Security and Privacy

How Trellis handles your data, what it does and does not transmit, and what your IT partners need to know.

> **The short version.** Trellis runs entirely in your browser. Your project data never leaves your machine. There are no user accounts, no analytics, no telemetry, and no outbound network requests in normal operation. Your work lives in browser storage and in .trellis files you save locally.

Where your data lives

All Trellis project data stays on your machine. Three places hold it:

- **Browser storage (localStorage).** Trellis auto-saves your current project to your browser so you can close the tab and pick up where you left off. This data lives in your browser profile and is never sent anywhere.
- **.trellis files on disk.** When you save or open a project, Trellis uses your browser's native file picker. You choose where the file lives. Trellis writes directly to that location and reads from it on subsequent saves.
- **Browser storage (IndexedDB).** Component packs — reusable components you save for re-use across projects — are stored in IndexedDB rather than localStorage, because saved components include preview images that would exhaust the smaller localStorage budget the project auto-save uses. This data lives in the same browser profile, under the same origin, and is never sent anywhere.

.trellis files are plain JSON. You can open one in a text editor to inspect it. There are no hidden payloads, no embedded scripts, and no executable content.

What Trellis transmits

Nothing. In normal use, Trellis makes zero outbound network requests. An audit of the source code confirms there is no fetch, no XMLHttpRequest, no WebSocket, and no analytics, telemetry, error reporting, or update-check behavior anywhere in the application.

Fonts are bundled with the application and served from the same origin as Trellis itself. There are no calls to Google Fonts or any other external CDN at runtime.

The only external link in the entire app is a LinkedIn attribution link on the mobile-blocker overlay, and that link is only followed if a user explicitly taps it.

File handling

Everything Trellis imports or exports happens locally in your browser:

- **Project files.** .trellis and .json imports go through a validation chain that checks the file structure, rejects malformed content, and refuses to load files created by a newer version of Trellis than the one you have installed.

- **Exports.** Field inventories, rules grids, and test case workbooks are generated as XLSX files entirely in the browser. PNG mockup exports are produced by rendering the canvas to an HTML5 Canvas element and downloading the result.
- **Clipboard.** Copy and paste of components uses a custom JSON payload that is validated on every paste before any data reaches the canvas.

Third-party dependencies

Trellis is built with a deliberately small dependency footprint. Five production libraries, all client-side, none with network behavior:

`react`	UI framework
`react-dom`	DOM rendering
`html-to-image`	PNG mockup export
`interactjs`	Drag and resize gestures
`xlsx-js-style`	XLSX file generation

npm audit reports zero known vulnerabilities in this dependency set. We re-run the audit on every release.

Hosting and security headers

trellismade.com is hosted on Netlify. The application is a static bundle: HTML, JavaScript, CSS, and locally hosted fonts. There is no backend server, no database, and no application API. HTTPS is enforced with a one-year HSTS policy. The following security headers are active on every response:

- Content-Security-Policy (restrictive; no external origins allowed)
- Strict-Transport-Security (HSTS with includeSubDomains)
- X-Frame-Options: DENY (no embedding in iframes)
- X-Content-Type-Options: nosniff
- Referrer-Policy: strict-origin-when-cross-origin

For your IT partners

A detailed source-code-audit document is available on request. It covers the full dependency tree, network behavior, file handling validation, deployment configuration, and a category-by-category review of client-side security posture. The audit confirms Trellis is suitable for deployment on restricted internal networks, including air-gapped environments, without code changes.

Questions about security or privacy? Reach out via the contact details on trellismade.com. This document reflects the state of Trellis as of the version stamped at the bottom of the page.