Workload — Security overview (informational)

Audience : IT / security / procurement teams.

Publication date : May 2026

Status : technical transparency document; not a certification (not equivalent to SOC 2, ISO 27001, etc.) and does not replace customer-led due diligence or a commissioned penetration test.

1. Service description

Workload is a SaaS platform for IT capacity planning and management (projects, teams, budgets, timesheets, third-party tool integrations). Typical data includes: user accounts, organizations, projects, allocations, KPIs, audit logs, and—depending on configuration—integration credentials for tools such as Jira or Azure DevOps.

2. Responsibility model

- Controller of personal data in the operational sense is usually the customer organization (often the employer) for data entered by its users in Workload.

- Workload acts as a processor for service delivery, within the limits set by the published Terms and Privacy Policy.

- Subprocessors (hosting, database, transactional email, payments, etc.) are listed on the website Subprocessors page (,).

3. Authentication and access control

| Topic | Documented implementation |

|--------|--------------------------|

| Web authentication | NextAuth.js; httpOnly session cookies; OAuth, credentials, SAML/OAuth SSO per organization. |

| Enterprise SSO | Per-organization configuration (Azure AD, Google Workspace, Okta, Auth0, generic SAML); CSRF state for SSO flows; SAML validation (certificates, signatures). |

| Passwords | bcrypt hashing (e.g. 10 rounds) for local password accounts. |

| API keys (REST API v1) | Stored as SHA-256 hashes; visible prefix in the UI; Bearer authentication. |

| Authorization | RBAC and fine-grained permissions; server-side checks on sensitive routes. |

4. Encryption and secrets

| Topic | Documented implementation |

|--------|--------------------------|

| In transit | HTTPS/TLS for browser traffic and public API calls. |

| At rest (app secrets) | OAuth tokens and similar integration material encrypted with AES-256-CBC before database storage; key from ** env var (format enforced by the app). |

| Passwords | Not stored in clear text (see bcrypt). |

5. REST API and integrations

- Versioned prefix : for the public documented API (OpenAPI).

- Input validation : Zod schemas on relevant endpoints.

- Rate limiting : per plan (e.g. 100/h up to 100,000/h depending on tier), informative response headers.

- Webhooks : HMAC-SHA256 signature; constant-time comparison (); randomly generated secret; retries with backoff and send timeout.

6. Logging and audit

- Audit trail for sensitive actions (resource, action, user, timestamp, IP, User-Agent as implemented).

- Audit log access is generally limited to administrative roles in the product.

7. HTTP headers and hardening

Documented configuration (e.g.) includes, among others:

-

- (tuned for the app)

- , , , ,

- disabled for Next.js

8. Application and data protection

- Prisma ORM : parameterized queries, reduced risk of classic SQL injection.

- Multi-tenant isolation : data scoped to organizations; access control must ensure users only see their organization’s data (validate during your reviews).

9. Personal data (GDPR snapshot)

Typical items to confirm on your instance / contract:

- User data export and deletion flows (documented in-product, e.g. settings / compliance pages).

- DPO / privacy contacts published on the Compliance page.

- Retention and subprocessors : formalize in your DPA and records of processing.

10. Hosting and availability

- Application commonly hosted on Vercel (Edge / Serverless); PostgreSQL managed database (provider depends on deployment: Neon, Supabase, Vercel Postgres, etc.).

- Status page on the website; optional link to an external status page when is set.

11. Security reviews

An internal pentest preparation document describes the expected posture and past remediations (secret encryption, headers, validation, etc.). This is not proof of a successful third-party pentest : customers may require their own test or vendor report.

12. Limitations

- Based on documentation and code at publication time; architecture may change.

- No absolute security guarantee; security also depends on customer configuration (SSO, roles, API key hygiene, user training).

- For contractual or regulatory matters, contact legal and Workload support**.

End of document.