Internet of Things (IoT) Security Framework for Industry 4.0

“Standard Authentication Methods: Digital Certificates and Hardware-Based Authentication”

|  |  |
| --- | --- |
| 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](#_Toc190893641)

[2. Purpose 4](#_Toc190893642)

[3. Scope 4](#_Toc190893643)

[4. Policy Statement 4](#_Toc190893644)

[4.1. Digital Certificates 4](#_Toc190893645)

[4.2. Hardware-Based Authentication 4](#_Toc190893646)

[5. Responsibilities 5](#_Toc190893647)

[6. Breaches of Policy 5](#_Toc190893648)

[7. Document Management 5](#_Toc190893649)

# Introduction

In the realm of information security, authentication serves as the first line of defence against unauthorised access. The increasing sophistication of cyber threats necessitates the adoption of robust and reliable authentication methods that can effectively verify the identity of users and devices. This policy outlines the policies for utilising digital certificates and hardware-based authentication mechanisms within the organisation, ensuring a heightened level of security for sensitive systems and data.

# Purpose

The purpose of this policy is to establish clear guidelines and requirements for the implementation and management of digital certificates and hardware-based authentication within the organisation. This policy aims to:

* Enhance the security posture of the organisation by employing strong authentication methods.
* Mitigate the risk of unauthorised access to critical systems and data.
* Ensure compliance with industry best practices and regulatory requirements.

# Scope

This policy applies to all users, devices, and systems within the organisation that require authentication for access. This includes, but is not limited to:

* Employees, contractors, and third-party vendors
* Workstations, laptops, and mobile devices
* Servers, network infrastructure, and cloud services
* Applications and databases containing sensitive information

# Policy Statement

## Digital Certificates

* **Certificate Issuance:** Digital certificates shall be issued by a trusted Certificate Authority (CA) that adheres to industry standards and best practices.
* **Certificate Management:** A robust system shall be implemented for managing the lifecycle of digital certificates, including issuance, renewal, revocation, and secure storage.
* **Key Protection:** Private keys associated with digital certificates shall be protected using strong encryption and access controls.
* **Certificate Usage:** Digital certificates shall be used for various authentication purposes, including:
  + Secure remote access (e.g., VPN)
  + Email encryption and signing
  + Document signing and verification
  + Secure web browsing (HTTPS)

## Hardware-Based Authentication

* **Approved Devices:** Only hardware-based authentication devices that meet the organisation's security requirements shall be permitted.
* **Secure Storage:** Hardware tokens shall be stored securely when not in use to prevent unauthorised access or theft.
* **Multi-Factor Authentication:** Hardware tokens shall be used in conjunction with other authentication factors (e.g., passwords, biometrics) to implement multi-factor authentication.
* **Lost or Stolen Tokens:** Procedures shall be in place for reporting and deactivating lost or stolen hardware tokens promptly.

# Responsibilities

* **Information Security Officer:** Responsible for overseeing the implementation and enforcement of this policy.
* **IT Department:** Responsible for managing the technical infrastructure and processes related to digital certificates and hardware-based authentication.
* **Users:** Responsible for using their authentication credentials responsibly 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