Internet of Things (IoT) Security Framework for Industry 4.0

"Secure Installation: Guidelines for preventing physical tampering"

|  |  |
| --- | --- |
| 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](#_Toc176332345)

[2. Purpose 4](#_Toc176332346)

[3. Scope 4](#_Toc176332347)

[4. Policy Statement 4](#_Toc176332348)

[4.1. Site Surveys and Risk Assessments 4](#_Toc176332349)

[4.2. Secure Installation Practices 4](#_Toc176332350)

[4.3. Tamper-Evident Measures 4](#_Toc176332351)

[4.4. Physical Access Controls 5](#_Toc176332352)

[4.5. Environmental Considerations 5](#_Toc176332353)

[5. Responsibilities 5](#_Toc176332354)

[6. Breaches of Policy 5](#_Toc176332355)

[7. Document Management 5](#_Toc176332356)

# Introduction

The physical security of Internet of Things (IoT) devices is paramount in safeguarding the confidentiality, integrity, and availability of sensitive data and critical infrastructure. IoT devices, often deployed in diverse and sometimes publicly accessible environments, are susceptible to physical tampering, unauthorised access, and malicious manipulation. This policy outlines the procedures and guidelines for ensuring the secure installation of IoT devices, with a focus on preventing physical tampering.

# Purpose

The purpose of this policy is to establish a framework for the secure installation of IoT devices within the organisation's environment. This policy aims to:

* Mitigate the risk of unauthorised physical access and tampering with IoT devices.
* Ensure that IoT devices are installed in a manner that protects their integrity and functionality.
* Detect and respond to any attempts at physical tampering or compromise.

# 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

## Site Surveys and Risk Assessments

* **Prior to Installation:** A comprehensive site survey and risk assessment shall be conducted before installing any IoT device. This assessment shall consider factors such as:
  + Physical location and accessibility
  + Potential threats and vulnerabilities
  + Environmental conditions
  + Proximity to sensitive areas or critical infrastructure

## Secure Installation Practices

* **Authorised Personnel:** Only authorised personnel with appropriate training and clearance shall be involved in the installation of IoT devices.
* **Secure Mounting and Placement:** IoT devices shall be securely mounted or placed in a manner that minimises the risk of tampering or unauthorised removal.
* **Cable Management:** Cables and connections shall be properly secured and protected to prevent tampering or accidental disconnection.

## Tamper-Evident Measures

* **Tamper-Evident Seals:** Tamper-evident seals or labels shall be applied to IoT devices and enclosures to provide visual evidence of any unauthorised access or modification.
* **Intrusion Detection:** Where appropriate, intrusion detection sensors or mechanisms shall be employed to detect attempts at physical tampering.

## Physical Access Controls

* **Restricted Access:** Physical access to areas where IoT devices are installed shall be restricted to authorised personnel only.
* **Access Control Systems:** Physical access control systems, such as locks, key cards, or biometric authentication, may be implemented to further restrict access to sensitive areas.

## Environmental Considerations

* **Environmental Protection:** IoT devices shall be protected from harsh environmental conditions, such as extreme temperatures, humidity, or dust, to ensure their proper functioning and security.
* **Electromagnetic Interference (EMI) Protection:** Measures shall be taken to protect IoT devices from EMI that could disrupt their operation or compromise their security.

# Responsibilities

* **Information Security Officer:** Responsible for overseeing the implementation and enforcement of this policy.
* **IT Department:** Responsible for conducting site surveys and risk assessments, implementing secure installation practices, and managing physical access controls.
* **Facilities Management:** Responsible for assisting in the physical security of areas where IoT devices are installed.
* **Device Owners:** Responsible for ensuring that their IoT devices are installed securely and in compliance with this policy.

# 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