aircall

Security White Paper

Revision : October - 2025

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.

Office Physical Security

Aircall implements a multi-layered security approach to ensure employee safety across its global locations. Secured access control systems utilize individual badges that are automatically deactivated upon loss, employee termination, or infrequent use. Additionally, video surveillance and other preventative measures are in place throughout Aircall's offices worldwide.

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 periodic updates, notices, and internal communications.

Aircall not only provides general awareness training but also conducts phishing awareness training and simulations multiple times throughout the year.

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 a minimum password length of 13 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), session time-out, and single sign-on solutions.

Authorizations are periodically reviewed to ensure consistency with the employee’s 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.

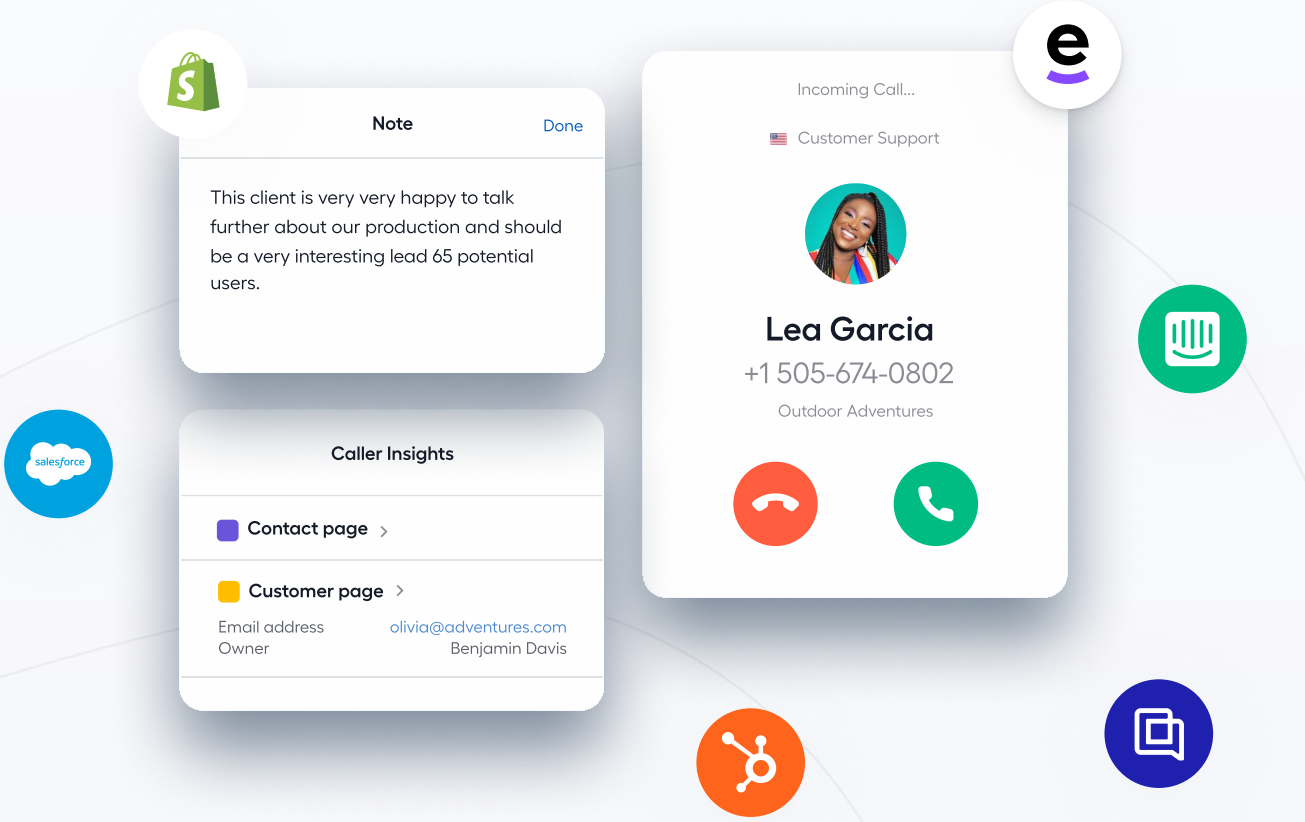
Access to Production Infrastructure

Access to Aircall's internal data stores and production infrastructure is limited to the Corporate device and requires connection through the Virtual Private Network (VPN) with phish-resistant Multi-factor Authentication (MFA). User access is meticulously regulated, with Aircall employees gaining entry based on a role-based access control (RBAC) model.

Routine access is restricted to the Engineering team members, and continuous administrative access is carefully monitored.

In cases of temporary or emergency access to administrative functions (such as alert responses or troubleshooting), the Aircall system employs a Just-In-Time-Access (JITA) model.

This model grants users privileged access for a specific duration and undergoes review by a Senior Engineering member (Director level or above).



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.

Backup and Recovery

Regular backups are made daily and are hosted on different region in AWS's data center 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.

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 our customer data.

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 (Aircall Status) which is subsequently updated until the issue is resolved.

The Disaster Recovery strategies and our recovery procedures are therefore designed to guarantee a 4-hour recovery point objective (RPO) and a 12-hour recovery time objective (RTO) for a major incident.

Logging and Monitoring

Aircall keeps a detailed log of everything that happens within service. This information is securely stored in a central location within Aircall's AWS environment. Security logs are especially important, so they're indexed and kept for longer periods to help us investigate and respond to any issues quickly.

Aircall leverages proactive incident management to ensure service continuity. Our SIEM is constantly monitored for anomalies, such as unexpected error spikes, potential security breaches, or malicious activity in our systems. When an incident is detected, our engineers and administrators are automatically notified through our incident management tool. This triggers a well-defined response plan, enabling swift investigation, resolution, and service restoration.

Tenant Separation

Aircall offers a highly scalable, multi-tenant SaaS solution that ensures logical separation of customer data by utilizing unique IDs to link data and objects to individual customers.

Application Security

Aircall has adopted a DevSecOps approach, integrating security into every stage of the Software Development Life Cycle. This shift has enabled early detection of security risks, and introduced a culture of shared responsibility for security. The result is a more secure, efficient, and collaborative development process.

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 once 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.

Security Gates

In addition to the pre-commit code review, all code undergoes Static Application Security Testing (SAST) and Software Composition Analysis (SCA). SAST and SCA help identify potential vulnerabilities in the code and its libraries while Security Gates prevent any critical vulnerabilities from being deployed to production.

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**

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

Privacy and Data Retention

Aircall maintains a Privacy Program. You can learn more about privacy and data retention here : **(Privacy FAQs | Aircall).**

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. All laptops are also protected by an endpoint Detection and Response (EDR) solution.

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

Compliance

To ensure the highest level of security for your data, Aircall undergoes annual SOC 2 Type 2 audits. This independent verification confirms the effectiveness of our controls that safeguard your information. These controls align with industry-leading Trust Service Principles (TSPs) set by the AICPA.