Security and Compliance Summary

AtlasOA v1.0.0 ships with the security controls listed below. All features are built today, verified in code, and available on first install. No cloud components, no telemetry, no data leaving your server.

Category	What is built today
Authentication	Local account authentication with PBKDF2-SHA256 password hashing. 8-hour session timeout. Brute-force lockout. HttpOnly, SameSite=Lax, Secure cookies (when HTTPS enabled).
Authorization	Role-based access control with three roles (admin, editor, viewer) and six granular permissions: read, modify, delete, admin, import, export. Every route checks permissions before rendering content.
Data at Rest	All data stored in a local SQLite database on the institution's server. Credentials (SMTP, SFTP, S3 keys) encrypted with Fernet AES-128 using PBKDF2-HMAC-SHA256 key derivation (200,000 iterations).
Data in Transit	HTTPS via IIS reverse proxy with institution-managed TLS certificate. No data transmitted to any external server under normal operation.
Audit Log	Tamper-evident SHA-256 hash chain in a separate SQLite database. 22 event types logged across authentication, data operations, and system events. Append-only design: no update or delete operations. Survives database restores.
HTTP Security	X-Frame-Options: SAMEORIGIN, X-Content-Type-Options: nosniff, nonce-based Content-Security-Policy, HSTS (when HTTPS enabled), Referrer-Policy: strict-origin-when-cross-origin. CSRF tokens on all POST routes.
Compliance	FERPA school-official exception (34 CFR 99.31(a)(1)(i)(B)). On-premise architecture satisfies data residency requirements. DPA with shared responsibility model (Section 4A) available on request.
Incident Response	Shared responsibility model: vendor handles codebase vulnerabilities (7-day critical, 30-day high severity disclosure). 72-hour breach notification scoped to vendor-side incidents only. Institution manages host OS, network, and physical security.
Backup	Automatic database snapshots before every import operation. Scheduled background backups with configurable retention (default: 50). One-click restore from admin panel.

AtlasOA LLC | 8112 Maryland Ave, Suite 400, St. Louis, MO 63105 | ashleyreddick@atlasoa.com | atlasoa.com