Internet of Things (IoT) Security Framework for Industry 4.0

" Physical Security Procedure"

|  |  |
| --- | --- |
| 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](#_Toc177467006)

[2. Scope 4](#_Toc177467007)

[3. Procedures 4](#_Toc177467008)

[3.1. Access Control 4](#_Toc177467009)

[3.2. Environmental Controls 4](#_Toc177467010)

[3.3. Equipment Security 4](#_Toc177467011)

[3.4. Surveillance and Monitoring 4](#_Toc177467012)

[3.5. Security Awareness 5](#_Toc177467013)

[4. Responsibilities 5](#_Toc177467014)

[5. Breaches of Policy 5](#_Toc177467015)

[6. Summary 5](#_Toc177467016)

[7. Document Management 5](#_Toc177467017)

# Introduction

The purpose of this procedure is to establish guidelines and controls to protect the physical assets associated with the organisation's IoT ecosystem from unauthorised access, damage, theft, or disruption.

# Scope

This procedure applies to all physical locations where IoT devices, systems, and data are housed, processed, or transmitted. This includes, but is not limited to, data centres, server rooms, network closets, offices, warehouses, and remote or mobile IoT deployments.

# Procedures

## Access Control

* **Physical Access Control:** Implement appropriate physical access controls to restrict entry to sensitive areas. This may include the use of key cards, biometric authentication, or security personnel.
* **Visitor Management:** Establish procedures for managing visitors, including logging their entry and exit, issuing visitor badges, and escorting them within restricted areas.
* **Secure Areas:** Designate and clearly mark secure areas where IoT devices and systems are located. Limit access to authorised personnel only.
* **Remote Access:** Implement secure remote access mechanisms for managing and monitoring IoT devices in remote or inaccessible locations.

## Environmental Controls

* **Temperature and Humidity:** Maintain appropriate temperature and humidity levels within data centres and server rooms to prevent equipment damage.
* **Fire Suppression:** Install and maintain fire suppression systems to protect against fire hazards.
* **Power Protection:** Utilise uninterruptible power supplies (UPS) and backup generators to ensure continuous operation of critical IoT systems.
* **Water Damage Prevention:** Implement measures to prevent water damage, such as leak detection systems and proper drainage.

## Equipment Security

* **Secure Installation:** Ensure IoT devices are securely installed and protected from physical tampering or theft.
* **Asset Management:** Maintain an inventory of all IoT devices and their locations.
* **Tamper-Evident Seals:** Use tamper-evident seals on critical IoT devices to detect unauthorised access or modifications.
* **Secure Disposal:** Implement procedures for the secure disposal of IoT devices and media to prevent data leakage.

## Surveillance and Monitoring

* **CCTV:** Deploy CCTV cameras in strategic locations to monitor sensitive areas and deter unauthorised access.
* **Intrusion Detection:** Utilise intrusion detection systems (IDS) to detect and alert on unauthorised physical access attempts.
* **Log Management:** Maintain logs of physical access events and review them regularly for anomalies or suspicious activity.

## Security Awareness

* **Training:** Provide regular security awareness training to all personnel on physical security best practices.
* **Clean Desk Policy:** Enforce a clean desk policy to minimise the risk of sensitive information being left unattended.
* **Visitor Awareness:** Educate visitors on physical security protocols and ensure they adhere to them.

# Responsibilities

* **Information Security Officer:** Responsible for overseeing the implementation and enforcement of this policy.
* **IT Department:** Responsible for selecting and configuring appropriate encryption protocols and key management solutions.
* **Device Manufacturers/Vendors:** Responsible for implementing secure communication capabilities in their devices.
* **Users:** Responsible for adhering to this policy 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.

# Summary

By implementing these physical security procedures, organisations can significantly reduce the risk of physical attacks, theft, and damage to their IoT assets. A robust physical security posture is essential for maintaining the confidentiality, integrity, and availability of IoT data and systems.

# 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