# **Fawzooz AI - AI System Development Lifecycle (SDLC) Policy**

Version: 1.0

Effective Date: [Date]

Policy Owner: [e.g., Head of AI Development / Chief Technology Officer]

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

### 1. Purpose and Scope

This policy defines the mandatory phases, controls, and deliverables for the entire lifecycle of Artificial Intelligence (AI) systems at Fawzooz AI. Its purpose is to ensure that all AI systems are designed, developed, tested, deployed, and managed in a manner that is secure, effective, and consistently aligned with our core commitment to responsible and ethical AI in mental wellness.

This policy integrates safety, security, privacy, fairness, and clinical efficacy directly into the development process. It establishes a structured, auditable, and repeatable framework for all AI projects.

This policy applies to all Fawzooz AI employees, contractors, and teams involved in any phase of the AI system lifecycle, including but not limited to product management, data science, engineering, quality assurance, and clinical oversight.

### 2. The Fawzooz AI SDLC Phases

The Fawzooz AI SDLC consists of seven distinct phases. Progression from one phase to the next is contingent upon the successful completion of mandatory gate reviews and deliverables, ensuring a rigorous and controlled development process.

#### **Phase 1: Conception and Planning**

This phase lays the foundation for a responsible AI project.

* **Mandatory Activities:**
  1. **Problem Formulation:** Clearly define the intended use, user base, and therapeutic or wellness goal of the proposed AI system.
  2. **AI System Impact Assessment (AIA):** Conduct a formal AIA to identify potential ethical, societal, and human rights impacts. This is a prerequisite for any further work.
  3. **Initial Risk Assessment:** Perform a preliminary risk assessment based on the AIA findings, identifying high-level clinical, security, and ethical risks.
  4. **Requirements Definition:** Document functional, technical, security, privacy, and, critically, **ethical and safety requirements**.
* **Mandatory Deliverables:**
  + Project Charter
  + Completed AI System Impact Assessment Report
  + Initial AI Risk Assessment Record
  + Formal Requirements Document
* **Gate Review:** The AI Governance Committee (AIGC) must review all deliverables and provide formal approval before the project can proceed to Phase 2.

#### **Phase 2: Design and Data Management**

This phase translates requirements into a technical blueprint with a focus on data integrity and responsible architecture.

* **Mandatory Activities:**
  1. **Ethics-by-Design:** The design must incorporate principles of fairness, transparency, and accountability. The Chief AI Ethics Officer (CAIO) must be consulted.
  2. **Human Oversight Design:** The mechanisms for human oversight (e.g., clinician review panels, crisis intervention handoffs) must be explicitly designed and documented.
  3. **Data Sourcing and Vetting:** Identify and document all data sources. Data must be vetted for quality, relevance, and potential biases.
  4. **Data Governance:** Apply data minimization principles. Classify all data and define handling procedures in line with the Data Governance Policy.
* **Mandatory Deliverables:**
  + System Architecture and Design Document
  + Human Oversight Protocol Document
  + Data Management Plan (including sources, schema, and bias assessment)
* **Gate Review:** Technical and ethical review by the AI Development Lead and the CAIO.

#### **Phase 3: Model Development and Training**

This is the core development phase where the AI model is built and trained.

* **Mandatory Activities:**
  1. **Secure Development Practices:** All development must follow the Secure AI Development Lifecycle (Secure ADLC) standards.
  2. **Bias Mitigation:** Implement and document techniques used to mitigate biases identified in the data.
  3. **Reproducibility:** All aspects of the training process—including code, data versions, hyperparameters, and the trained model itself—must be meticulously version-controlled to ensure full reproducibility.
* **Mandatory Deliverables:**
  + Version-controlled training code and datasets
  + Trained AI model(s) with versioning
  + Model Development and Training Log

#### **Phase 4: Verification and Validation (V&V)**

This phase ensures the AI system is accurate, safe, secure, and fair before it reaches users.

* **Mandatory Activities:**
  1. **Functional Testing:** Verify that the system meets all functional requirements.
  2. **Responsibility Testing:** This is a comprehensive and mandatory testing suite:
     + **Fairness Testing:** Evaluate model performance across different demographic subgroups.
     + **Robustness & Security Testing:** Test against adversarial attacks, edge cases, and unexpected inputs.
     + **Clinical Safety Validation:** The Clinical Lead and their team must conduct a formal validation to assess the clinical safety and efficacy of the AI system's outputs. This is a non-negotiable step for all user-facing wellness tools.
* **Mandatory Deliverables:**
  + Completed Test Plans and Test Results
  + Fairness and Bias Audit Report
  + Security Penetration Test Report
  + **Signed Clinical Safety Validation Report**
* **Gate Review:** Final V&V results must be reviewed and approved by the Head of QA and the Clinical Lead.

#### **Phase 5: Deployment**

This phase manages the controlled release of the AI system into the production environment.

* **Mandatory Activities:**
  1. **Final AIGC Approval:** No AI system can be deployed without a final review of all V&V deliverables and formal deployment approval from the AI Governance Committee.
  2. **Phased Rollout:** High-impact systems must be deployed using a phased or canary rollout strategy to monitor real-world performance on a limited scale before a full release.
  3. **Communication:** Execute the communication plan to inform users and clinicians of the new system or changes.
* **Mandatory Deliverables:**
  + Deployment Plan
  + AIGC Deployment Approval Record

#### **Phase 6: Operation and Monitoring**

This phase covers the ongoing management of the live AI system.

* **Mandatory Activities:**
  1. **Continuous Performance Monitoring:** Implement automated monitoring for model drift, data drift, performance degradation, and the emergence of new biases.
  2. **Incident Response:** The AI Incident Response Plan must be active. All incidents must be logged and managed.
  3. **User Feedback Loop:** Actively collect and review user and clinician feedback to identify issues and areas for improvement.
  4. **Crisis Protocol Activation:** For relevant systems, ensure the Crisis Intervention and Escalation Protocol is active and tested regularly.
* **Mandatory Deliverables:**
  + Live Performance Monitoring Dashboards
  + User Feedback Log
  + AI Incident Log

#### **Phase 7: Decommissioning**

This phase ensures the orderly and secure retirement of an AI system.

* **Mandatory Activities:**
  1. **User Notification:** Inform users of the system's planned retirement.
  2. **Data Disposition:** Securely archive or delete all associated data in accordance with our data retention policies and regulatory requirements (e.g., HIPAA, GDPR).
  3. **Archiving:** Archive the final model, its documentation, and key operational logs for regulatory and legal purposes.
* **Mandatory Deliverables:**
  + Decommissioning Plan
  + Data Destruction/Archiving Certificate

### 3. Policy Compliance

Adherence to this AI SDLC Policy is mandatory. Any deviation must be formally documented, justified, and approved by the AI Governance Committee. Failure to comply may result in project suspension and disciplinary action.

**End of Policy**