# Fawzooz AI - AI Risk Register

Version: 1.0

Effective Date: [Date]

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

Maintained By: [e.g., AI Development Teams, Risk Owners]

### 1. Purpose and Scope

This document establishes the official AI Risk Register for Fawzooz AI. The purpose of this register is to provide a single, authoritative record of all identified risks related to our AI systems. It is a living document used to actively manage and communicate risk information across the organization.

The register ensures that all risk management activities—from initial identification through to treatment and monitoring—are systematically documented, assigned ownership, and tracked to completion in accordance with the **AI Risk Management Procedure**.

The scope of this register includes all risks (ethical, security, privacy, operational, clinical, etc.) associated with AI systems covered by the Fawzooz AI Management System (AIMS).

### 2. Instructions for Use

* **Risk Identification:** Any employee can identify a potential risk. It must be submitted to the relevant AI Development Team Lead or the CISO for initial assessment.
* **Recording:** Once validated, the risk must be formally logged in this register and assigned a unique **Risk ID**.
* **Maintenance:** The **Risk Owner** is responsible for keeping the entry for their assigned risk up-to-date, reflecting any changes in status, treatment progress, or risk level.
* **Review:** This register will be reviewed quarterly by the CISO and annually by the AI Governance Committee (AIGC) as part of the management review process.

### 3. AI Risk Register Template

#### **Risk Entry: [Risk ID]**

| **Field** | **Description / Instructions** | **Entry** |
| --- | --- | --- |
| **Risk ID** | A unique identifier (e.g., AI-RISK-001). |  |
| **Date Identified** | The date the risk was formally logged. |  |
| **Risk Source/Category** | The origin of the risk (e.g., Model-related, Data-related, Security, Ethical, External). |  |
| **Risk Description** | A clear, concise description of the risk, explaining the potential event and its cause. |  |
| **AI System/Component Affected** | The specific AI system, model, or component that the risk pertains to. |  |
| **Potential Impact Areas** | The areas that could be affected (e.g., Individuals' rights, Organizational reputation, Legal/Compliance, User well-being). |  |
| **Impact Description** | A detailed description of the potential negative consequences if the risk materializes. |  |
| **Impact Severity Rating (1-5)** | The severity of the impact, based on the criteria in the AI Risk Management Procedure. |  |
| **Likelihood of Occurrence (1-5)** | The likelihood of the risk occurring, based on the criteria in the AI Risk Management Procedure. |  |
| **Overall Risk Level** | The calculated risk level (e.g., Critical, High, Medium, Low) based on the risk matrix. |  |
| **Existing Controls** | Any current measures or controls that are already in place to mitigate this risk. |  |
| **Risk Treatment Decision** | The chosen treatment option (Modify, Retain/Accept, Avoid, Share). |  |
| **Proposed Treatment Action(s)** | A detailed description of the actions or controls to be implemented. |  |
| **Control Reference** | Reference to a specific control in ISO 42001 Annex A or an internal organizational control. |  |
| **Risk Owner** | The individual with the authority and accountability to manage the risk. |  |
| **Treatment Due Date** | The target date for completing the treatment action. |  |
| **Treatment Status** | The current status of the treatment plan (e.g., Planned, In Progress, Implemented, Closed). |  |
| **Residual Risk Level** | The expected risk level *after* the proposed treatment has been successfully implemented. |  |
| **Date of Last Review** | The date the risk entry was last reviewed and updated. |  |
| **Next Review Date** | The date for the next scheduled review of this risk. |  |
| **Comments/Notes** | Any additional relevant information. |  |

### 4. Sample Entry

#### **Risk Entry: AI-RISK-001**

| **Field** | **Entry** |
| --- | --- |
| **Risk ID** | AI-RISK-001 |
| **Date Identified** | 2025-07-20 |
| **Risk Source/Category** | Model-related / Ethical |
| **Risk Description** | The AI-powered chatbot for anxiety support might provide inappropriate or harmful advice in a crisis situation due to limitations in understanding complex user emotional states. |
| **AI System/Component Affected** | Anxiety Support Chatbot (v2.1) |
| **Potential Impact Areas** | Individuals (psychological safety, well-being), Organizational (reputational, legal) |
| **Impact Description** | Could exacerbate a user's mental health crisis, leading to severe psychological harm. Could result in legal liability and catastrophic damage to Fawzooz AI's reputation and user trust. |
| **Impact Severity Rating (1-5)** | 5 (Catastrophic) |
| **Likelihood of Occurrence (1-5)** | 2 (Unlikely) |
| **Overall Risk Level** | High |
| **Existing Controls** | Keyword detection for certain crisis terms; Static links to external crisis hotlines. |
| **Risk Treatment Decision** | Modify |
| **Proposed Treatment Action(s)** | 1. Implement a more sophisticated crisis detection model trained on clinically-validated datasets. 2. Design and implement a "Human-in-the-Loop" protocol that automatically flags high-risk conversations for immediate review by a licensed therapist. 3. Make the "escalate to a human" option more prominent and accessible at all points in the conversation. |
| **Control Reference** | ISO 42001: A.4.7 (AI system operation), ORG-AI-CTRL-001 (Ethical AI Review Board Charter) |
| **Risk Owner** | Head of Clinical AI |
| **Treatment Due Date** | 2025-10-31 |
| **Treatment Status** | Planned |
| **Residual Risk Level** | Low |
| **Date of Last Review** | 2025-07-24 |
| **Next Review Date** | 2025-10-24 |
| **Comments/Notes** | Treatment plan approved by AIGC on 2025-07-23. Budget allocated for therapist oversight. |