Workload — Synthèse sécurité (informationnelle)

Document : vue d’ensemble à l’usage des équipes IT / RSSI / achats.

Date de rédaction : mai 2026

Statut : document technique interne de transparence ; il ne constitue pas une certification (pas d’équivalence SOC 2, ISO 27001, etc.) et ne remplace pas une due diligence ni un pentest mandaté par le client.

1. Objet du service

Workload est une plateforme SaaS de planification de capacité et de pilotage pour directions des systèmes d’information (projets, équipes, budgets, feuilles de temps, intégrations outillage). Les données traitées incluent typiquement : comptes utilisateurs, organisations, projets, affectations, indicateurs, journaux d’audit et, selon configuration, identifiants d’intégration vers des outils tiers (Jira, Azure DevOps, etc.).

2. Modèle de responsabilité

- Responsable du traitement des données personnelles au sens opérationnel : l’organisation cliente (souvent l’employeur), pour les données saisies par ses utilisateurs dans Workload.

- Workload agit en tant que sous-traitant pour l’exécution du service, dans les limites décrites par les conditions générales et la politique de confidentialité publiées sur le site.

- Les sous-traitants techniques (hébergement, base de données, messagerie transactionnelle, paiement, etc.) sont listés sur la page Sous-traitants du site (,).

3. Authentification et contrôle d’accès

| Sujet | Implémentation documentée |

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

| Authentification web | NextAuth.js ; sessions via cookies httpOnly ; support OAuth, identifiants, SSO SAML/OAuth par organisation. |

| SSO entreprise | Configuration par organisation (Azure AD, Google Workspace, Okta, Auth0, SAML générique) ; état CSRF pour les flux SSO ; validation SAML (certificats, signatures). |

| Mots de passe | Hachage bcrypt (ex. 10 rounds) pour les comptes en mot de passe local. |

| Clés API (API REST v1) | Stockage sous forme de hash SHA-256 ; préfixe visible pour identification côté UI ; authentification Bearer. |

| Autorisation | Modèle RBAC et permissions fines ; contrôles côté serveur sur les routes sensibles. |

4. Chiffrement et secrets

| Sujet | Implémentation documentée |

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

| Transit | HTTPS/TLS pour le trafic navigateur et les appels API publics. |

| Au repos (secrets applicatifs) | Secrets OAuth, jetons d’intégration et matériel similaire chiffrés en AES-256-CBC avant stockage en base ; clé via variable d’environnement ** (format imposé côté application). |

| Mots de passe | Non stockés en clair (voir bcrypt). |

5. API REST et intégrations

- Préfixe versionné : pour l’API publique documentée (OpenAPI).

- Validation des entrées : schémas Zod sur les endpoints concernés.

- Limitation de débit : rate limiting par plan (plages du type 100/h à 100 000/h selon offre), avec en-têtes de réponse informatifs.

- Webhooks : signature HMAC-SHA256 ; comparaison en temps constant () ; secret généré de façon aléatoire ; retry avec backoff et timeout côté émission.

6. Journaux et audit

- Audit trail : journalisation d’actions sensibles (ressource, action, utilisateur, horodatage, IP, User-Agent selon implémentation).

- Accès aux journaux d’audit généralement réservé aux rôles d’administration dans le produit.

- Export organisation (rôles ADMIN/OWNER) : export Excel ou JSON des données organisation, incluant le type ** pour due diligence et revues RSSI — parcours organisation*.

7. En-têtes HTTP et durcissement

Configuration documentée (ex.) incluant notamment :

-

- (adaptée à l'application)

- , , , ,

- Désactivation de l'en-tête Next.js

8. Protection applicative et données

- ORM Prisma : requêtes paramétrées, réduction du risque d'injection SQL classique.

- Cloisonnement multi-tenant : données rattachées à l'organisation ; les contrôles d'accès doivent garantir qu'un utilisateur ne lit que les données de son organisation (logique métier à valider lors de vos revues).

9. Données personnelles (aperçu RGPD)

Fonctionnalités courantes à vérifier sur votre instance / contrat :

- Export et suppression de données utilisateur (parcours documentés côté produit, ex. paramètres compte / conformité).

- Contact DPO / confidentialité : adresses publiées sur la page Conformité du site.

- Durées de conservation et sous-traitance : à formaliser dans votre DPA et votre registre des traitements.

10. Hébergement et disponibilité

- Application typiquement hébergée sur Vercel (Edge / Serverless) ; base PostgreSQL managée (fournisseur selon déploiement : Neon, Supabase, Vercel Postgres, etc.).

- Page Statut sur le site ; lien optionnel vers une page de statut externe si la variable ** est configurée.

11. Revues de sécurité

Un document interne de préparation pentest décrit la posture attendue et des correctifs passés (chiffrement des secrets, en-têtes, validation, etc.). Cela ne vaut pas attestation de pentest réussi : le client peut exiger son propre test ou un rapport tiers.

12. Limites de ce document

- Contenu basé sur la documentation et le code à la date de rédaction ; l’architecture peut évoluer.

- Aucune garantie de sécurité absolue ; la sécurité dépend aussi de la configuration client (SSO, rôles, hygiene des clés API, formation des utilisateurs).

- Pour toute question contractuelle ou réglementaire, s’adresser au juridique et au support** Workload.

Fin du document.