Ashby Security Overview

Introduction

Recruiting and HR data is critical to your business and we take the security of customer data extremely seriously. We host Ashby using comprehensively hardened infrastructure-as-a-service (IaaS) platforms from Heroku and Amazon Web Services.

Ashby is SOC2 compliant and Type 2 audited annually. Our SOC2 report is available to customers upon request.

Product Security

Authentication

Ashby only allows authentication from Google Workspace (formerly GSuite) and Office 365 corporate accounts. Ashby does not store any passwords.

Permissions

Ashby supports flexible permission levels for teammates. Permission levels can be set globally or within specific departments, jobs, and other organizational data.

Physical Security

Ashby production data is processed and stored within world-renowned data centers that use state-of-the-art multilayer access, alerting, and auditing measures.

System Security

Servers and Networking

All Ashby servers and structured datastores use managed infrastructure services provided and secured by Heroku.

Our web servers encrypt data in transit using the industry standard for HTTPS security (TLS 1.2) so that requests are protected from eavesdroppers and man-in-the-middle attacks. Our SSL certificates are 2048 bit RSA, signed with SHA256.

Storage

All persistent data is encrypted at rest using industry-standard AES-256 algorithms.

Operational Security

Policies

Ashby has developed a comprehensive set of security policies covering a range of topics. These policies are updated frequently and shared with all employees.

Employee Training

All Ashby employees are trained on security best practices and awareness during onboarding. We perform annual disaster recovery and data restoration tests.

Employee Equipment

All employee computers have strong passwords, encrypted disks, and virus scanners. No Windows computers or servers are used at all other than in isolated testing environments.

Employee Access

We use Google account infrastructure to verify employee account identity and require two-factor authentication for apps that access critical infrastructure or customer data.

Access to administrative interfaces additionally enforce administrator permissions where applicable, and all administrative access is logged and auditable both in the form of traditional web server logs and session recordings to make it easy to find and review any administrative activities with full fidelity.

All employee contracts include a confidentiality agreement.

Code Reviews and Production Deployment

All changes to source code are subject to automated testing and any that affect security require pre-commit code review by a qualified engineering peer that includes security, performance, and potential-for-abuse analysis.

All code is deployed to a staging environment for quality assurance and automated tests must pass prior to updating production services.

Service Levels, Backups, and Recovery

Ashby infrastructure utilizes multiple and layered techniques for increasingly reliable uptime, including the use of load balancing and task queues. Ashby uses highly redundant datastores, rapid recovery infrastructure, and point-in-time backups making unintentional loss of customer data very unlikely.

Application Security

Server and Client Hardening

Ashby servers use Heroku managed infrastructure which utilize firewalls to restrict system access from external and internal networks, DDoS mitigation, spoofing and sniffing protections, and port scanning. Request-handling code paths have frequent user re-authorization checks, payload size restrictions, rate limiting where appropriate, and other request verification techniques. All requests are logged and searchable by operations staff.

Client code utilizes multiple techniques to ensure that using the Ashby app is safe and that requests are authentic, including XSS and CSRF protection, signed and encrypted user authentication cookies, and session expiration.

Pentests

We engage third-party security experts to perform detailed penetration tests on the Ashby app and infrastructure.

API and Integrations

Access to the Ashby RPC API endpoints requires an access key that can be regenerated on demand by customers.

Integrations with other apps are all opt-in and authenticate via OAuth or other applicable mechanisms required by the third party app. Integrations can be disabled at any time.

Customer Payment Information

We use Stripe for payment processing and do not store any credit card information. Stripe is a trusted, Level 1 PCI Service Provider.

Incident Reporting

Incident Response

Ashby implements a protocol for handling security events which includes escalation procedures, rapid mitigation, and post mortem. All employees are informed of our policies.

Responsible Disclosure

Ashby has a Responsible Vulnerability Disclosure program. You can read more details about our program, the rules of engagement, and how to submit vulnerability reports at https://www.ashbyhq.com/disclosure.

If you have a security concern, question, or are aware of an incident, please send an email to security@ashby.com, a carefully controlled and monitored email account.