ECE 49595 - Team 5 Final Software Development Plan

Fall 2025

Previous SDP Work

This document consolidates our initial Software Development Plan and all subsequent updates from project journals into one final plan. Per course instructions, MoSCoW artifacts are excluded, and the resulting priorities are reflected directly in the requirements, deliverables, and schedule.

Updates Since Initial SDP and Journal Updates (Summary):

- Decomposed project scope into distinct capabilities (MentraOS camera capture, secure frame transmission, preprocessing, registration/consent, LinkedIn parsing, directory construction, real-time identification, context display, similarity scoring).
- Clarified assumptions: no pre-parsed directory exists; event directories are built only from participant-provided headshots + LinkedIn profile uploads + explicit consent.
- Refined FR-2 verification criteria by specifying pass threshold (≥ 48/50 accounts enforce email verification and block uploads prior to explicit opt-in).
- Updated privacy enforcement language to reflect event-based access controls (event membership + consent + role) and controlled backend access patterns.
- Reworked deliverables to be stakeholder-deliverable artifacts (deployed MentraOS demo app, event registration portal, directory pipeline, backend deployment package, testing/validation report, compliance report, documentation package).
- Removed the draft Gantt chart from the Verification & Validation Plan and replaced it with a final Spring 2026 Gantt chart artifact.

Project Overview

We are creating Memento so that professionals and students meeting new people can know names and roles before the conversation begins, leading to more confident introductions, efficient discussions, and stronger connections.

Project Scope

In Scope:

- **MentraOS Camera Capture:** The system shall capture live image frames using the MentraOS camera API at a sufficient rate and resolution for face detection

and identification.

- **Secure Frame Transmission:** The system shall transmit captured frames from the smart glasses or companion application to the backend using secure network communication.
- **Frame Preprocessing:** The system shall preprocess frames (e.g., cropping, normalization, compression) prior to backend processing to reduce latency and improve recognition reliability.
- **Event Registration and Consent Workflow:** The system shall allow users to register for a specific event, upload a headshot image, submit a LinkedIn profile, and explicitly consent to facial recognition and profile usage within that event.
- **LinkedIn Profile Parsing and Structuring:** The system shall parse participant-uploaded LinkedIn profiles into structured fields such as name, role, organization, education, clubs, and projects, and store the results in the database.
- **Event-Specific Directory Construction:** The system shall construct an event-specific directory by indexing uploaded headshots into an AWS Rekognition collection and linking Rekognition Face IDs to user profile records.
- **Real-Time Face Identification:** The system shall identify registered participants in real time by comparing incoming frames against the event-specific Rekognition collection.
- **Profile Context Retrieval and Display:** Upon identification, the system shall retrieve and display non-invasive profile information including name, role, organization, or academic affiliation.
- **Similarity Scoring:** The system shall compute a similarity score between the user and the identified individual based on shared structured profile attributes.

Under Evaluation:

- **Post-Event Interaction Log:** A complementary mobile application that allows users to log in after an event to review who they met, including timestamps and names, creating a personal “networking history.”
- **Post-Event Interaction Review UI:** A complementary mobile or web view that lets users review recognized encounters after the event (names + timestamps).
- **Conversation Transcription / Note-Taking:** Optional transcription or note capture stored securely for personal recall.

Out of Scope:

- **Unrestricted Web Scraping or Background Retrieval:** The system will not search the internet for personal data or attempt to identify individuals solely by facial recognition without explicit consent and event registration.
- **Deep Profiling or Sensitive Information:** Information beyond professional or

academic context (such as personal life details, social media activity, or private data) will not be retrieved or displayed.

- **External Identity Matching:** The app will not attempt to match unidentified faces to public images or profiles outside the designated directory.

Assumptions:

- Each participant will upload their own LinkedIn profile and a clear headshot during event registration and explicitly consent to facial recognition within that event.
- LinkedIn profiles provided by participants contain sufficient information to extract relevant professional or academic attributes.
- Smart glasses hardware provides adequate image quality for face detection under typical event lighting conditions.
- Network connectivity is available during events; if connectivity degrades, the system will handle delays gracefully.
- No pre-parsed directory exists prior to registration. All event directories are constructed from participant-provided data.

Constraints:

- **Hardware Limitations:** Image quality and recognition accuracy will be limited by the smart glasses' camera specifications, which may have low megapixel sensors or restricted processing power.
- **Privacy and Ethical Restrictions:** The system must comply with institutional and legal privacy standards, ensuring no unauthorized data collection or storage.
- **Performance Requirements:** The facial recognition and context retrieval must operate in near real time to maintain usability, given the short attention window in live events.
- **Resource Constraints:** Development is limited by available team size, time, and access to machine learning APIs or facial recognition libraries.
- **Data Dependency:** System functionality depends on the completeness and accuracy of participant-provided headshots and LinkedIn profile data submitted during event registration.

Functional Requirements

FR-1: Real-Time Face Recognition Pipeline

Statement: The system shall capture live video from the Mentra smart glasses, stream it to the companion app, and perform face recognition through the backend using AWS Rekognition, identifying registered users with a minimum confidence threshold of 90%.

Rationale: Fast, accurate identification enables real-time social assistance and is the system's core function.

Test Method: Perform 100 face-recognition trials with registered participants; requirement is met if ≥95% of recognized users are correctly identified above 90% confidence and end-to-end latency meets p50 ≤ 1.5s and p95 ≤ 3s.

Supporting Context: "Real-time" = identification visible in the app within 1.5 s (p50) of frame capture. "Confidence threshold" = AWS Rekognition score cutoff.

Trace: Supports real-time user identification and system integration.

Priority: Must Have

FR-2: User Registration & Authentication

Statement: The system shall allow secure user signup and login through Supabase Auth, requiring each user to verify an email address and explicitly opt in before uploading profile and face data.

Rationale: Ensures that only consented and verified users participate in recognition.

Test Method: Create 50 test accounts. This requirement is met if at least 48 out of 50 accounts successfully enforce email verification and prevent profile or face data uploads prior to explicit opt-in consent.

Supporting Context: "Opt-in" = user explicitly grants consent to appear in the recognition database.

Trace: Supports secure user management and ethical data collection.

Priority: Must Have

FR-3: Privacy & Consent Enforcement

Statement: The system shall restrict recognition results to opted-in users and maintain Row-Level Security (RLS) and audit logs in Supabase to record every identification and data access event.

Rationale: Protects privacy and enables compliance with ethical and institutional policies.

Test Method: Attempt 20 unauthorized lookups on non-opted-in users; confirm zero matches returned and corresponding audit entries created.

Supporting Context: RLS policies restrict access based on event membership + consent + role but backend uses service role for controlled access, while user-facing queries are restricted.

Trace: Supports privacy management and system accountability.

Priority: Must Have

FR-4: Profile Context Card

Statement: The system shall display a user's key profile data (name, role, major/organization, and common interests) on the app within 1 second of identification.

Rationale: Immediate visual context enhances real-time networking usefulness.

Test Method: Measure 100 recognitions; 95 % of responses must render profile card ≤ 1 s after face match.

Supporting Context: Data pulled from Supabase profiles table; response latency measured from match receipt to UI render.

Trace: Supports real-time information delivery.

Priority: Must Have

FR-5: Backend Integration with AWS Rekognition and Supabase

Statement: The system shall store each user's Rekognition Face ID and link it to their Supabase profile ID to enable subsequent recognition and profile retrieval.

Rationale: Links AWS data with the application database for consistent identity management.

Test Method: Index 30 user faces; confirm Face IDs exist in collection and corresponding Supabase entries reference correct profile IDs.

Supporting Context: Face ID = unique identifier returned by Rekognition IndexFaces API.

Trace: Supports backend data integration and recognition accuracy.

Priority: Must Have

FR-6: Event-Based Privacy Filters

Statement: The system shall allow recognition only within designated, approved events and prevent cross-event identification by isolating Rekognition collections and Supabase records per event.

Rationale: Prevents unauthorized recognition outside consented contexts.

Test Method: Conduct 100 cross-event trials using two separate event collections. For each trial, submit a frame containing a participant from Event A to Event B's collection (and vice versa). Requirement is met if 0 true matches are returned and the false positive rate ≤ 1% across all trials.

Supporting Context: "Event" = a defined session such as a career fair; each event has its own collection ID.

Trace: Supports contextual privacy enforcement.

Priority: Must Have

FR-7: Extended Profile Layers (Similarity Score)

Statement: The system shall compute and display a similarity score (0–100) based on shared structured profile attributes, including organizations, education, clubs, projects, and interests (and mutual connections only if explicitly provided by the user).

Rationale: Helps users prioritize meaningful networking connections.

Test Method: Provide 20 known user pairs; computed scores should correlate ≥ 0.6 with manual similarity rankings.

Supporting Context: Similarity derived from overlap in structured profile fields (e.g., clubs, majors, projects).

Trace: Supports relationship insight and connection relevance.

Priority: Must Have

FR-8: Conversation Starter Generation

Statement: The system shall generate 3–5 short, neutral conversation starters using OpenAI API based on shared profile attributes (e.g., same major or organization).

Rationale: Improves networking engagement by reducing initial awkwardness.

Test Method: Feed 20 profile pairs; verify outputs ≤ 120 characters each, reference shared attribute, and contain no PII.

Supporting Context: “Shared attribute” = field common to both profiles (major, organization, interests).

Trace: Supports conversational assistance.

Priority: Should Have

FR-9: UI/UX Refinement

Statement: The system shall implement an accessible React frontend with consistent layout, color contrast, and responsive design for web viewports.

Rationale: Improves usability and accessibility for all users.

Test Method: Perform WCAG 2.1 AA audit; ≥ 95 % of pages pass contrast and navigation checks.

Supporting Context: WCAG AA = Web Content Accessibility Guidelines 2.1 Level AA compliance.

Trace: Supports accessibility and user experience.

Priority: Should Have

FR-10: Conversation Tracking

Statement: The system shall log each recognized interaction (event ID, user ID, matched ID, timestamp) in Supabase for later analytics and user review.

Rationale: Enables users and organizers to see networking activity and evaluate event impact.

Test Method: Simulate 30 recognitions; verify 30 corresponding log rows with correct IDs and timestamps.

Supporting Context: “Interaction” = a successful match during an event.

Trace: Supports analytics and user history.

Priority: Should Have

FR-11: Gamified Networking Metrics

Statement: The system shall calculate and display metrics such as “new connections made this week” and event badges based on conversation logs.

Rationale: Encourages continued use and engagement through positive feedback.

Test Method: Generate test data for 20 users; verify badge criteria trigger at configured thresholds (≥ 5 connections/week).

Supporting Context: Badges = visual rewards stored in the user profile record.

Trace: Supports engagement and retention.

Priority: Could Have

FR-12: Cloud Analytics Dashboard

Statement: The system shall provide a dashboard for event organizers displaying aggregate metrics such as number of encounters, unique connections, and average similarity score.

Rationale: Helps career services evaluate event effectiveness without exposing personal data.

Test Method: Seed 100 encounters across 10 events; verify dashboard aggregates match SQL ground truth within ± 1 %.

Supporting Context: Aggregation = summary of non-identifiable metrics for administrative

review.

Trace: Supports post-event analytics.

Priority: Could Have

Non-Functional Requirements

NFR-1: Performance (Latency)

Statement: The system shall display recognized profile information within 1.5 seconds (p50) and 3 seconds (p95) of face capture under normal load (≤ 20 concurrent users).

Rationale: Low latency is essential for natural interaction in live networking scenarios.

Test Method: Load test 20 simultaneous sessions; measure latency across 300 requests; verify p50 ≤ 1.5 s, p95 ≤ 3 s.

Supporting Context: “Normal load” = 20 active attendees at one event.

Trace: Supports real-time interaction and user experience.

Priority: Must Have

NFR-2: Security & Data Protection

Statement: The system shall encrypt all data in transit (TLS 1.2 or higher) and at rest (S3 SSE-KMS and Supabase encryption) and limit AWS permissions to least privilege.

Rationale: Protects user PII and biometric-adjacent data from breach or misuse.

Test Method: Security audit; verify TLS certificates, S3 bucket policies, and IAM roles grant minimal access.

Supporting Context: “Least privilege” = only resources required for specific function are permitted.

Trace: Supports system security and trustworthiness.

Priority: Must Have

NFR-3: Privacy (Data Retention & Consent)

Statement: The system shall purge event images and face records 30 days after event closure unless explicit retention approval is granted by organizers and users.

Rationale: Minimizes risk and complies with privacy best practices.

Test Method: Verify scheduled deletion jobs remove expired records and S3 objects ≥ 30 days old; random spot-check ensures no residual data.

Supporting Context: “Retention approval” = checkbox consent for long-term data use.

Trace: Supports ethical data handling and user trust.

Priority: Must Have

NFR-4: Accessibility (Voice Assistance)

Statement: The app shall offer optional voice-over mode to read aloud recognized user names and roles for visually impaired attendees.

Rationale: Promotes inclusivity and equal participation in networking events.

Test Method: Enable voice mode; perform 10 recognition tests; confirm speech outputs match displayed text ≥ 95 % accuracy.

Supporting Context: Uses Mentra Text-to-Speech SDK.

Trace: Supports accessibility and universal design.

Priority: Could Have

NFR-5: Reliability & Uptime

Statement: The system shall maintain ≥ 99.5 % uptime for the recognition API and frontend during active event hours.

Rationale: Event disruptions would undermine trust and demonstrations.

Test Method: Monitor API availability over 30-day test period; require ≥ 99.5 % availability excluding scheduled maintenance.

Supporting Context: “Uptime” = successful HTTP 200 responses to health checks every

minute.

Trace: Supports system stability and user confidence.

Priority: Should Have

Development Methodology

Our team will follow a Scrum-based development methodology adapted for an academic environment. We selected Scrum because it supports iterative development, frequent integration, and continuous validation across multiple subsystems including the MentraOS application, backend services, database, and user interface.

Work will be organized into weekly sprints with defined sprint goals, prioritized backlog items, and sprint reviews. Each sprint will include implementation, testing, and integration tasks to reduce risk and surface issues early. Acceptance criteria for backlog items are tied directly to functional and non-functional requirements, ensuring development progress aligns with verification and validation goals.

Deliverables

Deliverable 1: Deployed MentraOS Demonstration Application

- **Description:** An installable MentraOS application demonstrating real-time camera capture, facial recognition, and profile context display during a live event. Includes installation instructions and a recorded demo video.
- **Relevant Requirements:** FR-1 (Real-Time Face Recognition Pipeline), FR-4 (Profile Context Card), NFR-1 (Performance – Latency), NFR-5 (Reliability & Uptime)

Deliverable 2: Event Registration and Consent Portal

- **Description:** A standalone web-based portal allowing users to register for events, upload headshots, submit LinkedIn profiles, and explicitly consent to facial recognition and profile usage. Includes user-facing documentation describing consent and data handling.
- **Relevant Requirements:** FR-2 (User Registration & Authentication), FR-3 (Privacy & Consent Enforcement), NFR-2 (Security & Data Protection), NFR-3 (Privacy – Data Retention & Consent)

Deliverable 3: Event Directory Construction Pipeline

- **Description:** A documented pipeline for parsing LinkedIn profiles, indexing uploaded headshots into AWS Rekognition collections, and linking records in Supabase to create event-specific directories.

- **Relevant Requirements:** FR-5 (Backend Integration with AWS Rekognition and Supabase), FR-6 (Event-Based Privacy Filters), FR-7 (Extended Profile Layers – Similarity Score), NFR-2 (Security & Data Protection)

Deliverable 4: Backend API and Deployment Package

- **Description:** A deployed backend service exposing APIs for frame ingestion, recognition, profile retrieval, and event isolation. Includes API specifications and deployment instructions.
- **Relevant Requirements:** FR-1 (Real-Time Face Recognition Pipeline), FR-5 (Backend Integration), FR-6 (Event-Based Privacy Filters), NFR-2 (Security & Data Protection), NFR-5 (Reliability & Uptime)

Deliverable 5: Similarity Scoring and Context Generation Report

- **Description:** A technical report describing the similarity scoring approach, context generation logic, evaluation methodology, and example outputs.
- **Relevant Requirements:** FR-7 (Extended Profile Layers – Similarity Score), FR-8 (Conversation Starter Generation), NFR-1 (Performance – Latency)

Deliverable 6: Privacy, Security, and Compliance Report

- **Description:** A standalone report documenting consent mechanisms, access control policies, audit logging, data retention rules, and FERPA-aligned design decisions.
- **Relevant Requirements:** FR-3 (Privacy & Consent Enforcement), FR-6 (Event-Based Privacy Filters), NFR-2 (Security & Data Protection), NFR-3 (Privacy – Data Retention & Consent)

Deliverable 7: Post-Event Analytics Dashboard

- **Description:** A functional dashboard displaying anonymized aggregate networking metrics for event organizers, accompanied by administrator documentation.
- **Relevant Requirements:** FR-10 (Conversation Tracking), FR-11 (Gamified Networking Metrics), FR-12 (Cloud Analytics Dashboard), NFR-5 (Reliability & Uptime)

Deliverable 8: System Testing and Validation Report

- **Description:** A comprehensive report summarizing system testing results, including latency benchmarks, recognition accuracy, load testing, and privacy validation mapped to defined requirements.
- **Relevant Requirements:** FR-1 through FR-12 (Functional Coverage), NFR-1

through NFR-5 (Non-Functional Coverage)

Deliverable 9: Final System Documentation Package

- **Description:** A consolidated documentation package including architecture diagrams, developer onboarding guides, API references, deployment procedures, and end-user instructions.
- **Relevant Requirements:** FR-2 (User Registration & Authentication), FR-3 (Privacy & Consent Enforcement), FR-5 (Backend Integration), NFR-5 (Reliability & Uptime)

Verification and Validation Plan

The full Verification and Validation Plan is available as a PDF in the project GitHub documentation folder:

https://github.com/ailijevs/memento/blob/main/docs/Verification%20%26%20Validation%20-%20Team%205.pdf

The draft Gantt chart has been removed from the Verification and Validation Plan. The final project schedule is provided below.

Gantt Chart

The project Gantt chart for Spring 2026 is available at this link:

https://docs.google.com/spreadsheets/d/1OhSXQLeo4Q8HtHtceciCsrM4qdr8RMp9PEy_TYz5Rao/edit?usp=sharing

The schedule covers all 16 weeks of the semester, accounts for Spring Break, includes iterative testing and integration checkpoints, and assumes final system demonstrations during quiet week (April 27 – May 1).