Internet of Things (IoT) Security Framework for Industry 4.0

"Tamper-Evident Design"

|  |  |
| --- | --- |
| 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](#_Toc176332323)

[2. Purpose 4](#_Toc176332324)

[3. Scope 4](#_Toc176332325)

[4. Policy Statement 4](#_Toc176332326)

[4.1. Physical Seals 4](#_Toc176332327)

[4.2. Intrusion Detection 4](#_Toc176332328)

[5. Responsibilities 4](#_Toc176332329)

[6. Breaches of Policy 5](#_Toc176332330)

[7. Document Management 5](#_Toc176332331)

# Introduction

The physical security of Internet of Things (IoT) devices is paramount to ensuring the confidentiality, integrity, and availability of the data they collect, process, and transmit. IoT devices, often deployed in diverse and sometimes publicly accessible environments, are susceptible to tampering, unauthorised access, and physical attacks. Tamper-evident design incorporates physical and logical measures to detect and deter such attempts, thereby enhancing the overall security posture of the IoT ecosystem.

# Purpose

The purpose of this policy is to establish guidelines and requirements for implementing tamper-evident design principles in IoT devices within the organisation. This policy aims to:

* Detect and deter unauthorised physical access or modification of IoT devices.
* Trigger alerts and initiate appropriate incident response procedures in case of tampering attempts.
* Maintain the integrity and trustworthiness of IoT devices and the data they handle.

# 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

## Physical Seals

* **Tamper-Evident Seals:** IoT devices shall be equipped with tamper-evident seals or enclosures that provide visual evidence of any unauthorised opening or tampering.
* **Seal Integrity:** Seals shall be designed and applied in a manner that makes it difficult to remove or replace them without leaving clear evidence of tampering.
* **Regular Inspections:** Periodic inspections shall be conducted to verify the integrity of seals on IoT devices.

## Intrusion Detection

* **Sensors and Switches:** IoT devices shall incorporate sensors or switches that can detect physical intrusion or tampering attempts, such as:
  + Case opening sensors
  + Vibration sensors
  + Tilt sensors
* **Alerting and Logging:** Tamper events shall trigger alerts to designated personnel or systems, and detailed logs of such events shall be maintained.
* **Response Procedures:** Clear incident response procedures shall be established to address tamper events, including investigation, remediation, and potential device isolation.

# Responsibilities

* **Information Security Officer:** Responsible for overseeing the implementation and enforcement of this policy.
* **IT Department:** Responsible for configuring and monitoring tamper detection mechanisms and associated alerting systems.
* **Device Owners:** Responsible for ensuring that their IoT devices are equipped with appropriate tamper-evident features and that any tamper events are promptly reported.
* **Facilities Management:** Responsible for assisting in the physical security of areas where IoT devices are deployed.

# 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