ORYELE DOCUMENTATION

Security and Compliance

Protect your firm's data with enterprise-grade encryption, governance controls, and compliance tooling.

This guide covers data encryption at every layer, legal hold for litigation and audit preservation, audit trail exports in CSV format, and multi-factor authentication configuration.

Property of Oryele LLC All rights reserved.

Data Encryption

Oryele uses industry-standard encryption at every layer of the platform to protect your firm's data and your clients' information.

Layer	Encryption Standard	Details
Data in Transit	TLS 1.3	All API traffic, web sessions, and integration connections
Data at Rest	AES-256	Database records, backups, and file attachments
File-Level Encryption	AES-256-GCM	Individual documents encrypted with per-file keys
Key Management	AWS KMS	Keys rotated automatically every 90 days
Backups	AES-256	Daily, in the same AWS region, kept for 35 days

Legal Hold

Legal Hold prevents any content from being modified, deleted, or overwritten for the duration of a litigation, investigation, or audit. Content under hold is preserved exactly as it exists at the moment the hold is applied.

Applying a Legal Hold

- Open a client record and use the Legal Hold control to place an account-level hold - every document belonging to that client is immediately blocked from deletion or archiving.
- Enter a reason (required) and optional notes.
- The hold is logged in the audit trail with the applying user's identity and timestamp.

Managing Active Holds

- View a client's hold history - including who placed and released each hold, and when - from that client's record.
- Holds do not have expiry dates. They must be explicitly released.
- Only users with the ADMIN, SUPER_ADMIN, or MANAGER role can place or release a legal hold.
- When a hold is released, the client's documents return to the standard retention policy timeline immediately.

Important	Placing a legal hold does not create a separate copy of the data. It prevents the original records from being altered or removed. Always apply holds promptly when litigation is reasonably anticipated.

Exporting Audit Trails

Audit trails can be exported to CSV for regulators, external auditors, or internal compliance review.

Exporting in CSV Format

- Go to Audit Log and click Export CSV to download the events currently displayed on screen.
- Click Export with hashes to download your company's full audit history - up to the most recent 10,000 records - including each record's position in the audit chain's cryptographic hash.
- CSV columns include timestamp, event type, actor, company, description, IP address, and user agent.
- Verify chain independently confirms the stored audit history has not been altered or had records removed - each record's hash is cryptographically linked to the one before it. This checks the log as stored, not a specific export.
- Records created before the hash chain was introduced are marked separately as unverifiable rather than treated as validated.

Multi-Factor Authentication

Oryele requires multi-factor authentication for all privileged roles.

Enforcing Multi-Factor Authentication

- Go to Settings > Security > Multi-Factor Authentication.
- Supported MFA method: TOTP authenticator app.

Recommendation	Enable MFA on every account with access to client data. A compromised password alone should never be sufficient to access the Oryele platform.