Legal Sector Guide

Client Confidentiality & Data Protection

Legal practices operate under stringent professional conduct requirements with absolute obligations for client confidentiality and legal professional privilege. Stannp operates under applicable US privacy regulations including state data protection laws, providing the security framework necessary for protecting privileged legal communications.

All client data and legal communications receive confidential classification with 256-bit AES encryption at rest and TLS 1.2/1.3 in transit, achieving an A+ SSL rating from Qualys.

Security Architecture & Access Control

Legal practices manage their own user accounts and access controls within the platform, enabling role-based access control with least privilege and need-to-know principles to support client file segregation and matter-based access restrictions essential for maintaining professional privilege.

Multi-factor authentication is available to enhance account security and support SRA compliance requirements for strong authentication. The platform operates continuous monitoring with 99%+ uptime SLA, ensuring legal communications including court deadline notifications and completion communications remain accessible. Critical database services maintain RTO 30 minutes and RPO 6 hours, supporting business continuity for time-critical legal work.

Compliance & Security Testing

ISO 27001 and PCI-DSS certifications provide regulatory compliance assurance appropriate for legal sector requirements. Our comprehensive security program supports solicitors in meeting their professional obligations for information security under SRA Standards and Regulations.

Monthly vulnerability scans using Qualys and Security Scorecard identify potential security weaknesses that could compromise client confidentiality. Security assessments validate the effectiveness of controls protecting privileged legal communications.

OWASP Top 10 application security testing protects against common web application vulnerabilities. Automated GitHub vulnerability scanning monitors source code continuously. CVSS-based patching ensures critical vulnerabilities are addressed within 7 days, important within 14 days, and moderate within 30 days, maintaining security while supporting urgent legal work.

Data Retention & Secure Disposal

Critical client data receives backup every 15 minutes with daily full backups retained for 30 days. All backup data is encrypted and stored in zonally separated locations, ensuring recovery capability for critical legal documents and communications.

Legal practices manage their own data retention policies within the platform, supporting compliance with varying retention requirements for different matter types. The system supports appropriate

Stannp
Unit 12, Taw Trade Park
Braunton Road, Barnstaple, EX31 1JZ

01271 320 863
www.stannp.com

Stannp Ltd
Company Reg: 09086822
ICO Data Protection Reference: ZA134992

data retention periods in compliance with applicable privacy regulations. Secure disposal procedures include physical destruction of hard drives before equipment disposal and applicable US privacy regulations requirements, ensuring privileged communications cannot be recovered from disposed equipment.

Incident Response & Business Continuity Testing

Data breaches are reported to relevant authorities within 72 hours as required by applicable US privacy regulations. Incident management framework classifies incidents by severity (Critical, Major, Minor) with structured response processes including detection, containment, investigation, eradication, recovery, and post-incident review.

Legal practices receive timely notification of incidents affecting client data, enabling them to meet their own notification obligations to the SRA and affected clients. Comprehensive Business Continuity Plan covers all facilities with regular testing through recovery scenarios and tabletop simulations, ensuring continuity for time-critical legal work including court deadlines and completion dates.

Data Security & Training

All staff receive annual security awareness training covering applicable US privacy regulations, data handling, phishing, social engineering, and incident reporting, with emphasis on the heightened sensitivity of legal communications. Technical personnel receive specialized training on secure coding practices and OWASP Top 10 guidelines, ensuring security considerations throughout the development lifecycle for systems handling privileged legal material.

All new employees are subject to background checks before commencing employment, ensuring appropriate vetting for personnel who may access privileged legal communications and client data.