Internet of Things (IoT) Security Framework for Industry 4.0

"Continuous Adaptive Authentication Methods"

|  |  |
| --- | --- |
| 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](#_Toc190893791)

[2. Purpose 4](#_Toc190893792)

[3. Scope 4](#_Toc190893793)

[4. Policy Statement 4](#_Toc190893794)

[4.1. Risk-Based Authentication 4](#_Toc190893795)

[4.2. Behavioural Analytics 4](#_Toc190893796)

[4.3. Contextual Factors 4](#_Toc190893797)

[4.4. Continuous Monitoring 5](#_Toc190893798)

[4.5. Adaptive Response 5](#_Toc190893799)

[5. Responsibilities 5](#_Toc190893800)

[6. Breaches of Policy 5](#_Toc190893801)

[7. Document Management 5](#_Toc190893802)

# Introduction

The traditional model of authentication, relying primarily on static credentials like passwords, is increasingly inadequate in the face of evolving cyber threats. The dynamic nature of modern IT environments, coupled with the proliferation of mobile devices and remote access, necessitates a more adaptive and intelligent approach to authentication. Continuous Adaptive Authentication (CAA) addresses this challenge by continuously evaluating user and device behaviour, context, and risk factors to make real-time access decisions, thereby enhancing security and user experience.

# Purpose

The purpose of this policy is to establish guidelines and requirements for the implementation and management of Continuous Adaptive Authentication within the organisation. This policy aims to:

* Strengthen the organisation's security posture by continuously verifying user and device identities.
* Reduce the reliance on static credentials and passwords.
* Detect and respond to suspicious or anomalous behaviour in real-time.
* Provide a seamless and user-friendly authentication experience.

# 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

## Risk-Based Authentication

* **Risk Assessment:** A risk-based approach shall be adopted to evaluate the risk associated with each access attempt, considering factors such as user role, device type, location, and sensitivity of the requested resource.
* **Adaptive Authentication:** The level of authentication required shall be dynamically adjusted based on the assessed risk, with higher-risk access attempts requiring stronger authentication methods.

## Behavioural Analytics

* **User and Device Profiling:** User and device behaviour patterns shall be analysed to establish baseline profiles.
* **Anomaly Detection:** Deviations from established baseline profiles shall be flagged as potential indicators of unauthorised access or compromised accounts.

## Contextual Factors

* **Geolocation:** User and device location data shall be considered in access decisions, with access potentially restricted from unusual or high-risk locations.
* **Network:** The type of network (e.g., corporate, public Wi-Fi) and its security posture shall be factored into access decisions.
* **Time of Day:** Access attempts outside of normal working hours may be subject to additional scrutiny.

## Continuous Monitoring

* **Session Monitoring:** User sessions shall be continuously monitored for suspicious activity, even after initial authentication.
* **Behavioural Biometrics:** Behavioural biometrics, such as typing patterns or mouse movements, may be used to continuously verify user identity.

## Adaptive Response

* **Step-up Authentication:** In response to suspicious activity or increased risk, users may be prompted to provide additional authentication factors.
* **Session Termination:** User sessions may be terminated automatically if anomalous behaviour is detected.
* **Account Lockout:** Accounts may be temporarily locked in response to repeated failed authentication attempts or other suspicious activity.

# Responsibilities

* **Information Security Officer:** Responsible for overseeing the implementation and enforcement of this policy.
* **IT Department:** Responsible for deploying and managing the technical infrastructure and tools required for CAA.
* **Users:** Responsible for cooperating with CAA measures 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