Information Security

Whitepaper

August 2020

Airbo

Abstract

Airbo provides an engaging, cloud-based Employee Communication Platform — Virtual Fairs plus Year-Round Benefit Communications — to a wide variety of organizations and industries since 2011. We maintain the trust of our clients, from public school districts to Fortune 500 enterprises, adhering industry-standard security management without compromising functionality or ease-of-use.

This whitepaper examines information security at Airbo:

Internal Policies and Procedures

Hardware Security

Airbo is a forward-thinking, completely cloud-based company — both our internal systems as well as our client-facing systems. We do not maintain physical infrastructure other than company issued laptops.

Airbo-issued laptops are required to be password protected with cryptographically-strong passwords changed at interval. When required, client information is downloaded to a password protected, encrypted partition.

Personnel

In addition to thorough reference checks, Airbo also conducts full criminal background checks on all employees as part of our hiring process. All Airbo employees are provided comprehensive training on security standards and policies as well as industry best practices regarding information security.

Separation of Concerns and Access

Airbo restricts access to resources based on functional roles:

1. All engineers have reference access to source code
2. Non-privileged engineers are restricted to development and QA environments with test data fixtures
3. Designated engineering team members can author changes
4. Pre-approved team leads can affect production

Non-Technical Business Access

All non-technical information access (client contracts, communications, personnel data and financials) is restricted to only those whose roles require access.

Third-Party and Vendor Services

As Airbo is completely cloud-based, we take tremendous care to partner with and procure services from industry-leading providers of Paas, IaaS and SaaS hosting. Our partners exhibit extensive expertise in information security management and have adopted the most stringent industry standards, certifications such as SSAE16 & ISO 27001.

Airbo works closely with both vendors and partners, ensuring best practices are followed:

- Enforcement of secure login and password storage for access to vendor and external interfaces A, C
- Enforcement of MFA/2FA, cryptographically-hardened passwords: 12-char min., alpha+numeric+special and no reuse
- Role-based Access Control with least privileges granted
- Rotation of administrative passwords every 60 Days
- Prompt application of all vendor recommended software updates and patches related to security A, B, C, *D*

Physical Security

Incoming Employees

All Airbo employees are screened prior to employment with checks:

- Six (6) years address history
- Three (3) years employment history
- Education Verification
- Criminal background checks

Airbo employees with authorized access to production and test environments are further screened prior to access being granted.

Outgoing Employees

Upon termination of employment, the departing employee's access to all Airbo resources and systems is immediately blocked:

- Revoke, disable or remove all system and accounts associated with the employee (including databases, code repository, application)
- Change administrator passwords in all systems to which the employee had access
- Disable employee access to email but keep the account active to monitor any security-related communications

Logical Security

Secure Development

All of Airbo's services are engineered with stringent OWASP-derived practices for change-management. Airbo's engineering team subscribes to industry mailing lists [F], scans all code on every change for quality, security and implements recommended security [D G] patches within 24 - 48 hours to mitigate vulnerability exposure. [E] Penetration testing is with our partners at re and Amazon. [A, C]

External Platform Protection

Airbo partners with industry leaders in PaaS and IaaS infrastructure, organizations with well-established, 3rd-party-audited governance programs in place. [A, C] They adhere to the most stringent security management methodologies and standards such as ISO 27001, AT101, and SSAE16.

Data In Transit and At Rest

Airbo encrypts all customer data in a secure database (AES-256) and protects all data in-transit with the HTTPS/TLS 1.3 protocol, utilizing strong AES ciphers capable of up to 256 bits.

Disaster Recovery and Business Continuity

Airbo maintains 7 days of continuous rollbacks with a month follower, in arrears. Redundancy and high-availability is achieved with auto-scaling of Heroku instances. Our business continuity and recovery plans are audited continuously and tested monthly.

Customer Security

Separation of Concerns

Airbo's services are multi-tenanted and follow stringent security that ensures no information disclosure is permitted between customers.

Secure Customer Management

Airbo uses RBAC architecture to restrict user access to resources. Access is granted on a "least privilege" basis. There are four types of roles, each with specific privileges:

1. *Guest Users* — view content at a public URL on the airbo.com domain. While Airbo does not track this user, a cookie is added to remember subsequent sessions.
2. *Ordinary Users* — view content and alter their own information.
3. *Client Administrators* — are designated as administrators to create content, send digest emails to groups, add new users and designate other *Ordinary Users* to be *Client Administrators*.
4. *Site Administrators* — are Airbo staff acting as *Client Administrators.* Additionally, they can switch between any instance to access additional reporting.

Further separation is applied to critical operations, such as deletion of a client instance, which requires C-level password approval.

HIPAA / California's CCPA / GDPR

Electing not to collect Personal Health Identification (PHI), Airbo maintains compliance. For other data, confidentiality, privacy and ownership of information is maintained. Access must be granted explicitly.

Secure Use of Service

Airbo users are provided with the knowledge of how to best implement and manage the product to ensure content remains accessible and available on a need-to-know basis achieved through:

- Customer Success Managers
- Extensive online help
- Live online support portal

Identity and Authentication

Airbo users authenticate with their username and password to access non-public features of the website. In certain scenarios, authenticated users with a non-expired session can access Airbo via a randomly-generated authentication token attached an email link.

Audit Information and Provision to Customers

Airbo provides reports that detail usage and access to all content stored in its services.

Appendix

Vendor Security

A. Heroku Security Policy (division of SalesForce)

B. Compose Security Policy (division of IBM)

C. Amazon Web Services ISO 27001 Certification

Code Analysis and Vulnerability Detection

D. Code Climate

E. NIST Computer Resource Center

F. Ruby on Rails Security

G. GauntIt