



Fill-in template: controls, gaps, approval scope and attestation, for information security and privacy reviewers · spertsuite.com/approval-kit

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

Prepared by: [PROJECT MANAGER NAME] for [REVIEWING TEAM] · **Request reference:** [REQUEST ID] · **Date:** [DATE]

Item	Value
Apps requested	[APPS REQUESTED]
Tiers requested	[TIERS REQUESTED]
Users and duration	[NUMBER] users in [TEAM], for [PILOT LENGTH]
Highest data classification proposed	[DATA CLASSIFICATION]
Versions reviewed	SPERT® Scheduler 0.79.26 (86b3e49), SPERT® Story Map 0.53.14 (5e613c4), SPERT® Forecaster 0.47.4 (ff7ac3b), SPERT® CFD 0.15.23 (c7f9c68), GanttApp™ 0.29.8 (64d1647), MyScrumBudget™ 0.44.4 (0825168); shared backend spert-landing 2.7.2 (52b7fbf), Connect AI server 1.14.1
Legal documents relied on	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)
Kit review date	2026-10-25
Operator	famousdavis, LLC, a Florida limited liability company (ToS §1)

This profile is prepared by [ORGANIZATION]'s requester, not issued by the operator. It 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.

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.

For the project manager. The middle column of each table states what SPERT® Suite does today, with its source; leave it as it is. Fill in the right-hand column with [ORGANIZATION]'s requirement, or leave it for [REVIEWING TEAM] to complete. Delete rows for tiers you are not requesting. For SPERT® Scheduler, the *Security Questionnaire Answer Sheet* gives longer answers with code references. Delete this box before you send the profile.

1. APPROVAL SCOPE

SPERT® Suite can be approved in separate tiers. Each has its own data flows and risks, so [REVIEWING TEAM] can approve tier 1 without the others. The numbers are labels, not a ladder: tiers 2 and 3 are separate decisions.

Tier	What it involves	What leaves the user's device	Requested?
1. Local-only use (default)	The app runs in the browser and saves projects in browser storage. No account	Page requests to Vercel (IP address, browser type). SPERT® Scheduler's Calendar page requests Nager.Date's country list when opened, and a country's holidays for a chosen year when loaded (Privacy §1). No project data	[YES / NO]
2. Cloud storage and sharing	Sign-in with Google or Microsoft; projects saved to Google Cloud and optionally shared	Name, email, saved projects, Terms acceptance record, technical data	[YES / NO]
3. Connect AI (three apps only)	The user connects their own AI assistant to one open project	AI edits pass through a relay in Google Cloud. With Read Mode on, a copy of the open project goes to the relay and on to the AI provider, even in local-only mode	[YES / NO]. Read Mode: [YES / NO]

Scope note for tier 2. The most recent security hardening (2026-10-24 and 25) was applied first to SPERT® Scheduler and the shared backend. A suite-wide self-review was completed on 2026-10-25; its fixes are being released in stages. If tier 2 is requested for an app other than SPERT® Scheduler, ask the operator (contact@spertsuite.com) for its status before approval.

Approval versus enforcement. Approving tier 1 only is a policy decision. SPERT® Suite has no administrator switch, so staff could still turn on cloud storage or Connect AI. The technical options below are all **untested**; [ORGANIZATION]'s IT team should test any block it relies on.

Control	What it would stop	Tested by IT?
Block <code>spert-suite.firebaseio.com</code> , the operator's Firebase sign-in handler	Cloud sign-in (tier 2)	Not tested by the operator. [RESULT]
Block the pairing function, <code>generatePairingCode</code> on <code>us-central1-spert-suite.cloudfunctions.net</code> , or that whole host (which also stops sharing invitations)	Starting Connect AI (tier 3)	Not tested by the operator. [RESULT]
[AI PLATFORM]'s own controls over which custom connectors users may add	Connect AI (tier 3); the most effective option where available	[RESULT]

2. PRODUCT AND OPERATOR

Topic	SPERT® Suite today (source)	Requirement and finding
What it is	Six browser-based planning apps. Each is a single-page web application; planning calculations run on the user's device. No app repository contains a server-side API route (<i>Architecture Overview</i> §1)	[REQUIREMENT / FINDING]
Who runs it	famousdavis, LLC (Florida) since 2026-09-12, a single-operator business; software copyright held by William W. Davis and licensed to the operator (ToS §1.1, §3)	[REQUIREMENT / FINDING]
Source code	Public on GitHub under GPL-3.0 with additional terms (attribution, trademarks reserved, modified versions renamed) (ToS §3)	[REQUIREMENT / FINDING]

Topic	SPERT® Suite today (source)	Requirement and finding
Cost and contract	"Core application functionality is provided at no charge" (ToS §2). Standard online Terms; no negotiated contract	[REQUIREMENT / FINDING]
Service level	Best effort; "may be modified, suspended, or discontinued at any time without notice" (ToS §2). No SLA	[REQUIREMENT / FINDING]

3. DATA HANDLED

Topic	SPERT® Suite today (source)	Requirement and finding
Tier 1	"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)	[REQUIREMENT / FINDING]
Tier 2 personal data	Name, email and profile-photo link from the Google or Microsoft account, with the time the profile was last updated; record of the Terms version accepted, the sign-in provider and the first app used; IP address, browser and timestamps collected by Firebase, which keeps logged IP addresses for a few weeks (Privacy §2.1, §2.3). Sharing stores invitee and inviter emails (§2.6)	[REQUIREMENT / FINDING]
Tier 2 business data	The projects a user saves: planning data such as estimates, task names, sprint parameters and schedule structure, including any free text the user enters (Privacy §2.2)	[REQUIREMENT / FINDING]
Prohibited data	Third-party personal information, protected health information, payment card data, government ID numbers "or other sensitive or regulated data" (ToS §5.3). The apps do not detect such data technically	Permitted classification: [CLASSIFICATION]. Prohibited: [CLASSIFICATION]
Tracking	No analytics, telemetry or advertising; no tracking cookies; authentication cookies only when cloud storage is enabled (Privacy §3, §7.7)	[REQUIREMENT / FINDING]

4. HOSTING AND DATA LOCATION

Topic	SPERT® Suite today (source)	Requirement and finding
Web hosting	Vercel Inc. serves the pages and receives standard request data (Privacy §1, §4.6)	[REQUIREMENT / FINDING]
Cloud data at rest	"Cloud Storage data and AI Connectivity relay data are currently stored at rest in the United States (Google Cloud Firestore multi-region nam5)" (Privacy §9). The operator "will give notice by updating this Policy before changing that location" (§9)	[REQUIREMENT / FINDING]

Topic	SPERT® Suite today (source)	Requirement and finding
Server functions	Google Cloud Functions in us-central1 (AI Privacy Notice §5; code)	[REQUIREMENT / FINDING]
Processing elsewhere	Operational logs are kept 30 days in Google Cloud Logging, "whose default storage location is not restricted to a specific country or region" (Privacy §2.3); Google's authentication, security and support operations "may involve processing elsewhere" (§9)	[REQUIREMENT / FINDING]
Region choice	None: US only	[REQUIREMENT / FINDING]

5. IDENTITY AND ACCESS

Topic	SPERT® Suite today (source)	Requirement and finding
Sign-in	Tier 1 needs no account. Tier 2 uses Google Sign-In or Microsoft Sign-In only, "including Microsoft Entra ID / Azure AD organizational accounts" (Privacy §2.1). No passwords are stored	[REQUIREMENT / FINDING]
MFA and conditional access	Inherited from [ORGANIZATION]'s identity provider when users sign in with work accounts; no MFA setting in the apps	[REQUIREMENT / FINDING]
Microsoft admin consent	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). Alternatives: Google sign-in, or tier 1 only	[REQUIRED / NOT REQUIRED]
SSO enforcement, SCIM, admin console	Not provided. [ORGANIZATION] cannot force users onto its tenant or manage users centrally	[REQUIREMENT / FINDING]
Access control	Firestore security rules: users list and read only projects they are members of, by role (owner, editor, viewer); only owners delete; settings are private to each user (<i>Architecture Overview</i> §3). Rules are kept in source control, deployed automatically and checked for drift every six hours	[REQUIREMENT / FINDING]
Tenant isolation	One multi-tenant database, separated logically by authentication and rules (ToS §5.2)	[REQUIREMENT / FINDING]
Operator access	The operator administers the cloud project and so has technical access to tier 2 data; licensed to host and back it up "solely as necessary to provide the Services" (ToS §5.6). No access-logging commitment. Tier 1 data is never accessible to the operator	[REQUIREMENT / FINDING]

Topic	SPERT® Suite today (source)	Requirement and finding
Shared computers	Local projects belong to the browser profile, so anyone using that profile can see them. Signing out resets the Terms acceptance flag in five apps (2026-10-25); in SPERT® Scheduler acceptance is still remembered per browser	[REQUIREMENT / FINDING]

6. ENCRYPTION

Topic	SPERT® Suite today (source)	Requirement and finding
In transit	"HTTPS encryption for all data in transit" (Privacy §5)	[REQUIREMENT / FINDING]
At rest	Relies on "Google Cloud's infrastructure-level security controls" (Privacy §5); no separate statement by the operator. Local data is protected only as well as the user's device	[REQUIREMENT / FINDING]
Customer-managed keys	Not supported	[REQUIREMENT / FINDING]

7. LOGGING, MONITORING AND AUDIT

Topic	SPERT® Suite today (source)	Requirement and finding
Operational logs	Request metadata (IP address, timestamp, requested URL) kept 30 days, used "only to operate, secure, and troubleshoot the Services" (Privacy §2.3). Available to the operator only	[REQUIREMENT / FINDING]
Audit log for [ORGANIZATION]	None for users or administrators	[REQUIREMENT / FINDING]
Availability monitoring	The operator checks the web apps every 5 minutes with an external uptime service; the Connect AI server is checked about every six hours, not at its public address (operator's statement and repository workflow, 2026-10-25). No status page	[REQUIREMENT / FINDING]

8. VULNERABILITY MANAGEMENT AND SECURE DEVELOPMENT

Topic	SPERT® Suite today (source)	Requirement and finding
Code and dependency scanning	Dependabot alerts, CodeQL code scanning, secret scanning with push protection, and protected main branches on all eight public SPERT® repositories since 2026-10-25. Dependency updates are applied by hand after a soak period	[REQUIREMENT / FINDING]

Topic	SPERT® Suite today (source)	Requirement and finding
Vulnerability reporting	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	[REQUIREMENT / FINDING]
Security reviews	The developer's own: SPERT® Scheduler's SECURITY.md records earlier audits; a self-audit of SPERT® Scheduler v0.79.8 (2026-10-24) led to fixes in the shared backend and that app, listed in their public changelogs; a suite-wide self-review was completed on 2026-10-25, with fixes released in stages. None is independent	[REQUIREMENT / FINDING]
Penetration test	None by a third party. The Terms of Service (§4) forbid probing, scanning or testing the live service's security; review the public source, run a separate copy, or ask the operator in writing first	[REQUIREMENT / FINDING]
Browser security headers	Vary by app. Checked in each repository's configuration, not measured live for every app (<i>Architecture Overview</i> , Reviewer notes)	[REQUIREMENT / FINDING]

9. CONNECT AI (TIER 3 ONLY)

Topic	SPERT® Suite today (source)	Requirement and finding
Built-in AI	None. The user connects their own AI assistant through the Model Context Protocol (AI Privacy Notice §1)	[REQUIREMENT / FINDING]
Which apps	SPERT® Scheduler and SPERT® Story Map (Write Mode required, Read Mode optional); SPERT® Forecaster (Read Mode only). Not offered in SPERT® CFD, GanttApp™ or MyScrumBudget™ (AI Privacy Notice §2.3)	[REQUIREMENT / FINDING]
Data to the AI provider	Write Mode: "Your existing project data remains in your browser's local storage and is not uploaded to any server" (§2.1). Read Mode: a snapshot of the one open project, including free text, goes to the relay and the AI provider, "regardless of your storage setting" (§2.2). The <i>Data Flow Diagram</i> lists the fields per app	[REQUIREMENT / FINDING]

Topic	SPERT® Suite today (source)	Requirement and finding
Relay retention	Deleted on disconnect, when Read Mode is turned off, or seven days after the session's last activity, including requests from the AI assistant; backups up to 98 days (AI Privacy Notice §2.2, §4). Signing out ends the session on the server in all three apps (since SPERT® Scheduler 0.79.25, SPERT® Story Map 0.53.13 and SPERT® Forecaster 0.47.3); if the server cannot be reached at that moment, for example when offline, the app tells the user and keeps retrying. Disconnecting also ends the session on the server, but if the server cannot be reached, SPERT® Scheduler and SPERT® Story Map do not tell the user. Until a later attempt succeeds, the relay data stays until the session expires seven days after the session's last activity, including requests from the AI assistant; because each AI request extends the session, one that an AI keeps using does not expire. The AI provider's own terms govern what it keeps	[REQUIREMENT / FINDING]
What the AI can change	Scheduler: 25 tools; some overwrite names, estimates, descriptions and order, and two remove links (a dependency, a milestone assignment). Story Map: 21 tools; some overwrite or clear text, sizes and allocations. Forecaster: 3 read-only tools. No tool deletes an activity, milestone, story-map item or project	[REQUIREMENT / FINDING]
Server access model	No API key or user login; access rests on a single-use pairing code (one word plus 10 digits, valid 15 minutes), then the session's random identifier, plus a rate limit. Stronger session protection is planned but not built (<i>Architecture Overview</i> §4)	[REQUIREMENT / FINDING]
Organization control	No administrator switch; consent is per user, per app, per browser (AI Privacy Notice §1). Effective controls: an acceptable-use rule, and [AI PLATFORM] 's own connector controls if it has them. 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.	Approved AI platform and account type: [AI PLATFORM]
Model training	"The Operator does not use your data to train machine learning models" (Privacy §3). The AI provider's terms govern it	[REQUIREMENT / FINDING]

10. THIRD PARTIES

Provider	Role	Receives	Tier	Source
Google LLC (Firebase, Google Cloud)	Sign-in, database, functions, Connect AI server, logs	Account, cloud project, relay and technical data	2, 3	Privacy §2.3, §4.1
Vercel Inc.	Hosts the web pages	Standard request data	All	Privacy §1, §4.6
Resend	Sends invitation emails	Invitation details	2	Privacy §2.6, §4.6

Provider	Role	Receives	Tier	Source
Nager.Date	Public-holiday lookup in SPERT® Scheduler only	Country list; country code and year; sees the request's IP address	1 (optional)	Code; Privacy Policy §1
The user's AI provider ([AI PLATFORM])	Chosen by the user; not a service provider of the operator	Prompts; Read Mode snapshots; AI-generated edits	3	Privacy §4.5

Microsoft (Exchange Online), which hosts the operator's [spertsuite.com](#) mailbox and so receives anything emailed to those addresses ([Privacy](#) §2.7, §4.6), Formspreer (website contact forms) and Stripe ("if subscription payments are implemented") are also named in [Privacy Policy](#) §4 but play no part in using the apps. No separate subprocessor list is published. Google Cloud and Vercel publish their own security and compliance reports, which cover their infrastructure, not SPERT® Suite's code; [REVIEWING TEAM] should read the current versions directly.

11. RETENTION, DELETION AND PORTABILITY

Topic	SPERT® Suite today (source)	Requirement and finding
Retention	Cloud data while the account is active; logs 30 days; invitation records until purged; backups up to 98 days (Privacy §2.3, §2.6, §6)	[REQUIREMENT / FINDING]
Deletion	By request; "not to exceed thirty (30) days under normal circumstances"; no self-service control (Privacy §6, §7.3). Google's Firebase Authentication may keep a deleted account's sign-in information for up to 180 days (§6). Turning off cloud storage does not delete stored data (§7.4). Local data is deleted by the user	[REQUIREMENT / FINDING]
Portability	Projects can be exported from each app at any time (Privacy §7.1)	[REQUIREMENT / FINDING]
Backups for [ORGANIZATION]	None: operator backups are "not available to you as a restore service" (Privacy §6); users are "solely responsible for maintaining independent backups" (ToS §5.2)	[REQUIREMENT / FINDING]

12. INCIDENT RESPONSE AND CONTINUITY

Topic	SPERT® Suite today (source)	Requirement and finding
Breach notification	If an incident "creates a material risk of harm", affected users are notified "by email or in-app notice" and regulators "where required by applicable law" (Privacy §5.1). No contractual timeline	[REQUIREMENT / FINDING]
Incident response plan	None published	[REQUIREMENT / FINDING]
Liability	Capped at the greater of \$25 or fees paid in the previous 12 months (ToS §9); user indemnifies the operator (ToS §10)	[REQUIREMENT / FINDING]
Continuity	No continuity plan; single operator. Local data keeps working while the site is served; projects can be exported; the GPL permits self-hosting under a different name	[REQUIREMENT / FINDING]

13. ASSURANCE

The operator holds no certification (SOC 2, ISO 27001 or similar), has not completed a formal security questionnaire (CAIQ, SIG, HECVAT) and has had no independent penetration test. Evidence available instead: public source code; documented self-reviews and public changelogs; the hosting providers' own reports for their layers; and tier 1, in which no project data leaves the device. The operator says further security documentation is in preparation; it is not published, and none of it is an independent assessment.

14. GAPS AND THE ORGANIZATION'S RESPONSE

#	Gap	Tiers affected	Possible compensating control	Decision
1	No certification, independent audit or penetration test	2, 3	Tier 1 only; review of public source	[ACCEPT / MITIGATE / DECLINE]
2	No DPA; operator is controller (Privacy §7.6)	2, 3	Tier 1 only; no personal data beyond users' own name and email	[ACCEPT / MITIGATE / DECLINE]
3	No SLA, support or continuity commitment	All	Non-critical use; regular exports	[ACCEPT / MITIGATE / DECLINE]
4	No SSO enforcement, SCIM, admin console or audit log	2	Work accounts required by policy; classification limit	[ACCEPT / MITIGATE / DECLINE]
5	No organization switch for Connect AI	3	Acceptable-use rule; [AI PLATFORM] connector controls	[ACCEPT / MITIGATE / DECLINE]
5a	Microsoft sign-in may need admin consent in Entra ID (app not yet from a verified publisher)	2	Entra administrator grants consent; or Google sign-in; or tier 1 only	[ACCEPT / MITIGATE / DECLINE]
6	US-only cloud storage; logs not region-restricted	2, 3	Tier 1 only where residency matters	[ACCEPT / MITIGATE / DECLINE]
7	Deletion by request only	2	Record the request process in the conditions	[ACCEPT / MITIGATE / DECLINE]
8	Local projects belong to the browser profile	1	Assigned devices or one profile per person	[ACCEPT / MITIGATE / DECLINE]
9	[OTHER GAP RAISED BY REVIEWER]	[TIER]	[CONTROL]	[ACCEPT / MITIGATE / DECLINE]

15. CONDITIONS OF APPROVAL

[CONDITIONS]. For example: apps limited to [\[APPS REQUESTED\]](#); tier [\[TIERS REQUESTED\]](#) only; data classified [\[DATA CLASSIFICATION\]](#) or lower; work accounts only for tier 2; Connect AI only with [\[AI PLATFORM\]](#), Read Mode [\[ALLOWED / NOT ALLOWED\]](#); weekly exports; review on [\[REVIEW DATE\]](#).

REVIEWER NOTES

- **"Open source with no vendor review."** No third party has reviewed it, and this profile does not claim otherwise. What exists is public code, versioned and drift-checked access rules, and a written security history. [\[REVIEWING TEAM\]](#) can verify claims directly in the source.
- **"Data leaving the environment."** Tier 1 sends no project data anywhere. Tiers 2 and 3 are separate decisions in section 1, so declining them does not block tier 1.

- **"Audit and logging."** There is no customer audit log. If [ORGANIZATION] requires one for the proposed data, limit the classification or approve tier 1 only.
- **"Unfamiliar vendor."** A single-operator business with no contract. The pilot conditions in section 15 are designed around that: small, time-boxed, exportable, reversible.
- **Scope and limits.** Facts were checked against each app's source at the versions above and against the current legal documents. Not verified: live security headers for every app, export formats in each running app, deployed logging settings, and the providers' current certifications.

Attestation (for the organization to complete)				
Role	Name	Decision (tier 1 / 2 / 3)	Conditions	Date
[reviewer role]	[name]	[] / [] / []	[conditions]	[date]
[reviewer role]	[name]	[] / [] / []	[conditions]	[date]
[approver role]	[name]	[] / [] / []	[conditions]	[date]