Chatley AI, Inc.

Security Overview

Enterprise-grade security at every layer of the Chatley AI platform

Trust Center Document | Public
April 2026
chatley.ai/trust-portal

Chatley AI's voice infrastructure runs on a SOC 2 Type II certified platform. Chatley AI's application layer is currently in SOC 2 Type II readiness.

1. Introduction

At Chatley AI, trust is the foundation of our relationship with our customers. This document provides an overview of the security program implemented to protect your data and ensure the integrity and availability of the Chatley AI platform. Our security architecture is built on three layers — each with independently verified controls and clear ownership.

2. Platform Architecture

The Chatley AI platform is composed of three distinct infrastructure layers:

Application Layer	Managed by Chatley AI, Inc. Includes the customer-facing dashboard, API, agent configuration, and da
Voice Infrastructure Layer	Managed by our certified voice infrastructure provider. Handles all real-time voice AI processing includi
Telephony Layer	Managed by our certified telephony provider. Handles PSTN call routing, SIP trunking, and SMS. Holds

3. Security Governance

Chatley AI's security program is overseen by an advisory CISO (Ernesto Feliciano) who conducts quarterly security reviews and an annual deep review of all security documentation and controls. The engineering team (led by Hamza Baig) owns day-to-day security operations including the DevSecOps pipeline, access management, and incident response.

4. Application Security

Secure Development Lifecycle

Security is integrated into every phase of the development lifecycle through an automated DevSecOps pipeline:

- • Static Application Security Testing (SAST) via Semgrep runs on every pull request — Critical and High findings block merge
- • Secrets detection via GitLeaks scans every commit — any credential pattern triggers immediate remediation
- • Software Composition Analysis (SCA) monitors third-party dependencies for known CVEs
- • AI-assisted code review (Rover AI) provides an additional security-focused review layer
- • Multi-stage deployment: Dev → Test → Production with manual approval gate for all production deployments

Vulnerability Management

Formal remediation SLAs: Critical vulnerabilities within 24 hours; High within 7 days; Medium within 30 days. Annual third-party penetration testing is conducted. Penetration test executive summaries are available to enterprise customers under NDA.

5. Infrastructure Security

Network Security

- • All customer-facing traffic routes through Cloudflare WAF with OWASP Top 10 rulesets active
- • DDoS protection at Layers 3, 4, and 7 via Cloudflare
- • Internal operations infrastructure is not accessible from the public internet — all administrative access routes through Tailscale Zero Trust mesh network (WireGuard-based)
- • UFW host firewall with default-deny inbound policy on all internal servers
- • SSH access requires cryptographic key authentication — password-based SSH permanently disabled

Cloud Infrastructure

The Chatley AI application layer is hosted on Amazon Web Services (AWS). AWS maintains SOC 2 Type II, ISO 27001, and PCI DSS certifications for its infrastructure. Chatley AI inherits these physical and network security controls at the infrastructure layer.

6. Data Protection

Encryption

In Transit	TLS 1.2 minimum across all communication paths. TLS 1.3 supported. All paths between the caller, ou
At Rest	AES-256 encryption for all data stored in the Chatley database.
Backups	AES-256 encryption. Backup keys stored separately from data.

Access Controls

- • Multi-factor authentication mandatory for all administrative access to production systems
- • Role-Based Access Control (RBAC) — principle of least privilege enforced
- • All access reviewed quarterly — inactive and over-provisioned accounts remediated
- • All access revoked within 2 hours of employee or contractor departure
- • All secrets (API keys, credentials) stored in Bitwarden Enterprise — zero-plaintext policy enforced

7. Compliance Posture

Framework	Status	Notes
SOC 2 Type II	Infrastructure: Certified App layer: Readiness	Voice infrastructure certified via Voice infrastructure provider (active). Application layer in r
HIPAA	Supported	HIPAA-compliant deployments via our certified voice infrastructure. BAA available. Requir
PCI DSS	Supported	Our voice infrastructure holds PCI DSS Level 1 certification. Requires correct implementat
GDPR	Ready	DPA available at chatley.ai/dpa. Subprocessor registry at chatley.ai/subprocessors.
CCPA	Compliant	Consumer rights supported. Data not sold to third parties.

8. Incident Response

Chatley AI maintains a formal Incident Response Plan based on the SANS Institute six-phase methodology. Enterprise customers are notified within 72 hours of Chatley AI becoming aware of a Personal Data Breach affecting their data. For security incidents, contact: security@chatley.ai