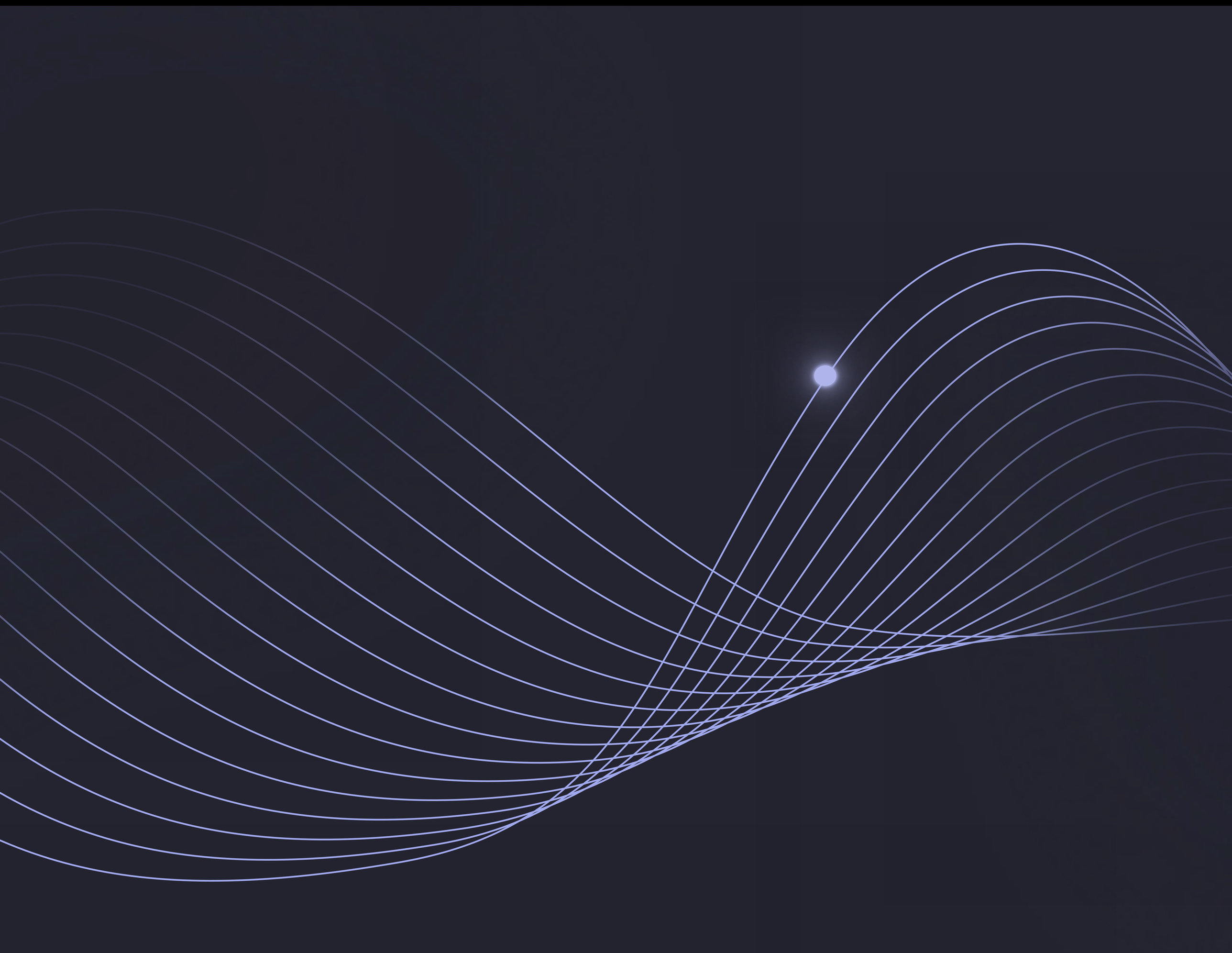
collate

Enterprise Security Overview

Last Update: March 24, 2025



Data Protection and Encryption

- All Documents are encrypted at rest. Documents are encrypted using AES-256.
- All interactions with Collate servers occur over HTTPS and are thus encrypted in transit. Collate enforces TLS v1.2+ for all Document retrieval operations.
- All interactions with Collate internal document control servers occur via Collate's web application backend. Document control servers are not publicly visible and only accept requests from Collate's web application backend and Collate's internal AI servers.
- All Documents reside within Collate's private VPC. Documents cannot be accessed outside of Collate software itself as they are not on a publicly visible network.

Third Party Data Retention

- OpenAI and Anthropic AI interactions have a zero day retention policy. No documents or embeddings we send to either provider will be retained on their servers.

Authentication

- Every user interacting with Collate must be authenticated. No operations can be performed for an unauthenticated user, and no user will be authenticated without first being added to the customer's installation by Collate support.
- Collate supports username-password authentication. Additional authentication methods (MFA/Passkey/SSO) will be added in the near future.

Authorization

- Collate provides an Admin access role for current users. Fine-grained authorization and access roles are on our near term roadmap.
- Document actions, such as approvals, release of documents, obsoletion of documents, and trainings are authorized to individual users.