or virtual private networks (VPNs), or physical separation of network infrastructure.
* **Segmentation Granularity:** The level of segmentation shall be determined based on the sensitivity and criticality of the data and systems involved, with more sensitive assets residing in more isolated segments.
* **VLANs:** Virtual LANs (VLANs) shall be used to create logical network segments, grouping devices based on their function, sensitivity, or security requirements.
* **Subnetting:** Subnetting shall be employed to divide the network into smaller subnetworks, enhancing security and improving network performance.
* **DMZs:** Demilitarised Zones (DMZs) shall be established to provide a controlled buffer zone between the internal network and the internet, allowing for the secure hosting of publicly accessible services.

## Access Control between Segments

* **Restricted Access:** Communication between network segments shall be strictly controlled and limited to authorised traffic only.
* **Firewalls and Security Gateways:** Firewalls and security gateways shall be deployed at the boundaries of network segments to enforce access control policies and filter traffic.
* **Intrusion Detection and Prevention Systems (IDPS):** IDPS shall be utilised to monitor traffic between segments and detect and block any suspicious or malicious activity.
* **Rule-Based Access Control:** Access control lists (ACLs) or firewall rules shall be configured to explicitly permit or deny traffic between segments based on predefined criteria.

## Monitoring and Inspection

* **Network Traffic Analysis:** Network traffic within and between segments shall be monitored and analysed to identify anomalies, potential threats, and policy violations.
* **Log Collection and Analysis:** Logs from firewalls, IDPS, and other security devices shall be collected and analysed to gain insights into network activity and potential security incidents.
* **Regular Reviews:** Network segmentation architecture and access control policies shall be periodically reviewed and updated to ensure their continued effectiveness.

# Responsibilities

* **Information Security Officer:** Responsible for overseeing the implementation and enforcement of this policy.
* **Network Administrators:** Responsible for designing, implementing, and maintaining the network segmentation architecture.
* **Security Operations Centre (SOC):** Responsible for monitoring network traffic, analysing security events, and responding to incidents.
* **System Owners:** Responsible for defining and managing access control policies for their respective systems and data.

# 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