Security Pack

Last updated: June 10, 2026

Untitled UI® (ABN 65 655 466 729) is operated by **Sisyphus Ventures Pty Ltd** (ACN 655 466 729). **Untitled UI React** is a commercial React component and UI library developed and maintained by Untitled UI.

Untitled UI products are primarily delivered as downloadable source code and design assets. The platform does not process or store customer production application data, payment card information, healthcare information, or other highly sensitive end-user data.

This document outlines the current security architecture, operational practices, and data handling approach for Enterprise customers.

Infrastructure & Hosting

Untitled UI infrastructure runs entirely on managed cloud platforms. We do not operate our own servers or use cloud infrastructure (e.g. AWS) directly; our managed providers run on top of leading cloud infrastructure (Vercel and Supabase are themselves built on AWS).

Our managed providers are:

- **Vercel** — application hosting and serverless functions
- **Supabase** — managed Postgres database and authentication (runs on AWS)
- **Cloudflare** — CDN and edge security

Source code repositories are hosted via:

- **GitHub**

Authentication & Access Control

Untitled UI uses passwordless authentication via secure magic-link login flows.

- No customer passwords are stored by Untitled UI
- Authentication emails are delivered via Resend
- Magic-link sign-in tokens are single-use
- Enterprise customers can enable SAML 2.0 Single Sign-On (see Single Sign-On & Provisioning below)
- Access to private GitHub repositories is managed through invitation and access controls

Access to production systems is restricted to authorized personnel only.

Single Sign-On (SSO) & Provisioning (Enterprise)

Enterprise plans support SAML 2.0 Single Sign-On (SS) so that customers can manage employee access through their own identity provider (e.g. Okta, Microsoft Entra ID, OneLogin). SSO is built on Supabase Auth (GoTrue), which manages the SAML configuration; Untitled UI stores only a pointer to the configured provider and the customer's verified email domains.

- **Domain verification** — email domains must be verified via DNS before they can route SSO logins, preventing cross-organization domain claims.
- **Just-in-time provisioning** — users authenticating via SSO are provisioned into their organization automatically on first login.
- **SCIM 2.0** — optional automated user provisioning and de-provisioning, so that removing a user in the customer's identity provider revokes their access to Untitled UI. SCIM is authenticated with a per-organization bearer token (only a hash of the token is stored).
- When SSO is enabled for a verified domain, magic-link sign-in is disabled for that domain so access is consistently governed by the customer's identity provider.

Customer Data

Untitled UI stores limited customer information required for licensing, account management, and access control purposes.

Stored information may include:

- Account and team-member email addresses
- License tier and order reference information
- Team membership and access status
- API keys used to authenticate the CLI and component downloads (stored as hashes for newly issued keys)
- For customers who use the GitHub repository feature, the GitHub username being granted access
- For Enterprise SSO/SCIM customers: verified email domains and identity-provider identifiers
- Identity and access audit log events (see Audit Logging below), which include the acting user, timestamp, IP address, approximate location (city/country), and user-agent

Untitled UI does not store:

- Payment card details
- Banking information
- Customer application data
- End-user data belonging to customer applications

Payment processing and billing information is handled by Polar.sh as Merchant of Record.

Payments & Billing

Untitled UI does not directly process or store customer payment card information.

Billing and payment processing is managed by Polar.sh, which acts as Merchant of Record for Untitled UI purchases.

Polar.sh may store customer billing details and transaction-related information as part of payment processing and compliance obligations.

Repository Access

Enterprise customers may receive access to private GitHub repositories containing Untitled UI React source code.

Repository access is:

- Restricted to authorized customer users
- Managed through GitHub access controls (collaborator invitations to a private repository)
- Granted and revoked by the customer's organization administrator from their account, or by Untitled UI
- Revocable at any time in accordance with license terms

Audit Logging (Enterprise)

For Enterprise organizations, Untitled UI maintains an identity and access audit log covering security-relevant events such as SSO logins, SCIM provisioning and de-provisioning, domain verification, team membership changes, API key creation/rotation/revocation, and GitHub access changes.

Organization administrators can view their organization's audit log and export it as CSV from their account.

Each event records the actor, action, timestamp, source IP address, approximate location, and user-agent.

Audit records are stored in our managed Postgres database (Supabase) and are accessible only to the owning organization's administrators and authorized Untitled UI personnel.

AI Features & Data Processing

Untitled UI offers an optional semantic component search (via our MCP server and search tools). When this feature is used, the **search query text** entered by the user is sent to

Google's Generative AI (Gemini) embeddings API to compute a vector embedding for matching. No account data, customer application data, or stored personal data is sent to this service — only the search query itself. Component and template content is pre-embedded and stored by Untitled UI; the AI service is used only to embed live queries.

Security Reporting

Security vulnerabilities or concerns may be reported to:

→ **hello@untitledui.com**

Untitled UI requests responsible disclosure of any identified vulnerabilities.

Shared Responsibility

Untitled UI is delivered primarily as a downloadable code library and design system.

Customers are responsible for:

- Secure implementation within their own applications
- Infrastructure security of deployed customer systems
- Dependency management within customer environments
- Application-level authorization and data protection controls

Compliance

Untitled UI is not currently certified under SOC 2, ISO 27001, or similar compliance frameworks.

Additional security documentation may be made available to Enterprise customers upon request.

Security Questionnaire

Company Information

Question	Response
Company	Sisyphus Ventures Pty Ltd ACN 655 466 729
Trading as	Untitled UI ABN 65 655 466 729
Registered address	11 Parbery Street Kingston ACT 2604 AUSTRALIA
Products	Untitled UI React Untitled UI Figma Untitled UI Icons
Support contact	hello@untitledui.com
Security contact	hello@untitledui.com
Primary website	untitledui.com
Hosting regions	Managed cloud infrastructure providers.
Business type	Commercial software and design system provider.

Application Architecture

Question	Response
Is Untitled UI a SaaS platform?	Primarily no. Untitled UI products are primarily delivered as downloadable source code and design assets.
Does the platform process customer production data?	No
Does the platform process payment card data?	No
Does the platform process healthcare or regulated data?	No
Is customer application data stored by Untitled UI?	No

Authentication & Identity

Question	Response
Are passwords stored?	No
What authentication model is used?	Passwordless magic-link authentication; SAML 2.0 SSO for Enterprise.
Authentication delivery provider	Resend

Question	Response
Are sign-in tokens single-use?	Yes
Is SSO supported?	Yes — SAML 2.0 Single Sign-On on Enterprise plans.
Is automated provisioning supported?	Yes — optional SCIM 2.0 provisioning / de-provisioning.
Is the SCIM token stored securely?	Only a hash of the per-organization SCIM token is stored.
Are customer repositories access controlled?	Yes
How is repository access managed?	GitHub collaborator invitations, managed by the org admin or Untitled UI.

Data Storage

Question	Response
Primary database provider	Supabase (managed Postgres, runs on AWS).
Types of customer data stored	Email addresses, license/order info, team membership, hashed API keys, GitHub usernames (if used), SSO domains/IdP identifiers, and audit-log events (incl. IP and approximate location).

Question	Response
Is data encrypted at rest?	Yes — Supabase encrypts data at rest (AES-256)
Is data encrypted in transit?	Yes — HTTPS/TLS
Is payment data stored?	No
Is customer production data stored?	No

Infrastructure & Vendors

Question	Response
Do we use cloud infrastructure (e.g. AWS) directly?	No — we use managed platforms (Vercel, Supabase) that themselves run on AWS.
Application hosting provider	Vercel
Database & authentication	Supabase (managed Postgres on AWS).
CDN / Edge provider	Cloudflare
Source code hosting	GitHub
Merchant of Record	Polar.sh
Email delivery	Resend

Question	Response
AI / embeddings (semantic search)	Google Generative AI (Gemini) — receives search query text only.
Analytics providers	Google Analytics, Vercel Analytics

Access Control & Operations

Question	Response
Is production access restricted?	Yes — limited to the two company co-owners.
Is multi-factor authentication (MFA)enforced for production / provider access?	Yes — MFA is enabled across all infrastructure and service providers.
Number of personnel with production access	Two (both co-owners).
Is role-based access control (RBAC) used internally?	Not applicable at current team size — both personnel are co-owners requiring full administrative access; protected by MFA. Role separation will be introduced if the team grows.
Are formal periodic access reviews performed?	Not applicable at current team size (fixed two-owner team; no employee/contractor onboarding or offboarding).

Question	Response
Is repository access revocable?	Yes
Are customer permissions managed centrally?	Yes — organization administrators manage their members' access (and, for Enterprise, via SSO/SCIM).

Security Operations

Question	Response
Is a vulnerability disclosure channel available?	Yes
Security contact	hello@untitledui.com
Are formal penetration tests performed?	Not currently disclosed.
Is a formal SOC 2 or ISO certification maintained?	Not currently.
Is customer data encrypted in transit?	Industry-standard HTTPS/TLS connections are used.

Untitled UI

Untitled UI® (ABN 65 655 466 729) is operated by Sisyphus Ventures Pty Ltd (ACN 655 466 729), based in Melbourne, Australia.

If you have any questions regarding this Security Pack or Untitled UI's privacy and data protection practices, please get in touch with our friendly team via:

→ **hello@untitledui.com**