aircall

Aperçu de la sécurité

Sommaire

Introduction

Aircall prend la sécurité de l'information et la conformité très au sérieux. Ce document vise à assurer à nos clients que leurs données sont traitées de façon à répondre à leurs exigences en matière de protection des données et de conformité, et à offrir une transparence totale et une tranquillité d'esprit aux clients d'Aircall, en leur assurant que leurs informations sont entre de bonnes mains.

Nos contrôles et mécanismes de sécurité sont basés sur la norme ISO 27001 relative à la sécurité de l'information et sur les normes NIST, qui comprennent des programmes couvrants : les règles et procédures, le contrôle d'accès, la continuité des activités, la sécurité des RH, la sécurité de l'infrastructure réseau, la sécurité des tiers, la gestion des vulnérabilités, ainsi que la gestion des incidents.

Organisation de la sécurité

Aircall dispose d'une équipe chargée de la sécurité de l'information, qui est responsable de toutes les questions de sécurité au sein de l'organisation.

Notre équipe de sécurité est titulaire de diverses certifications et autres titres qui attestent de ses compétences dans le domaine.

Sécurité des ressources humaines

Vérification des antécédents et accords de non-divulgation

Les employés d'Aircall sont soumis à une vérification exhaustive de leurs antécédents par un tiers avant de recevoir une offre d'emploi officielle, dans la mesure où les réglementations locales et les normes d'emploi le permettent. Tous les employés d'Aircall doivent signer des accords de non-divulgation avant d'avoir accès aux systèmes ou aux données de l'entreprise.

Sensibilisation et formation

L'éducation est un élément central d'un programme efficace de sécurité de l'information. Sans elle, les contrôles techniques ne peuvent pas protéger efficacement les données des patients ni les autres informations sensibles.

Chaque nouvel employé doit assister à une session de formation à la sécurité de l'information lorsqu'il rejoint l'entreprise. Cette session vise à sensibiliser le nouveau membre du personnel à ses responsabilités et à souligner son rôle dans la protection contre les menaces internes, les rançongiciels, l'ingénierie sociale, l'utilisation appropriée des actifs et d'autres aspects connexes.

Après la formation initiale, une formation continue est assurée au moyen de mises à jour, notifications et communications internes effectuées au moins bimensuellement.

Gestion d'accès et d'identification

Aircall suit un processus strict pour accorder ou révoquer l'accès à ses ressources. L'accès au système est basé sur les concepts du « principe de moindre privilège » et du « besoin d'en connaître » afin de garantir que l'accès autorisé est conforme aux responsabilités définies. Tous les employés sont tenus d'utiliser un identifiant unique pour accéder aux systèmes de l'entreprise.

Aircall applique une politique d'entreprise standard en matière de mots de passe. Cette politique exige que les mots de passe soient changés tous les 90 jours. Elle impose également une longueur minimale de 10 caractères pour les mots de passe, ainsi que des exigences de complexité, notamment des caractères spéciaux, des caractères majuscules et minuscules et des chiffres. Nous appliquons également l'authentification multifactorielle (par exemple, les clés de sécurité physique) et les solutions d'authentification unique.

Les autorisations sont régulièrement réévaluées (au moins tous les trimestres) pour veiller à ce qu'elles correspondent au rôle de l'employé.

Processus de résiliation

Aircall a mis en place un processus de résiliation par écrit, qui définit les responsabilités en matière de collecte des informations et de suppression des droits d'accès des membres du personnel lorsqu'ils quittent leurs fonctions au sein de l'entreprise.

Infrastructure des produits Aircall

Conditions environnementales et physiques

Notre fournisseur d'infrastructure dans le cloud est Amazon Web Services (AWS). AWS applique un programme de sécurité certifié, notamment par les normes PCI, ISO 27000 et SOC2. Les contrôles mis en place sont les suivants :

- Caméras de télévision en circuit fermé (TVCF)
- Agents de sécurité
- Alimentation électrique de secours
- Contrôle de la température et de l'humidité
- Détecteur de fumée
- Détection des fuites

Aircall n'héberge pas de systèmes informatiques dans ses propres bureaux.

Sécurité réseau

Aircall divise son système en réseaux séparés pour mieux protéger les données les plus sensibles et pour séparer les services publics des services internes. Les données des clients partagées avec Aircall ne sont admises que dans le réseau de production. Nous utilisons une combinaison de groupes de sécurité, de pare-feu, de systèmes de détection et de prévention des intrusions (IDS/IPS) et de pare-feu d'applications Web afin de protéger les données de vos clients.

Nous maintenons une approche « d'infrastructure en tant que code » pour la sécurité du réseau et les règles de pare-feu et nous disposons d'alertes pour toute divergence entre la configuration approuvée et les paramètres de production.

Continuité des activités et reprise après sinistre

Aircall a mis en place un processus de continuité des activités et de reprise après sinistre. Nos services s'appuient sur des zones de disponibilité AWS dans des régions géographiques physiquement séparées afin de faire preuve de réactivité, même en cas de panne d'un des sites. Notre plan de reprise après sinistre est mis à jour au moins une fois par an.

Notre objectif est d'isoler et de résoudre rapidement et de manière transparente tout problème qui affecte nos clients. Nous maintenons une page d'état de service Aircall **(https://status.aircall.io/)** qui est mise à jour jusqu'à la résolution du problème.

Sauvegarde et restauration

Des sauvegardes régulières sont effectuées quotidiennement et sont hébergées sur l'infrastructure du centre de données d'AWS. Les sauvegardes sont chiffrées à l'aide du chiffrement AES 256 bits. Des tests de restauration des sauvegardes sont effectués au moins une fois par an.

Chiffrement

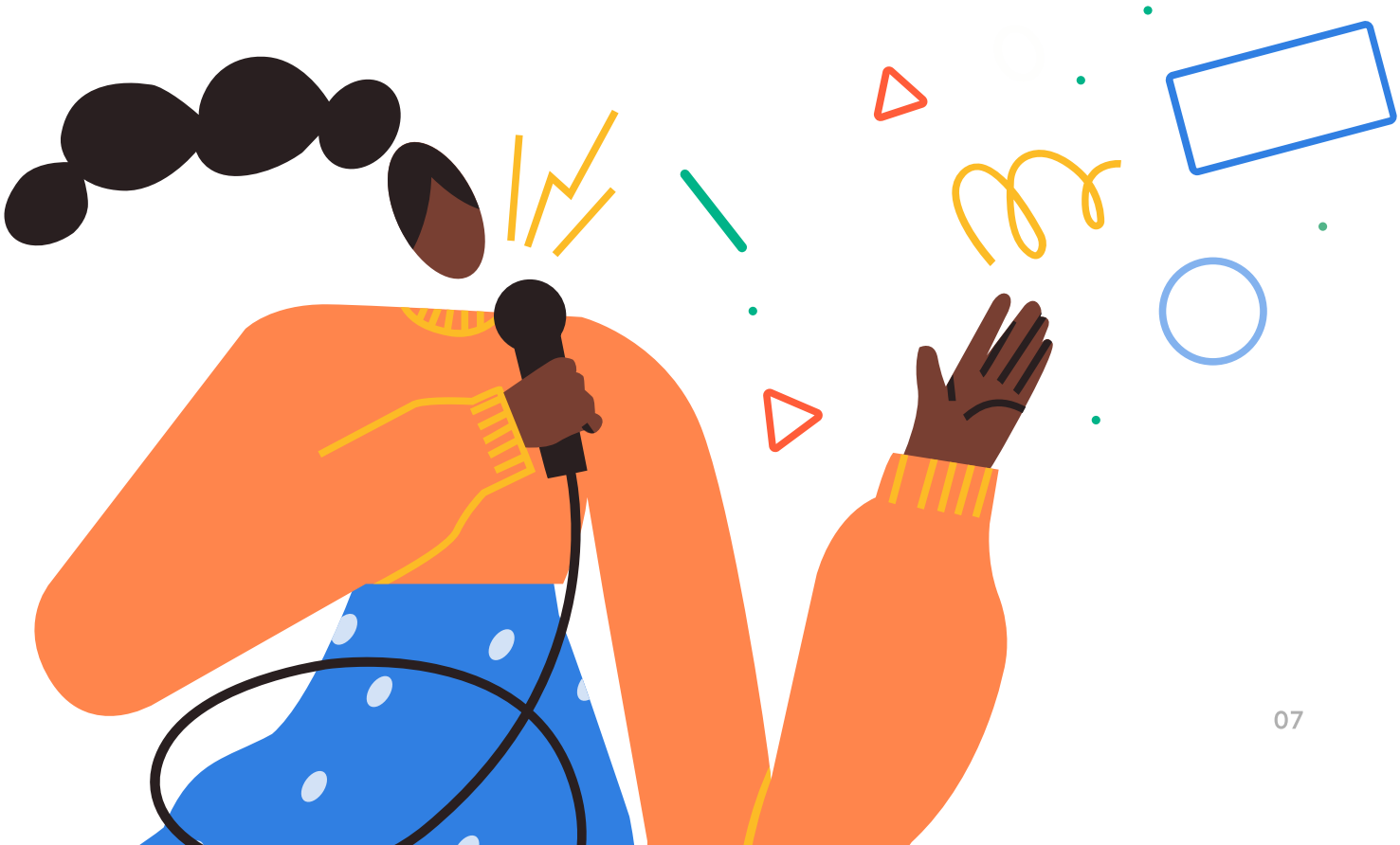
Aircall s'assure que toutes les données sensibles de ses clients en transit et stockées soient chiffrées en utilisant les normes du secteur TLS 1.2 et AES-256, respectivement. Notre équipe d'ingénierie utilise AWS KMS (Key Management Service). Toutes les clés sont gérées de manière centralisée par notre équipe de sécurité.

Surveillance

Aircall a mis en place des outils d'examen et de surveillance des registres afin d'identifier toute anomalie ou abus. Si un incident est détecté, l'équipe compétente l'examinera, mènera une enquête et appliquera des corrections.

Infrastructure mutualisée de cloud

Aircall offre un service mutualisé de cloud. Nos données clients sont logiquement séparées, ce qui signifie qu'Aircall vérifie que chaque utilisateur est autorisé à effectuer sa requête en vérifiant que la société de l'utilisateur correspond à celle des données d'entreprise demandées.



Sécurité des applications

Vulnérabilité et gestion des correctifs

Aircall a établi des processus pour effectuer des analyses périodiques de la vulnérabilité de ses systèmes informatiques. Les résultats sont saisis dans notre système de tickets, évalués en fonction du risque et de la priorité, et ajoutés à la liste des problèmes à résoudre. Tous les problèmes ou correctifs classés à haut risque sont résolus dans les 30 jours.

Tests d'intrusion

Aircall effectue des tests d'intrusion deux fois par an en ayant recours à des entités tierces indépendantes pour les tests d'intrusion au niveau des applications. Les menaces de sécurité et les vulnérabilités détectées sont classées par ordre de priorité, catégorisées et résolues rapidement. Les rapports sont disponibles sur demande et signés sous accord de confidentialité.

En outre, Aircall gère un programme de bug bounty (chasse aux bugs). Les chercheurs en sécurité indépendants sont invités à participer à l'identification de failles de sécurité dans les produits Aircall et sont récompensés pour leurs soumissions.

Gestion des changements

Aircall dispose d'un processus formel de gestion des changements pour administrer les modifications apportées à l'environnement de production des services, y compris toute modification de ses logiciels, applications et systèmes sous-jacents.

Tous les changements apportés au code source destiné aux systèmes de production sont soumis à un examen du code préalable par un pair qualifié en ingénierie, qui comprend une analyse de la sécurité, des performances et du potentiel d'abus.

Gestions des incidents

Aircall dispose de procédures établies pour la réception des rapports d'incidents de sécurité. L'équipe de sécurité Aircall dispose d'un processus établi de gestion des incidents. Celui-ci comprend :

- La connexion
- La catégorisation
- L'enquête
- La maîtrise
- Les enseignements tirés

Pour répondre à un incident, nous déterminons d'abord l'exposition des informations et l'origine du problème de sécurité, si possible. Nous communiquons avec le client (et tout autre client concerné) par e-mail ou par téléphone (si un e-mail ne suffit pas). Nous fournissons toutes les mises à jour périodiques nécessaires pour nous assurer de la bonne résolution de l'incident.

Si vous avez des inquiétudes concernant la sécurité ou si vous êtes au courant d'un incident, veuillez envoyer un e-mail à **report@aircall.io**.

Gestion des fournisseurs

Aircall applique un programme de gestion des fournisseurs afin de s'assurer que les contrôles de sécurité appropriés sont en place. Aircall évalue régulièrement chaque fournisseur (les fournisseurs critiques sont évalués au moins une fois par an) en tenant compte des normes de sécurité et de continuité des activités d'Aircall, y compris le type d'accès et la classification des données consultées (le cas échéant), des contrôles nécessaires à la protection des données et des exigences légales/réglementaires.

Aircall signe des accords écrits avec tous ses fournisseurs, y compris des obligations de confidentialité et de sécurité qui garantissent un niveau de protection adéquat pour toutes les données clients susceptibles d'être traitées par ces fournisseurs.

Sécurité de bout en bout

Tous les ordinateurs portables d'Aircall sont gérés de manière centralisée et sont entièrement chiffrés. Les utilisateurs finaux ne peuvent pas désactiver les logiciels antivirus ou toute autre fonction de sécurité.

Notre équipe informatique effectue des mises à jour régulières pour s'assurer que tous les appareils fonctionnent avec la dernière version du logiciel.

Conservation des données et sécurité

Aircall applique un programme de confidentialité. Vous pouvez en apprendre davantage au sujet de la confidentialité et de la conservation des données ici **(https://aircall.io/privacy-faqs/)**.