TrustIoT Framework for Industry 4.0

"Device Physical Security"

|  |  |
| --- | --- |
| 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](#_Toc176332287)

[2. Purpose 4](#_Toc176332288)

[3. Scope 4](#_Toc176332289)

[4. Policy Statement 4](#_Toc176332290)

[4.1. Secure Deployment and Placement 4](#_Toc176332291)

[4.2. Physical Access Control 4](#_Toc176332292)

[4.3. Tamper Detection and Response 4](#_Toc176332293)

[4.4. Secure Disposal and Decommissioning 5](#_Toc176332294)

[5. Responsibilities 5](#_Toc176332295)

[6. Breaches of Policy 5](#_Toc176332296)

[7. Document Management 5](#_Toc176332297)

# Introduction

The physical security of Internet of Things (IoT) devices is a critical aspect of overall information security. IoT devices, often deployed in diverse and sometimes publicly accessible environments, are susceptible to theft, tampering, and unauthorised access. Such breaches can lead to data compromise, disruption of services, and even physical harm. This policy outlines the measures to be taken to ensure the physical security of IoT devices throughout their lifecycle.

# Purpose

The purpose of this policy is to establish a framework for protecting the physical security of IoT devices within the organisation. This policy aims to:

* Prevent unauthorised physical access to IoT devices.
* Safeguard against theft, damage, and tampering of IoT devices.
* Ensure secure deployment and decommissioning of IoT devices.
* Maintain the confidentiality, integrity, and availability of data and systems associated with IoT devices.

# Scope

This policy applies to all IoT devices deployed or utilised by the organisation, regardless of their location or function. 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

## Secure Deployment and Placement

* **Risk Assessment:** A risk assessment shall be conducted prior to deploying IoT devices to identify potential physical security threats and vulnerabilities.
* **Secure Locations:** IoT devices shall be deployed in secure locations with restricted physical access.
* **Environmental Considerations:** Environmental factors, such as temperature, humidity, and electromagnetic interference, shall be considered during deployment to ensure the proper functioning and security of the devices.

## Physical Access Control

* **Physical Barriers:** Physical barriers, such as locked cabinets, cages, or rooms, shall be used to protect IoT devices from unauthorised access.
* **Access Control Systems:** Electronic access control systems, such as key cards or biometric authentication, may be implemented to further restrict access to sensitive areas.
* **Tamper-Evident Seals:** Tamper-evident seals shall be used on IoT devices to detect any attempts at unauthorised physical access or modification.

## Tamper Detection and Response

* **Tamper Detection Mechanisms:** IoT devices shall be equipped with tamper detection mechanisms, such as sensors or switches, to detect physical intrusion or tampering attempts.
* **Alerting and Response:** Tamper events shall trigger alerts to designated personnel or systems, initiating appropriate incident response procedures.

## Secure Disposal and Decommissioning

* **Data Sanitisation:** Prior to disposal or decommissioning, all sensitive data stored on IoT devices shall be securely erased or destroyed in accordance with data destruction policies.
* **Device Decommissioning:** IoT devices shall be securely decommissioned to prevent unauthorised access or reuse.

# Responsibilities

* **Information Security Officer:** Responsible for overseeing the implementation and enforcement of this policy.
* **IT Department:** Responsible for implementing physical security measures and managing access control systems.
* **Facilities Management:** Responsible for maintaining the physical security of facilities where IoT devices are deployed.
* **Device Owners:** Responsible for ensuring the physical security of their IoT devices and reporting any security incidents or concerns.

# 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