Déclaration de sécurité

Introduction

Nos mesures de sécurité sont conçues pour couvrir l'ensemble de la protection des données. Nous utilisons ces protocoles de sécurité pour détecter, prévenir et réagir rapidement à toute menace ou vulnérabilité potentielle. Qu'il s'agisse d'identifier proactivement les risques émergents, de mettre en œuvre des mesures préventives pour les atténuer ou de réagir rapidement et efficacement en cas d'incident, notre approche de la sécurité est globale et dynamique. Nous comprenons l'importance non seulement d'identifier les problèmes de sécurité, mais aussi d'agir rapidement pour préserver l'intégrité et la confidentialité de vos données et informations.

Les contrôles énumérés ci-dessous sont systématiquement mis en œuvre et font l'objet d'évaluations internes régulières, ainsi que d'évaluations menées par l'auditeur SOC2. Ces mesures sont appliquées afin d'obtenir une assurance raisonnable que nous maintenons les garanties nécessaires pour sécuriser nos actifs et ceux de nos clients.

Chiffrement des données
Les données au repos et en transit sont chiffrées. Cela inclut l'utilisation de SSL/TLS pour les données en transit et le chiffrement des données stockées dans les bases de données.

Contrôle d'accès
Le contrôle d'accès basé sur les rôles (RBAC) garantit que seuls les utilisateurs autorisés peuvent accéder à des ressources spécifiques de l'application.

Authentification et autorisation
Des mécanismes d'authentification robustes sont essentiels. Ceux-ci incluent les fournisseurs d'identité, l'authentification unique (SSO), l'authentification multifactorielle (MFA) et la capacité d'intégration aux systèmes d'identité existants.

Pistes d'audit et indicateurs
Des journaux d'audit détaillés sont générés pour consigner les activités des utilisateurs et les événements système. Ces journaux sont utiles à la fois pour la surveillance de la sécurité et la conformité. Des indicateurs sont générés pour les contrôles d'intégrité du système.

Pare-feu et sécurité réseau
Des pare-feu et des groupes de sécurité réseau sont mis en œuvre pour contrôler le trafic entrant et sortant. Cela empêche tout accès non autorisé aux applications et aux données.

Surveillance de la sécurité et intervention en cas d'incident
Surveillance continue de l'application pour détecter les impacts sur le rendement et les menaces à la sécurité, et plan de réponse aux incidents clairement défini en cas de faille de sécurité.

Sauvegardes et récupération de données
Sauvegardes régulières des données et plans de reprise après sinistre pour assurer la continuité des activités en cas de perte de données ou de panne du système.

Analyse des vulnérabilités et des correctifs
Analysez régulièrement les vulnérabilités et appliquez les mises à jour logicielles pour maintenir le système sécurisé et à jour.

Continuité des activités et reprise après sinistre
Établissez un plan pour assurer la disponibilité du service, même en cas d'interruption imprévue.

Certifications de conformité
Nous respectons les normes et réglementations sectorielles en vigueur (par exemple, RGPD, SOC 2).

Isolation des données
Les données appartenant à différents clients sont séparées de manière logique afin d'éviter toute fuite de données.

Développement de logiciels sécurisés
Des pratiques de codage sécurisées sont appliquées lors du développement de l'application SaaS afin de prévenir les vulnérabilités courantes.

Vérifications de sécurité et tests d'intrusion réguliers
Des audits de sécurité et des tests d'intrusion périodiques sont effectués afin d'identifier et de corriger les vulnérabilités.

Contrôles de confidentialité
Nous mettons en œuvre des contrôles de confidentialité pour protéger les données sensibles des utilisateurs et respecter les règlements en matière de protection des données.