Security Review Supplement

Purpose

This document serves as a supplement to the original technical proposal (v2). It consolidates and highlights key information regarding the system's data privacy scope, technology stack, and data flow to facilitate an efficient security review. All information presented here is sourced directly from the original proposal.

Data Privacy & System Scope Commitment

The system is architected to process **course materials only** and will not handle student records or any other Personally Identifiable Information (PII). This is a strict architectural boundary.

- *(Reference: Original Proposal, Page 15, "Data Protection")*

Technology Stack

The project will be deployed within UIC's managed AWS infrastructure.

- **Backend:** Python (PydanticAI, LangChain)
- **Frontend:** JavaScript / TypeScript (Astro, Radix UI, Tailwind CSS)
- **Infrastructure:** UIC-Managed AWS Environment (AWS ECS with Fargate, Redis, AWS S3, CloudFront CDN)
- *(Reference: Original Proposal, Page 4, "Technology Stack Rationale" and Page 5, "Infrastructure Specifications")*

Cloud Security & Compliance

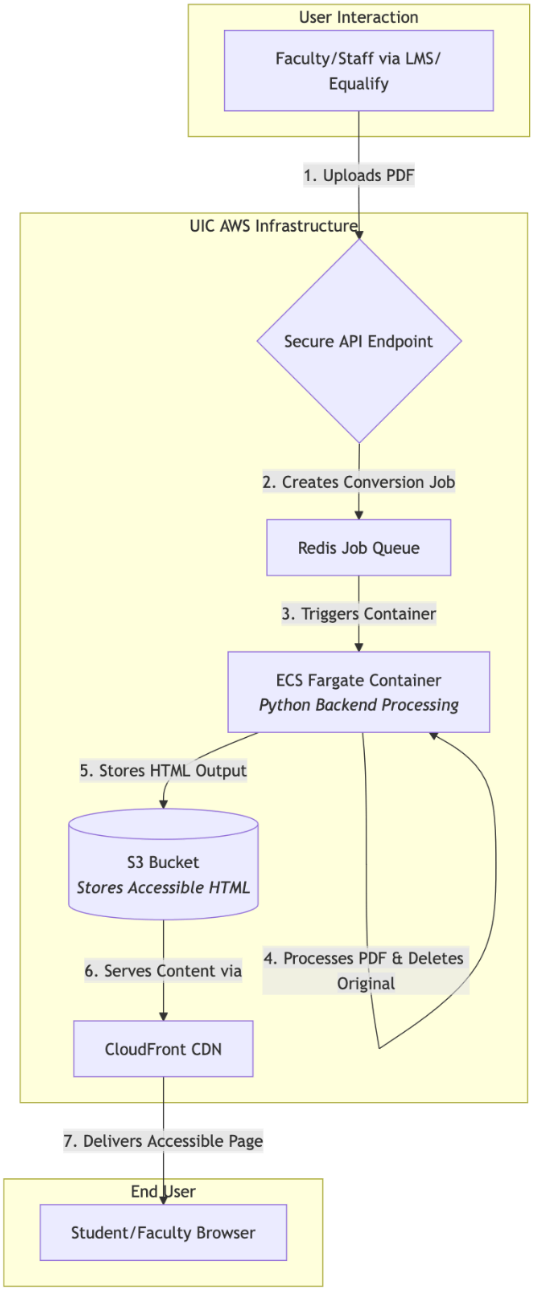
The system will adhere to AWS security best practices, including end-to-end encryption for data in transit and at rest, and will integrate with UIC's authentication systems for access control.

- *(Reference: Original Proposal, Page 15, "System Security")*

Content Data Flow

The following diagram illustrates the secure flow of a document from submission to delivery. The process is initiated via a secure API endpoint and utilizes ephemeral processing containers.

Data Flow Diagram:



- *(Reference: Original Proposal, Page 1, "Multi-Agent Processing Pipeline" and Page 7, "API-First Design")*