Internet of Things (IoT) Security Framework for Industry 4.0

"Endpoint Protection"

|  |  |
| --- | --- |
| Document Classification: | Internal |
| Document Ref. | *Internet of Things (IoT) Security 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](#_Toc176332403)

[2. Purpose 4](#_Toc176332404)

[3. Scope 4](#_Toc176332405)

[4. Policy Statement 4](#_Toc176332406)

[4.1. Endpoint Security Software 4](#_Toc176332407)

[4.2. Secure Configuration 4](#_Toc176332408)

[4.3. Vulnerability Management 4](#_Toc176332409)

[4.4. Network Segmentation 5](#_Toc176332410)

[4.5. Data Protection 5](#_Toc176332411)

[5. Responsibilities 5](#_Toc176332412)

[6. Breaches of Policy 5](#_Toc176332413)

[7. Document Management 5](#_Toc176332414)

# Introduction

IoT devices, often deployed at the edge of the network, represent a significant attack surface for cyber threats. These devices, with their diverse functionalities and varying levels of security maturity, can be vulnerable to exploitation, leading to data breaches, service disruptions, and even broader network compromises. Implementing robust endpoint protection measures is crucial to safeguard these devices and the sensitive data they handle.

# Purpose

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

* Mitigate the risk of unauthorised access, malware infections, and data breaches on IoT devices.
* Ensure that IoT devices are configured securely and maintained in a hardened state.
* Detect and respond to security incidents on IoT endpoints promptly and effectively.

# 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

## Endpoint Security Software

* **Anti-Malware and Intrusion Prevention:** IoT devices shall be equipped with endpoint security software, including anti-malware and intrusion prevention capabilities, tailored to their specific operating systems and resource constraints.
* **Regular Updates:** Endpoint security software shall be regularly updated to ensure protection against the latest threats.
* **Centralised Management:** Where feasible, endpoint security software shall be centrally managed to enable consistent policy enforcement and monitoring across all IoT devices.

## Secure Configuration

* **Hardening:** IoT devices shall be configured securely, following industry best practices and vendor recommendations. This includes:
  + Disabling unnecessary services and ports
  + Changing default passwords
  + Applying the latest security patches and updates
* **Configuration Management:** A process shall be established to manage and track device configurations, ensuring consistency and compliance with security standards.

## Vulnerability Management

* **Regular Scanning:** IoT devices shall be regularly scanned for vulnerabilities using automated tools and manual assessments.
* **Prompt Patching:** Identified vulnerabilities shall be addressed promptly by applying patches or updates from trusted sources.
* **Zero-Day Vulnerabilities:** Procedures shall be in place to respond to and mitigate the risks associated with zero-day vulnerabilities.

## Network Segmentation

* **Isolation:** IoT devices shall be logically or physically segmented from other parts of the network to limit the impact of potential breaches.
* **Access Control:** Access to IoT devices shall be restricted to authorised personnel and systems, utilising strong authentication and authorisation mechanisms.

## Data Protection

* **Data Encryption:** Sensitive data stored on or transmitted by IoT devices shall be encrypted to protect against unauthorised access or interception.
* **Data Loss Prevention (DLP):** DLP solutions may be implemented to prevent the unauthorised exfiltration of sensitive data from IoT devices.

# Responsibilities

* **Information Security Officer:** Responsible for overseeing the implementation and enforcement of this policy.
* **IT Department:** Responsible for deploying and managing endpoint security solutions, vulnerability management, and network segmentation.
* **Device Owners:** Responsible for ensuring that their IoT devices comply with this policy and receive timely updates.

# 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