Internet of Things (IoT) Security Framework for Industry 4.0

" End-of-life procedures for ensuring complete data destruction and hardware security"

|  |  |
| --- | --- |
| 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](#_Toc190904826)

[2. Purpose 4](#_Toc190904827)

[3. Scope 4](#_Toc190904828)

[4. Policy Statement 4](#_Toc190904829)

[4.1. Data Sanitisation 4](#_Toc190904830)

[4.2. Device Decommissioning 4](#_Toc190904831)

[4.3. Secure Disposal or Reuse 4](#_Toc190904832)

[5. Responsibilities 5](#_Toc190904833)

[6. Breaches of Policy 5](#_Toc190904834)

[7. Document Management 5](#_Toc190904835)

# Introduction

The Internet of Things (IoT) ecosystem involves the deployment of numerous devices with finite lifespans. When these devices reach their end-of-life or are no longer required, it is crucial to ensure their secure decommissioning and disposal to protect sensitive data and prevent unauthorised access. This policy outlines the procedures and controls to be followed when removing IoT devices from service.

# Purpose

The purpose of this policy is to establish a framework for the secure and responsible handling of IoT devices at the end of their lifecycle. This policy aims to:

* Ensure the complete and irreversible removal of sensitive data from IoT devices before disposal or reuse.
* Prevent unauthorised access to decommissioned devices and their residual data.
* Comply with relevant data protection regulations and environmental standards.
* Promote responsible and sustainable disposal practices.

# Scope

This policy applies to all IoT devices deployed or utilised by the organisation that have reached their end-of-life, are being decommissioned, or are no longer required for operational purposes.

# Policy Statement

## Data Sanitisation

* **Data Removal:** Prior to disposal or reuse, all sensitive data, including configuration settings, user credentials, operational data, and any other stored information, shall be securely erased from IoT devices.
* **Sanitisation Methods:** Approved data sanitisation methods shall be employed based on the sensitivity of the data and the device's storage technology. These methods may include:
  + Overwriting: Multiple passes of overwriting with random data to ensure data is unrecoverable
  + Cryptographic Erasure: Encryption of data with strong algorithms and subsequent destruction of the encryption keys
  + Physical Destruction: Physical destruction of storage media, such as shredding or degaussing, for highly sensitive data
* **Verification:** The effectiveness of data sanitisation shall be verified through appropriate technical means or by obtaining a certificate of destruction from a certified third-party provider.

## Device Decommissioning

* **Network Disconnection:** IoT devices shall be securely disconnected from the network and any associated cloud services or management platforms.
* **Access Revocation:** Access credentials and authorisations associated with the device shall be revoked or disabled.
* **Inventory Update:** The organisation's asset inventory shall be updated to reflect the decommissioning of the device.

## Secure Disposal or Reuse

* **Disposal:** IoT devices that are no longer usable or repairable shall be disposed of in an environmentally responsible manner, following applicable e-waste disposal regulations and utilising certified recycling partners.
* **Reuse:** If an IoT device is to be reused within the organisation or transferred to another party, it shall undergo a thorough data sanitisation process as outlined in section 4.1 and be re-provisioned with new credentials and configurations.
* **Third-Party Disposal:** When utilising third-party vendors for device disposal or recycling, due diligence shall be conducted to ensure they adhere to secure data destruction practices and environmental regulations.

# Responsibilities

* **Information Security Officer:** Responsible for overseeing the implementation and enforcement of this policy.
* **IT Department:** Responsible for performing data sanitisation, device decommissioning, and coordinating secure disposal or reuse processes.
* **Device Owners:** Responsible for initiating the decommissioning process and providing necessary information about the device and its data.
* **Procurement Department:** Responsible for ensuring that contracts with third-party disposal or recycling vendors include provisions for secure data destruction and environmental compliance.

# Breaches of Policy

Non-compliance with this policy may result in disciplinary action, up to and including termination of employment or contractual relationships. Additionally, improper disposal of IoT devices containing sensitive data may result in data breaches, privacy violations, and legal or financial penalties for the organisation.

# 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