# **Fawzooz AI - AI Competence Matrix**

Version: 1.0

Effective Date: [Date]

Document Owner: [e.g., Head of Human Resources]

Approved By: [e.g., AI Governance Committee (AIGC)]

### 1. Purpose and Scope

The purpose of this document is to define the required competencies for personnel in roles that are critical to the Fawzooz AI Management System (AIMS). This matrix serves as a framework for hiring, role definition, training, and professional development.

It ensures that Fawzooz AI has the right skills in place to develop, manage, and oversee our AI systems responsibly, safely, and effectively.

The scope of this matrix includes all roles identified as having a direct and significant impact on the AI lifecycle.

### 2. Competence Levels

The following levels will be used to define the required proficiency for each competence area:

* **Level 1 (Foundational):** Has a basic understanding of the concepts. Can follow procedures and knows when to ask for help.
* **Level 2 (Intermediate):** Can apply the skill independently to routine tasks. Understands the "why" behind procedures.
* **Level 3 (Advanced):** Can handle complex and non-routine tasks. Can analyze, evaluate, and create new solutions within the competence area.
* **Level 4 (Expert):** Recognized as a go-to expert. Can teach, mentor, and set strategy in the competence area.

### 3. Competence Matrix

| **Competence Area** | **Description** | **AI Developer** | **Data Scientist** | **Clinical Lead** | **Product Manager** | **CISO / DPO** | **AIGC Member** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **1. AI Ethical Principles** | Understanding of fairness, accountability, transparency, and Fawzooz AI's ethical policies. | 2 | 3 | 4 | 3 | 4 | 4 |
| **2. Data Governance & Privacy** | Knowledge of data protection regulations (GDPR, HIPAA) and Fawzooz AI's Data Governance Policy. | 2 | 3 | 3 | 2 | 4 | 3 |
| **3. AI Risk Management** | Ability to identify, assess, and treat AI-specific risks using the organization's procedures. | 2 | 3 | 3 | 3 | 4 | 4 |
| **4. Secure AI Development** | Knowledge of secure coding practices, vulnerability management, and adversarial attack vectors for AI. | 3 | 2 | 1 | 1 | 4 | 2 |
| **5. AI Model Development** | Technical skills in machine learning, deep learning, model training, and lifecycle management. | 3 | 4 | 1 | 2 | 1 | 2 |
| **6. Model Validation & Testing** | Ability to design and execute tests for model performance, robustness, fairness, and bias. | 3 | 4 | 2 | 2 | 2 | 2 |
| **7. Clinical Safety & Efficacy** | Understanding of mental health conditions, clinical safety protocols, and therapeutic best practices. | 1 | 1 | 4 | 2 | 1 | 3 |
| **8. ISO/IEC 42001 Standard** | Detailed knowledge of the AIMS framework and the requirements of the standard. | 1 | 2 | 2 | 2 | 4 | 4 |
| **9. AI Impact Assessment** | Ability to conduct and contribute to assessments of the societal and individual impacts of AI systems. | 2 | 3 | 4 | 3 | 3 | 4 |
| **10. Human Oversight Design** | Ability to design effective human-in-the-loop processes and crisis escalation pathways. | 2 | 2 | 4 | 3 | 2 | 3 |

### 4. Role-Specific Competence Requirements (Examples)

#### 4.1. AI Developer

An AI Developer must have advanced (L3) skills in Secure AI Development and Model Development. They need an intermediate (L2) understanding of ethical principles and risk management to build systems that are not only functional but also compliant with our AIMS policies from the ground up.

#### 4.2. Clinical Lead

A Clinical Lead must be an expert (L4) in Clinical Safety & Efficacy and have advanced (L3) knowledge of the ethical and impact assessment aspects of AI. Their role is to be the ultimate safeguard for user well-being, ensuring that technology serves therapeutic goals safely.

#### 4.3. CISO / DPO

The CISO/DPO must be an expert (L4) in the ISO 42001 standard, risk management, and data governance. They are responsible for architecting and overseeing the entire AIMS, ensuring it is robust, compliant, and effective.