# Fawzooz AI - AI Risk Management Procedure

Version: 1.0

Effective Date: [Date]

Procedure Owner: [e.g., Chief Information Security Officer (CISO)]

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

### 1. Purpose and Scope

This document outlines the systematic process for identifying, analyzing, evaluating, and treating risks associated with the design, development, deployment, and operation of Artificial Intelligence (AI) systems at Fawzooz AI.

The purpose of this procedure is to:

* Proactively manage risks to protect our users, our organization, and the community.
* Ensure that AI risks are understood, managed to an acceptable level, and communicated effectively.
* Provide a consistent and structured framework for risk-based decision-making.

This procedure applies to all AI systems within the scope of the Fawzooz AI Management System (AIMS) and all personnel involved in the AI lifecycle.

### 2. Roles and Responsibilities

| **Role** | **Responsibilities** |
| --- | --- |
| **AI Governance Committee (AIGC)** | Oversees the risk management framework, reviews and approves risk acceptance criteria, and provides strategic direction on high-level risks. |
| **Chief Information Security Officer (CISO)** | Owns and maintains this procedure. Ensures the integration of AI risk management with the overall enterprise risk management framework. |
| **Risk Owner** | An individual with the accountability and authority to manage a specific risk. Responsible for monitoring the risk and the effectiveness of treatment plans. |
| **AI Development Teams** | Responsible for identifying and assessing risks during the AI system lifecycle, implementing risk treatment controls, and documenting risks in the AI Risk Register. |
| **AI Ethics Officer** | Provides expert guidance on ethical, fairness, and societal risks, and is a key participant in AI Impact Assessments. |

### 3. AI Risk Management Process

The AI risk management process at Fawzooz AI is an iterative cycle composed of the following stages:

*(Diagram: Risk Identification -> Risk Analysis -> Risk Evaluation -> Risk Treatment. This entire process is subject to ongoing Monitoring, Review, and Communication.)*

#### 3.1. Stage 1: Risk Identification

Risks shall be identified proactively and continuously throughout the AI system lifecycle. Methods for identification include:

* **AI Impact Assessments:** Conducted for all new AI systems or major changes to existing ones to identify potential impacts on individuals, society, and human rights.
* **Threat Modeling:** Performed during the design and development phases to identify security vulnerabilities and potential attack vectors.
* **Workshops and Brainstorming:** Held with cross-functional teams (developers, clinicians, ethicists, legal).
* **Incident Analysis:** Reviewing past incidents and near-misses to identify recurring risks.
* **External Sources:** Monitoring regulatory changes, industry reports, and academic research.

All identified risks must be recorded in the **AI Risk Register**.

#### 3.2. Stage 2: Risk Analysis

For each identified risk, the likelihood of occurrence and the potential impact must be analyzed.

**Impact Criteria:** The impact of a risk will be assessed across multiple dimensions, with a primary focus on user well-being given our specialization in mental wellness.

| **Rating** | **User & Societal Impact** | **Operational & Financial Impact** |
| --- | --- | --- |
| **5 (Catastrophic)** | Severe psychological harm, loss of life, widespread violation of rights, significant societal distrust. | Major service disruption, catastrophic financial loss, business failure. |
| **4 (Major)** | Significant psychological distress, discrimination, widespread privacy breaches. | Significant service degradation, major financial loss, regulatory action. |
| **3 (Moderate)** | Measurable negative impact on user well-being, localized bias, privacy concerns. | Service impairment, moderate financial loss, reputational damage. |
| **2 (Minor)** | Minor inconvenience or temporary distress to users, low-level inaccuracies. | Minor operational issues, minor financial loss. |
| **1 (Insignificant)** | Negligible or no discernible impact on users. | Negligible operational impact. |

**Likelihood Criteria:** The likelihood of a risk occurring will be assessed based on available data, historical trends, and expert judgment.

| **Rating** | **Description** |
| --- | --- |
| **5 (Almost Certain)** | Expected to occur in most circumstances; >90% probability. |
| **4 (Likely)** | Will probably occur in most circumstances; 50-90% probability. |
| **3 (Possible)** | Might occur at some time; 20-50% probability. |
| **2 (Unlikely)** | Could occur at some time, but not expected; 5-20% probability. |
| **1 (Rare)** | May occur only in exceptional circumstances; <5% probability. |

#### 3.3. Stage 3: Risk Evaluation

The overall risk level is determined by combining the impact and likelihood ratings using the following risk matrix. This evaluation determines the priority for risk treatment.

| **Likelihood** | **Insignificant (1)** | **Minor (2)** | **Moderate (3)** | **Major (4)** | **Catastrophic (5)** |
| --- | --- | --- | --- | --- | --- |
| **Almost Certain (5)** | Medium | High | Critical | Critical | Critical |
| **Likely (4)** | Low | Medium | High | Critical | Critical |
| **Possible (3)** | Low | Medium | High | High | Critical |
| **Unlikely (2)** | Low | Low | Medium | Medium | High |
| **Rare (1)** | Low | Low | Low | Low | Medium |

* **Critical:** Immediate action required. Must not be accepted without AIGC approval.
* **High:** Senior management attention needed. A documented treatment plan is required.
* **Medium:** Risk should be managed through standard procedures.
* **Low:** Risk may be accepted but should be monitored.

#### 3.4. Stage 4: Risk Treatment

Based on the risk evaluation, a treatment option is selected and documented in the **AI Risk Register**.

* **Modify:** Implement controls to reduce the likelihood or impact of the risk. This is the preferred option for most risks.
* **Retain (Accept):** Formally accept the risk without further action. This is only acceptable for Low risks, or for Medium/High risks where the cost of treatment outweighs the benefit, and requires formal sign-off from the Risk Owner and, in some cases, the AIGC.
* **Avoid:** Decide not to proceed with the activity that gives rise to the risk (e.g., halting an AI project).
* **Share:** Transfer or share a portion of the risk with a third party (e.g., through insurance or contractual agreements).

All treatment plans must include a responsible person, a timeline, and required resources.

### 4. Monitoring, Review, and Communication

* **Monitoring:** Risk Owners are responsible for continuously monitoring their assigned risks and the effectiveness of treatment plans.
* **Review:** The AI Risk Register will be formally reviewed by the CISO quarterly, and by the AIGC annually, or whenever a significant change occurs.
* **Communication:** Risk-related information will be communicated to relevant stakeholders in accordance with the Communication Plan.

### 5. Documentation

All activities performed as part of this procedure shall be documented in the **AI Risk Register**. This procedure is supported by the AIMS Manual and the AI Policy.

**End of Procedure**