aircall

Security Overview

What's inside?

Introduction

Aircall takes Information Security and Compliance very seriously. This document is designed to help reassure our customers that their data is handled in a manner that meets their data protection and compliance requirements, and to provide full transparency and peace of mind for Aircall customers and assure them that their information is in good hands.

Our security controls and mechanisms are based on the ISO 27001 Information Security Standard and NIST Standards, which include programs covering: Policies and Procedures, Access Control, Business Continuity, HR Security, Network Infrastructure Security, Third-Party Security, Vulnerability Management, as well as Incident Response.

Security Organization

Aircall has a formal Information Security team that is responsible for all security matters in the organization.

Our security team holds a variety of certifications and other credentials that attest to their proficiency in the field.

Human Resources Security

Background Checks and NDAs

Aircall employees undergo an extensive third-party background check prior to formal employment offers, wherever local regulations and employment standards permit. All Aircall employees must sign non-disclosure agreements before gaining access to company systems or data.

Awareness and Training

Education is something that is central to an effective Information Security program; without it, the technical controls cannot effectively protect patient data and other sensitive information.

Every new employee must attend an information security training session during onboarding. This session aims to make the new staff member aware of their responsibilities and emphasize their role in providing protection against insider threats, ransomware, social engineering, proper use of assets, and other related issues.

After initial training, continuous training is provided through at least bi-monthly updates, notices, and internal communications.

Identification and Access Management

Aircall follows a formal process to grant or revoke access to its resources. System access is based on the concepts of “least-possible-privilege” and a “need-to-know” basis to ensure that authorized access is consistent with the defined responsibilities. All employees are required to use a unique ID to access company systems.

Aircall enforces an industry-standard corporate password policy. This policy requires passwords to change every 90 days. It also stipulates a minimum password length of 10 characters, along with complexity requirements, including special characters, upper and lowercase characters, and numbers. We also enforce Multi-Factor authentication (e.g. physical security keys) and single sign-on solutions.

Authorizations are periodically reviewed (at least every quarter) to ensure consistency with the employee job role.

Termination Process

Aircall has established a documented termination process that defines responsibilities for collecting information assets and removing access rights for staff members when they leave the service of the company.

Aircall Product Infrastructure

Physical and Environmental

Amazon Web Services (AWS) is our cloud infrastructure provider. AWS maintains an audited security program including PCI, ISO 27000, and SOC2. The controls in place are as follows:

- Closed Circuit Television Camera (CCTV)
- Security guards
- Backup power supply
- Temperature and humidity control
- Smoke detection alarm
- Leakage detection

Aircall does not host any product systems within its own offices.

Network Security

Aircall splits its system into separate networks to better protect more sensitive data and to separate public services from internal services. Customer data shared with Aircall is only permitted to exist within the production network. We use a combination of Security Groups, Firewalls, Intrusion detection, and prevention systems (IDS/IPS), and Web Application firewalls to protect your customer data.

We maintain a “configuration-as-a-code” approach for network security and firewall rules and have alerts for any discrepancies between the approved configuration and production settings.

Business Continuity and Disaster Recovery

Aircall has established a Business Continuity and Disaster Recovery process. Our services rely on AWS availability zones in physically separate geographic regions in order to remain resilient even if one location goes down. Our Disaster Recovery plan is updated at least annually.

Our goal is to quickly and transparently isolate and address any issue that impacts our customers. We maintain an Aircall status page **(https://status.aircall.io/)** which is subsequently updated until the issue is resolved.

Backup and Recovery

Regular backups are made daily and are hosted on AWS's datacenter infrastructure. The backups are encrypted using AES 256-bit encryption. Backup restore testing is conducted at least on an annual basis.

Encryption

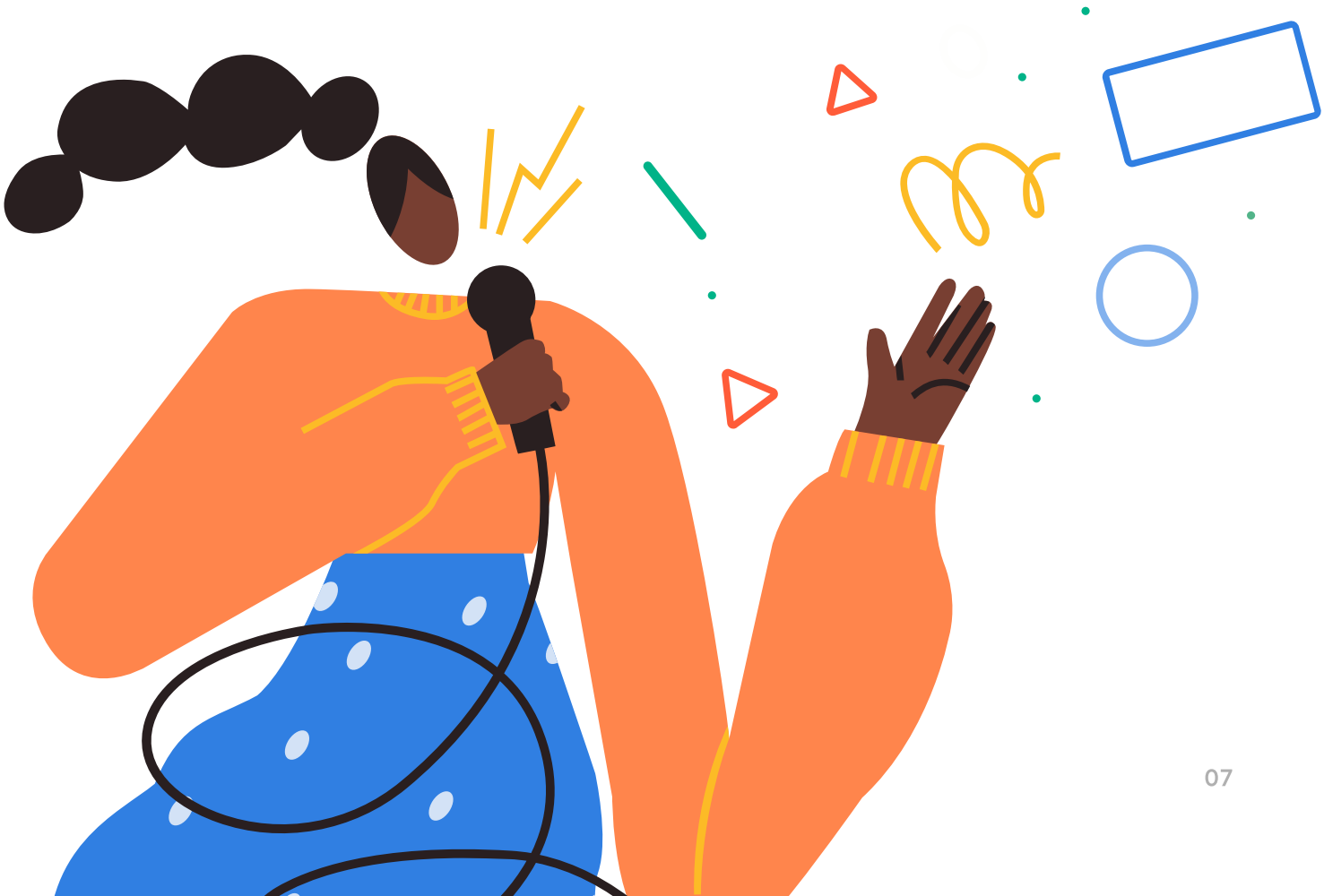
Aircall assures that all sensitive customer data is encrypted both in transit and at rest using industry standards TLS 1.2, and AES-256, respectively. Our engineering team uses AWS KMS (Key Management Service). All keys are centrally managed by our Security team.

Monitoring

Aircall has implemented logs review and monitoring tools to identify any anomalies or abuse. If an event is detected, the appropriate team will review, investigate, and apply corrections.

Multi-Tenant Cloud

Aircall is a Multi-tenant cloud service. Our customer data is logically segregated, which means Aircall checks that the user is authorized to perform the request by checking that the user's company is the same as the requested data's company.



Application Security

Vulnerability and Patch Management

Aircall has established processes for performing periodic vulnerability scans of its IT systems. The results are populated into our ticketing system, evaluated by risk and priority, and added to the backlog for resolution. All issues or patches classified as high risk are resolved within 30 days.

Penetration Test

Aircall performs penetration tests twice a year using independent third-party entities to conduct application-level penetration tests. Security threats and vulnerabilities that are detected are prioritized, categorized, and resolved promptly. Reports are available upon request and signed under NDAs.

In addition, Aircall manages a bug bounty program. Independent security researchers are invited to participate in identifying security flaws in the Aircall products and are rewarded for their submissions.

Change Management

Aircall has a formal change management process to administer changes to the production environment for the services, including any changes to its underlying software, applications, and systems.

All changes to source code destined for production systems are subject to pre-commit code review by a qualified engineering peer that includes security, performance, and potential-for-abuse analysis.

Incident Response

Aircall has documented procedures for receiving security incident reports. The Aircall Security team has a documented incident response process which includes:

- Logging
- Categorization
- Investigation
- Containment
- Lessons Learned

In responding to any incident, we first determine the exposure of the information and determine the source of the security problem, if possible. We communicate back to the customer (and any other affected customers) via email or phone (if email is insufficient). We provide periodic updates as needed to ensure that the incident is resolved appropriately.

If you have any security concerns or are aware of an incident, please send an email to **report@aircall.io**.

Vendor Management

Aircall maintains a vendor management program to ensure that appropriate security controls are in place. Aircall periodically reviews each vendor (critical vendors are reviewed at least once a year) in light of Aircall's security and business continuity standards, including the type of access and classification of data being accessed (if any), controls necessary to protect data, and legal/regulatory requirements.

Aircall enters into written agreements with all of its vendors, including confidentiality and security obligations that provide an appropriate level of protection for any customer data that these vendors may process.

Endpoint Security

All Aircall laptops are centrally managed and fully encrypted. The end users cannot disable antivirus software or any security features.

Our IT team pushes updates periodically to ensure that all devices are running with latest software version.

Privacy and Data Retention

Aircall maintains a Privacy Program. You can learn more about privacy and data retention here **(https://aircall.io/privacy-faqs/)**.