



Two-page overview for reviewers: what SPERT® Suite is, the three tiers, key facts and gaps, and where to read more · spertsuite.com/approval-kit

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

Two pages for anyone asked to review SPERT® Suite for use at [ORGANIZATION]. Every fact here is sourced in the longer kit documents named below. This summary supports an approval process; it is not legal, compliance or security advice.

WHAT IT IS

SPERT® Suite is six free planning apps that run in a web browser: SPERT® Scheduler, SPERT® Story Map, SPERT® Forecaster, SPERT® CFD, GanttApp™ and MyScrumBudget™. They help teams plan, schedule, forecast and budget projects with uncertainty taken into account; several use the Statistical PERT® technique. Nothing is installed, and planning calculations run on the user's device. The source code is public on GitHub under the GPL-3.0 licence. The operator is famousdavis, LLC, a Florida company run by one person. "Core application functionality is provided at no charge" ([ToS](#) §2), on best effort, with no SLA.

THREE TIERS, APPROVED SEPARATELY

Tier	What it involves	What leaves the user's device
1. Local-only (the default)	No account. Projects are saved in the browser	Page requests to the web host. SPERT® Scheduler's holiday lookup sends a country code and year (Privacy §1). No project data.
2. Cloud storage (opt-in)	Sign-in with Google or Microsoft; projects saved to Google Cloud and optionally shared	Name, email, saved projects, Terms acceptance record, technical data
3. Connect AI (opt-in, three apps)	The user connects their own AI assistant to one open project. No account needed; works with local or cloud storage	AI edits pass through the operator's relay in Google Cloud. With Read Mode on, a copy of the open project is held in that relay and passed to the AI provider

The numbers are labels, not a ladder: tiers 2 and 3 are separate decisions. Most organizations start with tier 1 only. Approving a tier is a policy decision: the apps have no administrator switch, so the *Approval Guide* (section 2) lists technical controls, all untested.

TOP FACTS

- **Local-only by default.** "The Apps do not send project data to the Operator or any third party" when cloud storage is off ([Privacy](#) §1).
- **Cloud data stays in the United States**, in Google Cloud Firestore multi-region nam5 ([Privacy](#) §9). Access is limited by database security rules to project members, by role.
- **Sign-in uses Google or Microsoft only**, including Entra ID work accounts, so [ORGANIZATION]'s own MFA and conditional access apply. No passwords are stored.
- **No analytics, advertising or tracking cookies** ([Privacy](#) §3), and "The Operator does not use your data to train machine learning models" ([Privacy](#) §3).
- **Connect AI is off until a user turns it on**, per app and per browser. In Write Mode, existing project data is not uploaded ([AI Privacy Notice](#) §2.1). No AI tool can delete an activity, story-map item or project.

- **Security practice:** public source, Dependabot and CodeQL scanning on all public repositories, and a suite-wide self-review completed on 2026-10-25.

MAIN GAPS

- No SOC 2, ISO 27001 or third-party penetration test. The [Terms of Service](#) (§4) forbid probing, scanning or testing the live apps, so raise any test with the operator first.
- No data processing agreement: the operator is the data controller, not a processor for [ORGANIZATION] ([Privacy](#) §7.6).
- No SLA, support contract or continuity commitment; the service can change or stop without notice ([ToS](#) §2).
- No single sign-on enforcement, user provisioning, administrator console or audit log.
- No choice of data region, and deletion is by request rather than self-service.
- Microsoft sign-in may need an Entra ID administrator to grant consent first, because the sign-in app is not yet a verified publisher.

WHERE TO FIND EACH DOCUMENT

If you are	Read
Information security	<i>Information Security Profile, Security Questionnaire Answer Sheet (SPERT® Scheduler), Architecture Overview</i>
Privacy	<i>Information Security Profile, Data Flow Diagram, Privacy Policy</i>
Enterprise architecture	<i>Architecture Overview, Data Flow Diagram, Value Brief</i>
AI governance (tier 3)	<i>Connect AI Data Explainer, Data Flow Diagram, AI Privacy Notice, AI Connectivity Consent Notice</i>
Legal or procurement	<i>Terms of Service, Privacy Policy, Reviewer FAQ</i>
The project manager	<i>Approval Guide and Approval Pathway Checklist</i>

The current kit is at spertsuite.com/approval-kit.

CONTACTING THE OPERATOR

Security reports: security@spertsuite.com, or GitHub private vulnerability reporting on any public SPERT® repository; the security policy is at <https://spertsuite.com/security>. Privacy questions and data requests: privacy@spertsuite.com. Everything else: contact@spertsuite.com.