

Memnora Identity

Biometric Access for Persistent AI Workspaces

Prepared for: TeraOpenScience - Idea, Innovation, Business: A Science Challenge

Project lead: Dwight R. Vaughn

Organization: Memnora Enterprizes Corp.

Entry tag: #IdealInnovationBusiness

Executive summary

AI-assisted work can span many sessions, documents, and devices. Users need convenient access to their own saved context and a clear way to control which memories the system may retain. This project proposes a research prototype connecting biometric access with a persistent AI workspace.

Research objective

Test whether biometric authentication can reduce access friction while a permission-controlled memory system preserves useful project context and prevents information from crossing between user accounts. Benefits will be evaluated rather than assumed.

Selected technology and proposed contribution

Selected platform listing: **Advanced Biometric Authentication using Facial Recognition and Artificial Intelligence**. The proposed application is access to persistent workspaces. The listing's detailed specification, availability, and licensing must be checked before integration; this proposal does not claim ownership of the selected technology.

Current status and scope

This document specifies a proposed extension of the Memnora concept. It does not establish that biometric functionality, security testing, or the combined prototype has already been implemented. The initial deliverable is a limited pilot demonstration with documented results.

01 / Prototype and data controls

Minimum viable prototype

Build an enrollment and sign-in flow, a private workspace for each account, user-approved memory records, project history, and a decision log. Users can inspect, correct, export, and delete retained information. Authentication alone must never authorize access to another account's records.

Proposed architecture

Layer	Responsibility
Access	Evaluate the selected facial-recognition approach against device-based biometric authentication. Bind successful verification to an account session.
Authorization	Check the authenticated account and explicit workspace permissions for every read and write.
Memory	Store approved context with its owner, source, creation time, revision history, and retention preference.
AI assistance	Retrieve only authorized context; separate stored evidence from generated interpretations.
Audit and control	Record access and memory changes without placing biometric secrets in logs. Support revocation, export, and deletion.

Biometric design decision

Device-based authentication is a comparator and possible implementation path; it is not equivalent to building a facial-recognition model. Where supported, it can verify a user through their device without sending face images to the workspace service. If the selected technology needs separate face enrollment, document its data flows and evaluate it with consenting adult volunteers in an isolated pilot.

Consent, recovery, and retention

Collect only information needed for the pilot. Explain enrollment, data uses, retention, and withdrawal before participation. Provide a non-biometric recovery method, session revocation, and access when biometric verification fails. Define backup expiry and deletion verification. Review actual deployment requirements before a public rollout.

Trynary workflow

Receive: accept authorized identity and context inputs. **Evaluate:** check permissions, evidence, and proposed changes. **Release:** provide an authorized result and a traceable record. This is a workflow structure whose practical effect will be tested.

02 / Research and evaluation

Pilot design

Recruit approximately 15-20 consenting adults for repeated sign-in and workspace tasks. Compare the prototype with a baseline sign-in flow and compare approved persistent memory with a session-only condition. Counterbalance task order where feasible. Use synthetic project records and report sample size, device mix, limitations, and unsuccessful trials.

Question	Measure and proposed pilot target
Can users sign in reliably?	Successful authorized sign-ins, rejection rate, and median completion time. Target: at least 95% success in defined supported conditions; compare time with baseline.
Can unauthorized access occur?	Run predefined cross-account requests and controlled impersonation/spoofing attempts. Target: zero cross-account disclosures in the test suite. Report attempts and all observed failures.
Does memory help continuity?	Score retrieval against a fixed answer key and measure repeated-task completion. Target: at least 90% correct approved-fact retrieval and improvement over session-only baseline.
Can users control records?	Verify edit, export, deletion, and session revocation through end-to-end scenarios. Target: every predefined control scenario passes.
Are failures understood?	Record recovery success and performance across tested devices, lighting conditions, and participant groups where consent and sample size permit.

Targets above are proposed acceptance criteria, not achieved results. A small pilot cannot establish population-level fairness, production security, or a reliable estimate of rare false acceptances. Report denominators and uncertainty; restrict conclusions to tested conditions.

Key open questions

Does the combined system provide enough value beyond separate authentication and memory tools? Can the selected technology be used under workable licensing terms? How much context should be retained? What happens after a lost device, failed verification, revoked consent, or conflicting memory update?

Expected evidence package

Deliver a working demo, architecture and data-flow documentation, reproducible test cases, anonymized aggregate findings, a failure register, and a short report comparing results with the baseline. Publish no volunteer biometric data or private workspace contents.

03 / Delivery and commercial plan

Five-month execution plan

Proposed build: November 16, 2026 through April 18, 2027, followed by final defense during April 19-23. Delivery targets follow the challenge reporting checkpoints.

Period	Milestone and evidence
Nov 16-Dec 15	Confirm technology permissions and dependencies; finalize scope, baseline tasks, architecture, data map, and participant protocol.
Dec 16-Jan 15	Implement account sessions, authorization, biometric access proof of concept, and basic memory. Prepare first report for the week of January 18.
Jan 16-Feb 15	Complete user controls, audit records, recovery, and test harness; conduct internal access and isolation testing.
Feb 16-Mar 15	Run pilot and customer interviews; compare baseline tasks and document failures. Submit second report in the week of March 15.
Mar 16-Apr 18	Fix priority failures, repeat affected tests, finish proof of concept, results report, market research, and full business plan.
Apr 19-23	Present final defense and demonstration; disclose limitations and remaining work.

Illustrative cash budget

Item	Estimate
Development and integration assistance	\$2,500
Independent security and authentication review	\$1,250
Hosting, storage, and AI API usage	\$900
Participant incentives (20 people at \$30)	\$600
Test devices and accessibility checks	\$500
Contingency	\$750
Total proposed cash requirement	\$6,500

Planning estimates only; no vendor quotes or grant award are represented. Assumes the lead contributes development time in kind, existing hardware is reused, and no expensive biometric license is required. Revise after technology review. This is not a statement of the contest's funding entitlement.

04 / Team, dependencies, and business

Team and commercial validation

Proposed lead: Dwight R. Vaughn, responsible for product scope and software integration. Additional roles to recruit or contract: authentication/security reviewer and pilot coordinator. No external participation is confirmed. Interview 10-15 prospective users, test individual subscriptions and small-team licensing concepts, and compare willingness to pay with hosting and support costs.

Initial markets: personal productivity, writing workspaces, small-business knowledge management, and research collaboration. Advance to a broader release only after reviewing pilot findings, unresolved access failures, costs, and technology permissions.

Project lead - short professional resume

Dwight R. Vaughn - independent software developer, Memnora creator, and project lead. Experience includes HTML, CSS, JavaScript, Python, Solidity, Node.js, TypeScript, React, Vite, Express, PostgreSQL, and Drizzle. Python certificate completed in July 2023. Prior work includes development of Memnora concepts and web applications, with experience translating product ideas into interfaces and application workflows. Profile information is supplied by the project lead; no biometric specialization or independent security certification is claimed.

Lead responsibilities: requirements, software integration, memory workflows, evaluation coordination, reporting, and business planning. Specialist biometric/security review will be contracted if funding permits. The project is planned as a solo entry; no other team members or reviewers are confirmed.

Supply-chain and dependency roadmap

Dependency	Procurement and fallback plan
Selected technology	First obtain its specification, license, integration requirements, and cost. If access is unavailable, seek organizer guidance on an eligible alternative before changing the project foundation.
Software and AI	Inventory libraries and licenses; select an AI service and database after cost and data-use review. Keep exportable records and an adapter layer to reduce vendor dependence.
Hardware and hosting	Reuse existing laptop/phone for initial work. Verify biometric capability and browser support; use budgeted test devices only where needed. Set hosting/API usage caps.
Specialist support	Seek a scoped security-review quote before committing expenditure. If budget is insufficient, narrow the pilot and document review limits.

05 / Commitments and completion

Institution policies and project commitments

This proposal is submitted as an independent project and does not represent university sponsorship or approval. The project lead commits to following all university or institution policies applicable to any affiliation, facilities, funding, or resources used. Before introducing such resources or collaborators, the lead will identify relevant IP, ethics, data, and research-approval requirements and obtain any required permissions. No institutional clearance is claimed by this proposal.

Business-plan outline and Phase 2 outputs

The Phase 2 business plan will cover customer need, competitors and differentiation, customer interviews, pricing experiments, operating costs, distribution and support, technology permissions, risks, and financing. It will include a 10-year financial projection and net present value calculation with explicit assumptions and sensitivity analysis. These are future deliverables; the present cash budget is a pilot estimate, not a revenue forecast.

Required completion package: executive summary; market research summary; execution evidence; field test or documented proof of concept; full business plan with financial projections and NPV; two progress reports; final defense. Scale claims and launch decisions will follow the results.

Entry administration: the project must carry the required #IdealInnovationBusiness tag. Its appearance inside this PDF or the project description does not establish that platform tagging or contest registration is complete. Obtain organizer confirmation if the tag cannot be added.