TrustIoT Framework for Industry 4.0

"Advanced Access Control Policies: Attribute-based access control (ABAC) & Dynamic Policy Enforcement"

|  |  |
| --- | --- |
| Document Classification: | Internal |
| Document Ref. | *TrustIoT 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](#_Toc176331375)

[2. Purpose 4](#_Toc176331376)

[3. Scope 4](#_Toc176331377)

[4. Policy Statement 4](#_Toc176331378)

[4.1. Attribute-Based Access Control (ABAC) 4](#_Toc176331379)

[4.2. Dynamic Policy Enforcement 4](#_Toc176331380)

[5. Responsibilities 5](#_Toc176331381)

[6. Breaches of Policy 5](#_Toc176331382)

[7. Document Management 5](#_Toc176331383)

# Introduction

Traditional access control models, while effective to a certain extent, often struggle to address the complexities and dynamic nature of modern IT environments. The proliferation of cloud services, mobile devices, and the Internet of Things (IoT) necessitates more flexible and adaptive access control mechanisms. This policy outlines the adoption of advanced access control policies, specifically Attribute-Based Access Control (ABAC) and Dynamic Policy Enforcement, to enhance the organisation's security posture and enable fine-grained access decisions based on a variety of attributes and contextual factors.

# Purpose

The purpose of this policy is to establish guidelines and requirements for the implementation and management of ABAC and dynamic policy enforcement within the organisation. This policy aims to:

* Enable more granular and context-aware access control decisions.
* Improve the flexibility and adaptability of access control mechanisms to address evolving business needs and security threats.
* Reduce the administrative overhead associated with managing access control policies.

# Scope

This policy applies to all systems, applications, and data within the organisation that require access control. This includes, but is not limited to:

* On-premises and cloud-based infrastructure
* Enterprise applications and databases
* Sensitive data and intellectual property

# Policy Statement

## Attribute-Based Access Control (ABAC)

* **Attribute Definition:** Access control decisions shall be based on a combination of attributes associated with users, devices, resources, and the environment. These attributes may include:
  + User attributes (e.g., role, department, clearance level)
  + Device attributes (e.g., type, location, security posture)
  + Resource attributes (e.g., sensitivity, classification, ownership)
  + Environmental attributes (e.g., time of day, network location, threat level)
* **Policy Creation:** ABAC policies shall be defined using a clear and expressive language that allows for the specification of complex access control rules based on attribute combinations and logical expressions.
* **Policy Enforcement:** A policy decision point (PDP) shall be implemented to evaluate access requests against ABAC policies and render authorisation decisions.
* **Policy Management:** A centralised system shall be established for managing ABAC policies, including creation, modification, review, and auditing.

## Dynamic Policy Enforcement

* **Real-Time Evaluation:** Access control policies shall be evaluated in real-time, taking into account the current context and any changes in user, device, or environmental attributes.
* **Continuous Monitoring:** Relevant attributes shall be continuously monitored to detect any changes that may impact access decisions.
* **Policy Adaptation:** Access control policies shall be dynamically adjusted in response to changes in attributes or risk levels.
* **Exception Handling:** Mechanisms shall be in place to handle exceptions and allow for temporary or emergency access, when necessary, with appropriate logging and auditing.

# Responsibilities

* **Information Security Officer:** Responsible for overseeing the implementation and enforcement of this policy.
* **IT Department:** Responsible for configuring and maintaining the technical infrastructure to support ABAC and dynamic policy enforcement.
* **Data Owners:** Responsible for defining and managing ABAC policies for the data they own.
* **System Owners:** Responsible for defining and managing ABAC policies for the systems they own.

# 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