LedgerPro™

Security & Trust Overview

Legal Accounting Software for UK Law Firms

Document version	v1.0 — April 2026
Classification	Public — for distribution to clients and prospects
Prepared by	LedgerPro™ Security Team
Contact	security@lawledgerpro.com
Website	lawledgerpro.com
Trademark	UK00004374963 — Class 42 (Software Services)
External review	Independent black-box security assessment — April 2026

Purpose: This whitepaper provides law firms, COFAs, practice managers and IT leads with a transparent overview of LedgerPro™'s security architecture, data protection measures, and compliance alignment. It supports procurement decisions and due diligence processes.

1. Executive Summary

LedgerPro™ is a multi-tenant SaaS legal accounting platform built for UK solicitors and SRA-regulated law firms. An independent external black-box security assessment conducted in April 2026 confirmed the platform as one of the more mature early-stage legal SaaS platforms from a security perspective.

- ✓ Mandatory MFA for Admin, Finance, and COFA roles
- ✓ AES-256 encryption at rest and TLS 1.3 in transit
- ✓ Complete tenant isolation — pen tested April 2026 (all 5 attack scenarios blocked)
- ✓ Append-only immutable audit logs with 7-year retention
- ✓ Enterprise-grade session controls (rated by external assessor)
- ✓ Daily automated backups to Google Drive (UK data region)
- ✓ UK/EU hosting via DigitalOcean managed infrastructure

External assessment conclusion (April 2026): "LedgerPro has progressed from a feature-strong but trust-light platform to a credible, security-aware legal SaaS product — one of the more mature early-stage legal SaaS platforms from a security perspective."

2. Authentication & Access Control

Multi-Factor Authentication (MFA)

MFA enforcement	Mandatory for Admin, Finance, and COFA roles. Prompted for all other users on first login.
TOTP authenticator	Compatible with Google Authenticator, Microsoft Authenticator, Authy, and any RFC 6238-compliant app.
Email OTP	One-time passcode delivered via email as alternative second factor.
Backup codes	Eight single-use recovery codes generated at MFA setup. Stored as bcrypt hashes.

Password Security

Hashing algorithm	bcrypt with cost factor 12 — industry standard for password storage.
Account lockout	Locked after repeated failed attempts. Rate limiting: 20 attempts per 15 minutes per IP.
Password change	Immediately invalidates all active sessions across all devices.

Role-Based Access Control — 8 Roles

Role	Permissions
Superadmin	Platform administration across all firms.
Admin	Firm-level administration, user management, settings.
COFA	Audit log, compliance reports, reconciliation.
Finance	Full posting and reporting. Cannot manage users.
Solicitor	Matter management and transaction posting.
Paralegal	Matter viewing and limited posting.
Trainee	Read-only with limited supervised posting.
Readonly	View only. Cannot post any transactions.

3. Session Management

Control	Implementation
Idle timeout	30 minutes of inactivity. User warned at 29 minutes, signed out at 30.
Absolute expiry	8-hour maximum session duration regardless of activity.
Server-side revocation	Sessions stored server-side with token hash. Revocation is immediate — token becomes invalid instantly across all API requests.
Password change	Changing password immediately revokes all other active sessions on all devices.
Session visibility	Users can view all active sessions (device, browser, IP, location) from their profile and revoke any session individually.
Re-authentication	High-risk transactions (client receipts, costs transfers, bulk imports) require password re-entry. Single-use tokens, 15-minute expiry.
Security events	SESSION_CREATED, SESSION_REVOKED, PASSWORD_CHANGED, MFA_ENABLED, PERMISSION_CHANGE all logged to immutable audit trail.

External assessor rating: "Enterprise-grade behaviour" — rated 5/5 stars.

4. Data Encryption

Layer	Implementation
Encryption at rest	AES-256 via DigitalOcean managed database. Keys managed using industry-standard key management.
Encryption in transit	TLS 1.3 enforced for all connections. No fallback to older TLS versions or SSL permitted.
Password storage	bcrypt (cost factor 12). Never stored in recoverable form.
MFA secrets	Encrypted at rest. Never transmitted after initial QR code display.
Backup encryption	Encrypted in transit and at rest within Google Drive (UK data region).
API tokens	JWT signed HS256. Session tokens stored as SHA-256 hashes server-side.

5. Multi-Tenant Architecture & Tenant Isolation

LedgerPro™ is a true multi-tenant platform. Each law firm is a completely isolated tenant. No firm can access, view, or modify the data of any other firm under any circumstances.

Control	Implementation
Token-level scoping	Every user token contains a firm_id claim set at login. Cannot be modified by the client.
Server-side enforcement	Every API route enforces firm_id from the JWT token. Query parameters requesting a different firm's data are ignored for non-superadmin users.
Database-level isolation	All queries include a firm_id WHERE clause. No cross-tenant query is possible through the application layer.
IDOR protection	Requests for records by ID are validated against the authenticated firm's ownership before data is returned.
Superadmin access	Cross-firm access separately authenticated, rate-limited, and every action logged with explicit firm attribution.

Penetration Test Evidence — April 2026

Test	Attack Scenario	Result
T1	Firm A accesses own matters	PASS — 1,441 matters returned correctly
T2	Firm A requests Firm B matters via firmId parameter	PASS — Own firm matters returned. Firm B parameter ignored
T3	Firm A accesses Firm B matter by direct record ID	PASS — Access denied (403)
T4	Firm A requests Firm B audit log via firmId parameter	PASS — Own firm events returned. Firm B parameter ignored.
T5	Firm A accesses Demo firm transactions by matter ID	PASS — Access denied (403)

External assessor: "Multi-tenant isolation was previously your weakest area. Now it is one of your strongest." Rated 5/5 stars.

6. Audit Logging & Immutability

Control	Implementation
Immutability	Database-level triggers prevent any UPDATE or DELETE on audit records. Even database administrators cannot modify or delete entries.
Retention	7-year minimum retention via automated monthly scheduler. Exceeds SRA Rule 12.1 (6-year minimum).
Events logged	Login, logout, transaction posting, bulk import, PDF export, matter management, user management, compliance checks, MFA events, session events, permission changes.
Log attributes	User name, ID, role, firm, timestamp (UTC), IP address, browser/device.
IP capture	Real client IP via X-Real-IP header from Nginx proxy. IPv4-mapped IPv6 prefixes stripped.
Export	COFA and Admin can export as CSV or PDF with date range, user, and action filters.
Access control	Read-only. Only Superadmin, Admin, COFA can view. No write or delete endpoint exists.

External assessor: "Huge differentiator vs competitors." Rated 5/5 stars.

7. Infrastructure & Data Residency

Component	Detail
Cloud provider	DigitalOcean — UK and EU data regions.
Database	DigitalOcean Managed PostgreSQL. Automatically patched with built-in high availability.
Web server	Nginx reverse proxy with TLS 1.3, HSTS (1 year, preload), and full security header suite.
Application	Node.js/Express API under PM2 cluster mode (2 instances) for high availability.
Backups	Daily automated backups via rclone to Google Drive (UK data region). 30-day retention. Restorable within 4 hours on request.

Subprocessors	DigitalOcean (hosting), Google Drive (backups — UK region), Cloudinary (images), Resend (email), Stripe (payments).
Data residency	All primary data stored within UK/EU. No data transferred outside UK/EU without explicit necessity and appropriate safeguards.

8. Security Headers & Network Controls

Header / Control	Configuration
Strict-Transport-Security	max-age=31536000; includeSubDomains; preload — forces HTTPS for 1 year.
Content-Security-Policy	Strict CSP limiting script, style, image, font, and connection sources to approved domains only.
X-Frame-Options: DENY	Prevents embedding in iframes on any domain.
X-Content-Type-Options: nosniff	Prevents MIME-type sniffing attacks.
Referrer-Policy	strict-origin-when-cross-origin — limits referrer data sent to third parties.
Permissions-Policy	Explicitly disables camera, microphone, geolocation, and payment APIs.
Rate limiting	1,000 requests/15 min globally. 20 login attempts/15 min per IP.
CORS	Restricted to explicitly approved origins. All others rejected.
x-powered-by	Disabled — server technology not disclosed in response headers.

9. Incident Response

Phase	Detail
Detection	Server monitoring, audit log analysis, and automated alerting for anomalous activity.
Assessment	Severity assessed within 4 hours of detection.
Firm notification	Affected firms notified within 24 hours of confirmed incident.
ICO notification	GDPR Article 33 — ICO notified within 72 hours where threshold met.
Affected individuals	High-risk breaches — individuals notified without undue delay (GDPR Article 34).
Remediation	Root cause identified, patched, tested. Post-incident review. Clients updated.
Contact	security@lawledgerpro.com — response within 4 hours during business hours.

10. Compliance & Regulatory Alignment

Framework	Position
SRA Accounts Rules 2019	Purpose-built to support SRA compliance including client/office separation, Rule 8.3 reconciliation, Rule 12.1 retention, and Rule 2.3 debit balance prevention.
UK GDPR	Personal data processed in accordance with UK GDPR. DPAs available on request.
Data Protection Act 2018	All processing aligned with DPA 2018. Data minimisation and purpose limitation applied.
Compliance disclaimer	LedgerPro™ provides tools to support compliance. Regulatory compliance remains the responsibility of each firm and its COFA.
Trademark	UK registered trademark UK00004374963, Class 42 — Software Services. Filed April 2026.
External review	Independent black-box security assessment April 2026.

Risk Summary — Post April 2026 Assessment

Area	Risk Level	Status
Branding and Trust	**Low**	Resolved
Compliance Positioning	**Low**	Resolved
Authentication (MFA)	**Low**	Implemented
Session Security	**Low**	Implemented — rated enterprise-grade
Data Encryption	**Low**	Implemented
Audit Log Immutability	**Low**	Implemented — rated differentiator
Multi-Tenant Isolation	**Low**	Tested & Verified — all 5 pen test scenarios passed
Security Headers	**Low**	Implemented
Backup Architecture	**Low**	Documented

Incident Response	**Medium**	Documented — testing planned
External Pen Test	**Medium**	Planned — staging environment in preparation

11. Contact & Further Information

Security enquiries	security@lawledgerpro.com
General enquiries	lawledgerpro.com/contact
Data Processing Agreement	Available on request — security@lawledgerpro.com
Privacy policy	lawledgerpro.com (footer link)
Document review cycle	Annual or following any material security change
Next scheduled review	April 2027

Disclaimer: This document describes security controls as of April 2026. Security is an ongoing process and controls are continuously reviewed. This document does not constitute a guarantee of security or a warranty against all possible threats. LedgerPro™ recommends all firms conduct due diligence appropriate to their risk profile. This document does not constitute legal advice.

LedgerPro™ | Legal Accounting Software for UK Law Firms | lawledgerpro.com