



For: [REVIEWING TEAM] at [ORGANIZATION] (information security, privacy, architecture)

Prepared by: [PROJECT MANAGER NAME], requesting approval to use SPERT® Scheduler

Reviewed against: SPERT® Scheduler v0.79.26 (source commit 86b3e49); shared Connect AI server code in the [spert-landing](#) repository v2.7.2 (commit 52b7fbf, 2026-10-25; server version 1.14.1, confirmed live 2026-10-25); [AI Privacy Notice](#) v2.3 (effective 2026-10-26); [AI Connectivity Consent Notice](#) v2.2 (effective 2026-10-26); [Privacy Policy](#) v1.4 (effective 2026-10-26). **Review date:** 2026-10-25.

This document supports an approval process. It is not legal, compliance or security advice, and it makes no commitments beyond those in the published legal documents.

THE SHORT VERSION

SPERT® Scheduler stores project data only in the browser by default. Connect AI is an optional feature, off unless a user turns it on, that lets the user's own AI chatbot (for example [AI PLATFORM]) build and edit a schedule. It has two permissions:

- **Write Mode** (required to connect). The AI can send edits into the project. Your existing project data is not uploaded.
- **Read Mode** (optional, off by default). A copy of the open project, including its free-text fields, is uploaded to a relay in Google Cloud (US) and is then passed to whichever AI provider the user chose. **This happens even when the app is set to local-only storage.**

[ORGANIZATION] can approve SPERT® Scheduler in local-only mode without approving Connect AI, and can approve Write Mode without approving Read Mode.

HOW THE DATA FLOWS

1. **Browser to relay.** When Read Mode is on, the browser writes a snapshot of the open project to Google Firestore (multi-region nam5, United States), in a session record under `anonymous_sessions/`. The snapshot is refreshed about two seconds after each edit while Read Mode stays on.
2. **AI provider to Connect AI server.** The user adds the SPERT® Suite connector to their chatbot: the Connect AI server, `https://mcp.spertsuite.com`, a Model Context Protocol server that runs as a Google Cloud Function (second generation, running on Cloud Run) in `us-central1`. The [AI Privacy Notice](#) (§5) calls the same service "Google Cloud Functions in us-central1". The user pairs the chatbot with a one-time code shown in the app: one word plus 10 digits, valid for 15 minutes and closed about a minute after the AI first uses it. The chatbot's servers call this connector. The browser never talks to the AI provider or to the Connect AI server directly.
3. **Relay to AI provider.** When the AI asks to read the project, the server reads the snapshot and returns it to the AI provider. The server refuses to read anything if Read Mode is off. From that point the AI provider's own terms govern retention and use.
4. **AI edits back to the browser.** In Write Mode, the AI's edits travel the reverse path through the same relay. Only the Connect AI server can write them (Firestore rules block browsers from doing so), and the browser checks each edit against bounds before applying it.

Anything the user types into the chatbot itself goes to the AI provider whatever the SPERT® settings are.

WHAT A READ MODE SNAPSHOT CONTAINS

A session is bound to the project it was opened for (since v0.79.19). If the user switches to a different project, edits meant for the first project are not applied to it; the session starts fresh for the new project.

Included (that one project only)	Excluded
Project name and id; every scenario in the project	Other projects
Activity names, three-point estimates, status, computed dates and critical-path flags	Owner id, members and sharing settings
Milestones and dependencies	Email addresses and names of the user
Free text: activity notes, descriptions, checklist and deliverable items	Calendar and holiday data

If a project's snapshot would exceed about 700 KB, the app drops the free text first. Smaller projects send it in full.

HOW LONG IT IS KEPT

Per the [AI Privacy Notice](#) (§2.2, §4): the snapshot is deleted from the live relay when the user turns Read Mode off, disconnects or signs out, or when the session expires seven days after the session's last activity, including requests from the AI assistant (deletion "typically completes within 24 hours"). Copies "may remain in the Operator's database backups until they expire: up to 98 days for daily backups and up to 7 days for point-in-time recovery data." Session records use a random identifier and are not linked to a name or email unless the user is signed in to a cloud account. Google Cloud operational logs (request metadata such as IP address, timestamp and URL) are kept 30 days, in a location that is not restricted to one region ([Privacy Policy](#) §2.3). The operator states it does not train models on user data. **What the AI provider keeps is outside SPERT®'s control.**

WHAT THE AI CAN CHANGE (WRITE MODE)

The Connect AI server offers SPERT® Scheduler 25 tools. They can create activities, milestones and dependencies; rename activities; change estimates; replace an activity description; append notes; add and tick checklist and deliverable items; reorder activities; and assign milestones. **Overwrite capabilities:** rename, estimate updates, description replacement, milestone updates, dependency updates and reorder. **Delete capability:** removing a dependency. No tool deletes an activity, milestone, scenario or project. Dependency changes require Read Mode. The server refuses out-of-range estimates (infinite, or longer than 3,650 days), and the browser checks every edit again before applying it.

WHAT A PROJECT MANAGER CAN DO TO LIMIT EXPOSURE

1. **Don't use Connect AI.** Local-only use sends no project data anywhere.
2. **Connect with Write Mode only.** The AI can build a schedule from what you tell it but cannot read your existing project.
3. **Use only an AI provider and account type [ORGANIZATION] has approved,** such as [AI PLATFORM] under an organizational agreement. Consumer accounts often have different retention and training terms.
4. **Keep sensitive content out of the project before turning Read Mode on,** or work in a separate project holding only what you are comfortable sharing. Notes and descriptions are the usual place sensitive detail ends up.
5. **Turn Read Mode off or disconnect when finished, while online.** If the server can be reached, this deletes the live snapshot immediately (backups still expire on their own schedule). If Disconnect cannot reach the server, the app does not say so, and the relay data stays until the session expires.

6. **Never store regulated data** (PHI, third-party personal data, payment data). The [Terms of Service](#) already forbid it.

REVIEWER NOTES

- **"Local-only" has an exception.** Read Mode uploads the open project regardless of the storage setting. The consent dialog for SPERT® Scheduler names the project and lists every field Read Mode shares, including the free-text fields, but does not itself say the upload happens in local mode; the [AI Privacy Notice](#) it links to does.
- **Shared computers.** Signing out ends any Connect AI session, in the browser since v0.79.11 and on the server since v0.79.25, including when a different person signs in on the same browser, so the next person cannot inherit a live AI connection. If the server cannot be reached at sign-out, for example when offline, the app tells the user and keeps retrying; until a retry succeeds, the relay session stays live. Sessions have no fixed end: each AI request extends one, so expiry alone is not a safeguard on a shared computer.
- **There is no administrator switch.** [ORGANIZATION] cannot centrally disable Connect AI or Read Mode inside SPERT® Scheduler. Controls available today are policy (for example, an acceptable-use rule) and the AI platform: if [AI PLATFORM] lets administrators restrict custom connectors, blocking `mcp.spertsuite.com` there prevents pairing. Blocking the Connect AI server (`mcp.spertsuite.com`) on [ORGANIZATION]'s network does not work, because the AI provider's servers call it, not the user's device. Starting Connect AI does need the user's browser to call SPERT® Suite's pairing function at `us-central1-spert-suite.cloudfunctions.net/generatePairingCode`, so blocking that path, or that whole host (which also stops sharing invitations), may stop Connect AI from starting. This is untested, so [ORGANIZATION]'s IT team should test any block it relies on.
- **No independent audit.** There is no SOC 2, ISO 27001 or third-party penetration test. The code is open source (GPL-3.0). A self-audit of this feature is published in the app's `SECURITY.md` (v0.57.4, findings A1–A7, C1–C2). A second self-audit, of v0.79.8 on 2026-10-24, found weaknesses in pairing-code strength, sign-out and session handling; the fixes shipped the same and following day (longer single-use pairing codes, sign-out teardown, sessions bound to one project, consent and estimate checks; see the SPERT® Scheduler and [spertsuite.com](#) changelogs for v0.79.11 to v0.79.19 and v2.6.3 to v2.6.5). Three server-side items remain open: stronger protection of session identifiers, abuse limits on unauthenticated relay writes, and a hard limit on session lifetime (each AI request extends a session, so one that an AI keeps using does not expire). A suite-wide self-review was completed on 2026-10-25; its fixes are being released in stages. Self-reviews are not independent assessments. Hosting runs on Google Cloud, whose own certifications cover the infrastructure but not the application.
- **Reporting a vulnerability.** Email security@spertsuite.com, or use GitHub private vulnerability reporting on each public SPERT® repository. The Security page (<https://spertsuite.com/security>) says the operator aims to acknowledge reports within 3 business days, and publishes a short advisory after fixing an issue that could have affected users' data. Machine-readable contacts are at <https://spertsuite.com/.well-known/security.txt> and <https://scheduler.spertsuite.com/.well-known/security.txt>.
- **Single operator, best effort.** famousdavis, LLC operates the service with no SLA. Questions or a data-flow summary for IT review can be requested at contact@spertsuite.com ([AI Privacy Notice](#) §7 offers the summary). The web apps are checked for uptime every 5 minutes, but the Connect AI server is checked only about every six hours, and not at its public address, so a Connect AI outage may take longer to notice.
- **Not verified for this document:** the full logging behavior of the Connect AI server (the code reviewed logs session ids, not project content, but deployed configuration was not inspected); the deployed region of the server beyond the code (`us-central1`) and the [AI Privacy Notice](#); and any AI provider's handling of the data. Verified live on 2026-10-25: `mcp.spertsuite.com` resolves to Google's Cloud Run domain-mapping front end and reports server version 1.14.1, the version in the reviewed code.