KOMIT
Trust Center

Security Overview

Version 1.0 – Juillet 2026

1. Objet du document

Ce document présente les mesures de sécurité actuellement mises en œuvre par Komit. Il décrit l'état réel de la plateforme à sa date de publication. Les informations présentées n'ont pas vocation à remplacer un contrat, une politique interne ou une certification.

2. Pourquoi la sécurité est essentielle

Komit conserve la mémoire des CSE : contrats, procès-verbaux, documents, décisions et historique de plusieurs mandats. La protection de ces informations est intégrée dès la conception du produit.

3. Nos principes

- Security by Design
- Principe du moindre privilège
- Transparence sur les mesures réellement déployées
- Amélioration continue
- Simplicité des mécanismes de sécurité

4. Cycle de vie des données

Création → Consultation → Modification → Archivage → Suppression. Chaque étape est réalisée dans le respect des droits attribués aux utilisateurs de l'organisation.

5. Protection des accès

Chaque utilisateur appartient à une organisation. Les autorisations sont contrôlées côté serveur avant toute opération sensible. Les mots de passe ne sont jamais stockés en clair.

6. Isolation des organisations

Les données d'un CSE sont isolées des autres organisations. Les contrôles d'autorisation sont réalisés avant tout accès aux informations.

7. Communications et e-mails

Les communications utilisent HTTPS/TLS. Les e-mails transactionnels reposent sur SPF, DKIM et DMARC. Les réponses utilisent le champ Reply-To afin de joindre directement l'interlocuteur concerné.

8. Sauvegardes et continuité

Des sauvegardes automatiques sont réalisées pour faciliter la restauration des données. Les procédures évoluent avec la plateforme.

9. Développement sécurisé

Les données sont validées côté serveur. Les entrées utilisateur sont contrôlées avant traitement. Les dépendances logicielles sont maintenues à jour dans le cadre du cycle de développement.

10. Ce que Komit ne fait pas

✓ Ne revend pas les données de ses clients.

✓ Ne partage pas les données entre organisations.

✓ Ne revendique pas de certifications non obtenues.

✓ Ne documente que les mesures effectivement déployées.

11. Responsabilités partagées

Komit	Organisation cliente
Sécurise la plateforme	Gère les utilisateurs
Protège les échanges	Attribue les droits
Effectue les sauvegardes	Supprime les comptes inutilisés
Maintient les composants	Veille à la confidentialité des identifiants

12. Transparence

Sujet	État
HTTPS / TLS	Oui
Contrôle des accès côté serveur	Oui
Isolation des organisations	Oui
SPF / DKIM / DMARC	Oui
ISO 27001	Non
SOC 2	Non
Audit indépendant	Non communiqué à ce stade

13. Contact sécurité

Pour toute question relative à la sécurité ou à la protection des données :

maxime@komit.fr