



Information Security Overview

June 13, 2025

Fastr.ai Information Security Overview

At Fastr.ai, security is not an afterthought — it is architected into every layer of our platform. This document provides an overview of the technical and organizational controls we employ to protect customer data. Fastr.ai undergoes independent SOC 2 Type II and ISO 27001 certification audits annually.

Architectural Security

Data Processing

Fastr.ai acts as the data processor; our customers remain the data controller at all times. Our AI platform operates exclusively on non-sensitive recruiting data, transmitted via secure APIs from the customer's Applicant Tracking System (ATS) with prior customer authorization. Data is limited to general candidate and job information required to deliver the service.

Data transferred from the customer's ATS to Fastr.ai does not include candidate-facing information and contains no personal data beyond what the customer has explicitly defined and authorized for transfer, strictly for the purpose of providing and supporting Fastr.ai services.

Data Location

All customer data is hosted on Fastr.ai's Microsoft Azure secure cloud infrastructure, including application servers, processing environments, and file storage services housed within secure Azure Virtual Networks (VNETs). Fastr.ai hosts customer data in a US-based Azure region (East US).

Data Residency

Customer data is hosted exclusively within US-based Microsoft Azure data centers. Data does not leave the designated region without explicit customer consent.

Data Protection

All customer data is encrypted at rest using AES-256 and encrypted in transit using HTTPS/TLS 1.2+ across all public network communication. Backup data is stored in encrypted Azure Blob Storage containers. Encryption keys are managed through Azure Key Vault, leveraging FIPS 140-2 validated hardware security modules (HSMs).

Data Segmentation

Each customer's data is maintained in a dedicated, isolated database. Every system request requires authentication with individual credentials and authorization verification. Data processing within Fastr.ai's platform is logically segregated per customer using business-layer implementation rules and controls.

Disaster Recovery

Fastr.ai maintains a documented Business Continuity and Disaster Recovery (BCDR) Plan to ensure continued delivery of critical services in the event of a disruption. The BCDR Plan is reviewed and updated on an annual basis. In the event of a disaster, Fastr.ai personnel follow defined escalation and response procedures aligned to their roles in the BCDR Plan, ensuring coordinated and effective recovery activities.

Access to Data

Customer environments reside within Azure VNets and are accessible only via two-factor authentication (2FA) VPN. Access is restricted to authorized Fastr.ai personnel with a demonstrated operational need. All access events are logged and subject to regular audit review.

Access privileges are granted on a Just-In-Time (JIT) basis for specific, time-bound needs and are revoked automatically upon task completion.

Network & Data Security

Fastr.ai's application servers reside within secure Azure VNets and are protected through a layered security model combining Azure Firewall, VPN gateways, OS-level hardening, database management system controls, and application-layer security. Continuous monitoring and intrusion detection systems are deployed across the environment.

Database servers are isolated within internal subnets with no direct internet exposure. Only explicitly authorized servers are permitted outbound internet access, and all traffic is filtered through firewall policy.

Logging & Monitoring

All Fastr.ai information systems generate automatic, event-driven logs. Logging is triggered by defined security events including, but not limited to, detections from our Intrusion Detection and Prevention System (IDS/IPS), anti-virus engines, and anti-spyware systems. Logs are centralized and retained in accordance with our data retention policy.

Logical Security

Fastr.ai enforces a comprehensive logical security strategy combining multiple access control mechanisms at both the individual and team levels to protect customer and proprietary data.

Role-Based Access Control (RBAC)

Access to Fastr.ai systems and information assets is granted on a strict need-to-know, need-to-use basis. Employees are not granted access to any resource that is not directly required to perform their job function. Fastr.ai maintains a defined set of user roles aligned to organizational positions and responsibilities, which are reviewed and updated continuously. Each employee is assigned a role and receives only the permissions associated with that role.

Network Segmentation

Fastr.ai's Azure VNet architecture implements logical network segmentation. Network segments communicate only through controlled firewall pathways and are not directly interconnected. Azure Firewall and Network Security Groups (NSGs) enforce strict traffic policies, permitting only authorized communications between segments and preventing lateral movement in the event of a breach.

Security & Privacy Awareness Training

Fastr.ai employees complete mandatory security and privacy awareness training upon onboarding and on a recurring annual basis. Training covers data handling procedures, phishing awareness, incident reporting, and adherence to Fastr.ai's security policies. Completion is tracked and enforced at the organizational level.

Physical Security

Fastr.ai does not operate physical data center infrastructure. All server environments are hosted on Microsoft Azure, which maintains SOC 2, ISO 27001, and FedRAMP-certified facilities with rigorous physical access controls, 24/7 security staffing, biometric access restrictions, and comprehensive surveillance.

Application Security

Encryption

All customer data is encrypted at rest using AES-256 and encrypted in transit via HTTPS/TLS 1.2+. Backup data is stored in encrypted Azure Blob Storage. Encryption key lifecycle management is handled through Azure Key Vault, which uses FIPS 140-2 validated HSMs to protect key material.

Penetration Testing

Fastr.ai conducts application-level and network-level penetration tests at least annually, performed by qualified third-party security firms. Application code is additionally subject to automated security testing pipelines, including recurring static application security testing (SAST). An executive summary of the most recent penetration test is available to customers upon request under NDA.

Vulnerability Management

Fastr.ai employs continuous automated vulnerability scanning tools across our production environment. Identified vulnerabilities are triaged, prioritized by severity, and remediated within defined SLA windows. Findings and remediation status are tracked through our internal security management platform.

Endpoint Security

All company-issued devices are protected by centrally managed endpoint security software, including antivirus and endpoint detection and response (EDR) capabilities. Security definitions and agent updates are applied automatically. Device compliance is enforced as a condition of accessing Fastr.ai corporate systems.

Infrastructure Change Management

Fastr.ai maintains a disciplined change management process for all modifications to its Azure production environment, balancing the need for agility with the imperative to protect system stability and customer data.

Software Development Lifecycle (SDLC)

All code and infrastructure changes follow Fastr.ai's formal SDLC, which includes design review, peer code review, security review, functional testing, and management approval phases prior to deployment. Automated security gates — including black box testing and static code analysis — are embedded throughout the pipeline to identify and mitigate risk before changes reach production.

Change Tracking & Governance

All change activity is tracked and maintained within Fastr.ai's change management system, providing a complete audit trail of requests, approvals, and deployments. Regular metrics reports are issued to the Management Team, providing key performance indicators for the change process. Risk assessments tied to each change are communicated to relevant stakeholders through the management reporting framework.

Availability Procedures

Production Monitoring

Fastr.ai's production environment is managed entirely within Microsoft Azure and is monitored around the clock by the Fastr.ai Technical Operations team using automated observability tools. Alert policies are configured to notify relevant team members via our internal incident communications platform based on predefined severity thresholds. Alerts are triaged and escalated by the Operations and Support team according to documented urgency tiers.

The production environment spans multiple components including API services, application servers, data processing layers, database clusters, monitoring infrastructure, and network components delivered through Azure Virtual Network services.

Backup

Full backups of Fastr.ai's production environment are performed on a daily basis. Backup integrity is validated through automated verification procedures.

Disaster Recovery Plan

Fastr.ai has developed a comprehensive Business Continuity and Disaster Recovery (BCDR) Plan to continue providing critical services in the event of a disaster. The BCDR Plan is reviewed, updated, and tested on an annual basis. In the event of a disaster, Fastr.ai personnel are directed in the company's response and participate in recovery activities based on their respective roles and responsibilities in accordance with the Fastr.ai BCDR Plan.

Recovery Objectives

Fastr.ai maintains defined Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) as part of its BCDR Plan, reviewed and tested annually.

Compliance & Certifications

Fastr.ai's security program is aligned to internationally recognized frameworks and subject to independent third-party validation on an annual basis.

Certification	Details
SOC 2 Type II	Audited annually and reports are available to customers under NDA upon request.
ISO 27001	Annual certification audit against the international standard for information security management systems (ISMS).
Azure Cloud Infrastructure	Fastr.ai's hosting provider, Microsoft Azure, maintains SOC 2, ISO 27001, and FedRAMP certifications for its US data center operations.

Third-Party Subprocessors

Fastr.ai engages subprocessors only where required to deliver services to customers. All third-party service providers are subject to rigorous vendor evaluation prior to onboarding, including assessment of their security posture, data privacy practices, and contractual obligations.

Security and privacy requirements are incorporated into all subprocessor agreements. Fastr.ai maintains an up-to-date list of subprocessors, which is available to customers upon request.

Subprocessor List

Customers may request Fastr.ai's current Subprocessor List by contacting their account representative or emailing infosec@fastr.ai.

For questions or additional technical details, contact your Fastr.ai account representative.