



Fill-in template: short, sourced answers to the questions each reviewer asks · spertsuite.com/approval-kit

SPERT® Suite Approval Kit v1.0.0 (Release) · Content reviewed 2026-10-25 · Built 2026-10-26

For: [REVIEWING TEAM] at [ORGANIZATION] · **Prepared by:** [PROJECT MANAGER NAME] · **Request reference:** [REQUEST ID]

Reviewed against: SPERT® Scheduler 0.79.26, SPERT® Story Map 0.53.14, SPERT® Forecaster 0.47.4, SPERT® CFD 0.15.23, GanttApp™ 0.29.8, MyScrumBudget™ 0.44.4; [spert-landing](#) 2.7.2 (Connect AI server 1.14.1); [Terms of Service](#) v1.4 and [Privacy Policy](#) v1.4 (effective 2026-10-26); [AI Privacy Notice](#) v2.3 (effective 2026-10-26); [AI Connectivity Consent Notice](#) v2.2 (effective 2026-10-26). **Review date:** 2026-10-25.

This FAQ supports an approval process. It is not legal, compliance or security advice, and it makes no commitments on the operator's behalf beyond those in the published legal documents.

For the project manager. Delete questions about tiers you are not requesting, and add the questions your reviewers actually ask at the end. Keep the answers' sources: reviewers use them. Delete this box before you send it.

GENERAL

What are we being asked to approve?

[APPS REQUESTED], used by [NUMBER] people in [TEAM] for [PILOT LENGTH], in tier [TIERS REQUESTED]. Tier 1 is local-only use; tier 2 is cloud storage and sharing; tier 3 is Connect AI, which can be approved with or without tier 2. Each can be approved or declined separately.

What is SPERT® Suite?

Six free, browser-based planning apps: SPERT® Scheduler, SPERT® Story Map, SPERT® Forecaster, SPERT® CFD, GanttApp™ and MyScrumBudget™. Each runs in the user's browser and, by default, saves projects in that browser's own storage. SPERT® Scheduler and SPERT® Forecaster use the Statistical PERT® estimation technique.

Who provides it?

famousdavis, LLC, a Florida limited liability company, operating since 2026-09-12 ([ToS](#) §1.1). It is a single-operator business. The software copyright is held by William W. Davis and licensed to the operator ([ToS](#) §3).

Does it replace [EXISTING TOOL]?

No. It is proposed as a complement for [THE SPECIFIC PLANNING QUESTION]. [EXISTING TOOL] remains the system of record. See the *Value Brief*.

What does it cost?

Nothing to license: "Core application functionality is provided at no charge" ([ToS](#) §2). No paid tier exists today. The real costs are review effort and learning time.

INFORMATION SECURITY

Is anything installed?

No. The apps are web pages. There is no agent, plug-in or desktop software.

Where does our data go in tier 1?

Nowhere. "Core App functionality that does not use Cloud Storage keeps your project data entirely within your local browser; the Apps do not send project data to the Operator or any third party" ([Privacy](#) §1). The web host,

Vercel, receives standard request data such as IP address and browser type. SPERT® Scheduler's Calendar page requests a public holiday service's country list when opened, and sends a country code and year when the user loads holidays ([Privacy](#) §1).

How do users sign in for tier 2?

With Google or Microsoft only, including Microsoft Entra ID work accounts ([Privacy](#) §2.1). There are no SPERT® passwords. [ORGANIZATION]'s MFA and conditional access apply to work accounts. There is no SSO enforcement, SCIM or admin console. The SPERT® Suite sign-in app is not yet a Microsoft "verified publisher": where Entra ID lets users consent only to verified publishers' apps, staff see "Need admin approval" and an administrator must grant consent first (operator's statement, 2026-10-25).

Can we stop staff turning on cloud storage or Connect AI?

Not inside the apps: there is no administrator switch, so approving tier 1 only is a policy decision. Technical options exist, but all are untested: blocking `spert-suite.firebaseio.com` may stop cloud sign-in, and blocking the pairing function may stop Connect AI (see "Can we turn Connect AI off for everyone?" below). [ORGANIZATION]'s IT team should test any block it relies on.

How is cloud data protected?

HTTPS in transit; Google Cloud's infrastructure controls at rest ([Privacy](#) §5); Firestore security rules that limit each project to its members by role, kept in source control, deployed automatically and checked for drift every six hours. No customer-managed keys.

Has it been independently audited or penetration tested?

No. There is no SOC 2, ISO 27001 or third-party penetration test, and the operator has not completed a formal questionnaire. Security reviews are the developer's own. The source code is public, so [REVIEWING TEAM] can review it.

Can we scan or test the live apps?

Not without raising it first. The [Terms of Service](#) (§4) forbid attempting "to probe, scan, test, or circumvent the security or authentication measures of the Apps". Review the public source, run a separate copy, or ask the operator in writing.

How are vulnerabilities reported and fixed?

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>. Dependabot alerts, CodeQL code scanning and secret scanning are on for every public repository (since 2026-10-25).

Is there an audit log?

No, not for users or administrators. Google Cloud keeps operational request logs for 30 days, for the operator's use only ([Privacy](#) §2.3).

PRIVACY

What personal data is collected?

Tier 1: none by the operator ([Privacy](#) §2.4). Tier 2: name, email and profile-photo link from the sign-in provider, a record of the Terms accepted (with the sign-in provider and first app used), technical data such as IP address, and invitee emails when projects are shared ([Privacy](#) §2.1, §2.3, §2.6).

Where is it stored?

In the United States: "Google Cloud Firestore multi-region nam5" ([Privacy](#) §9). Operational logs are not restricted to one region (§2.3). There is no regional choice.

How is it deleted?

On request to the operator, "not to exceed thirty (30) days under normal circumstances"; backup copies expire within 98 days ([Privacy](#) §6). There is no self-service delete-account control. Local data is deleted by the user.

Will the operator sign a data processing agreement?

None is offered. Under the [Privacy Policy](#) the operator is the data controller (§7.6). Tier 1 involves no personal data on the operator's side.

Who else receives data?

Google (Firebase and Google Cloud), Vercel and Resend, as named in [Privacy Policy](#) §4, and Microsoft for email sent to [spertsuite.com](#) addresses (§2.7, §4.6); the user's own AI provider for Connect AI (§4.5); and, for SPERT® Scheduler's holiday lookup only, a public holiday service, Nager.Date, that receives a country code and year ([Privacy](#) §1). The *Information Security Profile* lists them.

CONNECT AI (TIER 3 ONLY)

Does it use AI?

Not by default, and none of the apps has AI built in. Connect AI lets a user connect their own AI assistant, such as [\[AI PLATFORM\]](#), to one open project. It is opt-in each session, and only SPERT® Scheduler, SPERT® Story Map and SPERT® Forecaster offer it.

What does the AI provider receive?

Everything the user types into the AI chat, as with any AI use. In Write Mode, the user's existing project is not uploaded ([AI Privacy Notice](#) §2.1). In Read Mode, a snapshot of the one open project, including free-text notes and descriptions, goes to the relay and on to the AI provider, even in local-only mode (§2.2). The *Data Flow Diagram* lists the fields for each app.

Can the AI delete our work?

No tool deletes an activity, milestone, story-map item or project. Some tools overwrite names, estimates and descriptions, and some remove links or allocations. SPERT® Forecaster's connection is read-only. The *Data Flow Diagram* appendix lists every tool.

Can we turn Connect AI off for everyone?

Not inside the apps: consent is per user, per app and per browser ([AI Privacy Notice](#) §1). Controls that work: an acceptable-use rule, and [\[AI PLATFORM\]](#)'s own controls over which connectors users may add. 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.

Is our data used to train AI models?

"The Operator does not use your data to train machine learning models" ([Privacy](#) §3). The AI provider's terms govern what it does; they vary by account type ([AI Privacy Notice](#) §3).

LEGAL AND PROCUREMENT

Is there a contract?

Only the standard online [Terms of Service](#), [Privacy Policy](#) and, for Connect AI, the [AI Privacy Notice](#) and [AI Connectivity Consent Notice](#). There is no negotiated agreement.

What should legal look at first?

The authority representation for people acting for an employer ([ToS](#) §5.5, §5A.4); the as-is disclaimer and the right to discontinue without notice (§2, §8); the liability cap of the greater of \$25 or fees paid in 12 months (§9); the user's indemnity (§10); and Florida law, Florida courts and the class action waiver (§17).

Will our users have to accept new terms?

Users who accepted the Terms before October 26, 2026 are asked to accept the updated [Terms of Service](#) and [Privacy Policy](#); a user who is already signed in is signed out once and asked when they sign in again.

Is there an SLA or support?

No. The service is "provided on a best-effort basis" ([ToS](#) §2).

What if the operator stops?

Local-only data stays in the user's browser and can be exported at any time. The GPL licence permits [ORGANIZATION] to run its own copy, under a different name ([ToS](#) §3, §7).

OPERATIONS

What happens on a shared computer?

Local projects belong to the browser profile, so anyone using that profile can see them. Use assigned devices or one browser profile per person.

How will we know if the facts change?

The operator posts updated legal documents with a new version and effective date ([ToS](#) §16; [Privacy](#) §11), and has said it will give notice before changing where cloud data is stored ([Privacy](#) §9). Re-review triggers are recorded in the *Approval Pathway Checklist*.

HOW DO WE CONTACT THE OPERATOR?

Contacting the operator. Security reports and suspected account misuse: security@spertsuite.com, or GitHub private vulnerability reporting on any public SPERT[®] repository. Privacy questions, and requests to access, correct or delete data: privacy@spertsuite.com. Everything else, including the data-flow summary for IT review that the [AI Privacy Notice](#) (§7) offers: contact@spertsuite.com. The security policy is at <https://spertsuite.com/security>. The legal documents give the same addresses.

QUESTIONS ADDED BY THE ORGANIZATION

[QUESTION]

[ANSWER AND SOURCE]

REVIEWER NOTES

- **"Open source with no vendor review."** Every answer here cites the public source or a published legal document, so it can be checked; none is backed by an independent audit.
- **"Data leaving the environment."** Only in tiers 2 and 3, each a separate decision.
- **"Audit and logging."** There is no customer-visible log; size the data classification accordingly.
- **"Unfamiliar vendor."** A single operator with no contract; the pilot is small, time-boxed and exportable for that reason.