AEGISAI – ENTERPRISE RISK INTELLIGENCE PLATFORM

Official Master Specification Document (Version 1.0)

1. PROJECT OVERVIEW

Project Name: AegisAI – Enterprise Risk Intelligence Platform

Project Type: Full-Stack AI System (Production-Ready)

Domain: Enterprise Internal Banking Risk Monitoring System

Purpose:

Detect fraudulent transactions, perform credit risk scoring, detect anomalies,

generate explainable investigation reports using LLMs, implement agent orchestration,

deploy on Azure, and integrate full MLOps monitoring.

2. CORE PROBLEM STATEMENT

Financial institutions require real-time fraud detection, explainable decisions,

and automated investigation workflows. AegisAI solves this using ML, DL, NLP,

Agentic AI, Azure deployment, and MLOps.

3. HIGH-LEVEL ARCHITECTURE

Frontend (Next.js) → FastAPI Backend → ML Risk Engine → LLM Investigation Engine

→ Agent Orchestrator → Azure Storage & Monitoring

4. MACHINE LEARNING COMPONENTS

- Fraud Detection (Logistic Regression, Random Forest, XGBoost)

- Anomaly Detection (Isolation Forest, Autoencoder, One-Class SVM)

- Time-Series Risk Detection (LSTM)

Evaluation Metrics:

ROC-AUC, Precision-Recall, F1 Score

5. NLP + LLM INVESTIGATION ENGINE

- SHAP for explainability

- RAG pipeline for similar case retrieval

- Azure OpenAI for structured investigation reports

6. AGENT SYSTEM

Data Agent → Risk Agent → Investigation Agent → Decision Agent

7. DATA PIPELINE

Data Ingestion → Cleaning → Feature Engineering → Imbalance Handling →

Training → Evaluation → Model Saving → MLflow Logging

8. MLOPS PIPELINE

Experiment Tracking → Model Registry → Deployment → Monitoring →

Drift Detection → Auto Retraining

9. AZURE DEPLOYMENT

Azure App Service, Blob Storage, Container Registry, Azure OpenAI,

Azure Monitor (Student Plan Compatible)

10. CURRENT PROJECT STATUS

Completed:

- Project structure created
- Backend initialized
- Frontend initialized
- Azure resource group created
- Database configuration setup

Pending:

- EDA completion
- ML model training
- SHAP integration
- LLM integration
- Agent orchestration
- Deployment
- MLOps integration

11. FINAL OBJECTIVE

Demonstrate end-to-end AI system design covering:

EDA, Statistics, ML, DL, NLP, Explainable AI, Agentic AI,

Azure Cloud Deployment, and MLOps Monitoring.

Owner: Kunal Saini

Version: 1.0