Security Overview

Effective date: June 16, 2026

At Cerberus AI, Inc. (“Cerberus”) we take the security of your data seriously. This Security Overview describes the technical and organizational measures we use to protect the customer data we hold and the systems that process it. It is maintained by our Security and Compliance function and updated to reflect our current practices.

Encryption

Data moving between users and our services is protected with TLS 1.3 or higher. Data stored in our systems is encrypted at rest using AES-256. Encryption keys are managed through our cloud provider’s key management service.

Infrastructure Security

Our infrastructure runs on Google Cloud Platform (GCP), which maintains leading physical and environmental security controls across its data centers. We rely on GCP’s certified facilities for physical security and isolate our environments using private networking, firewalls, and security groups. Systems are continuously monitored, and we apply security patches on a regular cadence.

Access Control

Access to customer data and production systems is restricted to authorized personnel on a least-privilege, need-to-know basis. We enforce multi-factor authentication (MFA), use role-based access controls, and review access rights periodically. Access is granted when an employee’s role requires it and revoked promptly when it no longer does.

Secure Development Practices

Security is built into our development lifecycle. Code changes undergo review before being deployed, and we maintain separate development, and production environments. We use automated testing and dependency scanning to identify and remediate vulnerabilities early.

Incident Response

We maintain a documented incident response plan that defines how we detect, investigate, and respond to security events. Our team monitors for anomalous activity, and in the event of a confirmed incident affecting customer data, we will notify affected customers in accordance with applicable law and our contractual commitments.

Compliance

Cerberus is currently undergoing a SOC 2 Type II examination, which independently evaluates the design and operating effectiveness of our security controls over time. We continuously monitor our control environment to maintain our security posture. Updates to our compliance status will be reflected here as they become available.

Security Practices at a Glance

Area	Our Approach
Encryption in transit	TLS 1.3
Hosting	Google Cloud Platform (GCP)
Access control	Least-privilege, MFA, periodic review
Secure development	Peer review, environment separation, dependency scanning
Incident response	Documented plan with customer notification
Compliance	SOC 2 Type II in progress

Contact Information

If you have any questions about our security practices, please contact us at contact@cerberussecurity.ai or visit https://cerberussecurity.ai/security. This document is reviewed and maintained by the Cerberus Security and Compliance function.