Property & Estate Agents Guide

Data Protection & Compliance

Stannp operates under applicable US privacy regulations including state data protection laws. All client, tenant, and property data is classified as confidential and protected with 256-bit AES encryption at rest and TLS 1.2/1.3 in transit, achieving an A+ SSL rating from Qualys.

Multi-Branch Access Management

Property businesses manage their own user accounts and access controls within the platform, supporting role-based access control suitable for multi-branch operations and remote working arrangements common in the property sector. Multi-factor authentication is available to enhance account security.

The platform operates continuous monitoring with 99%+ uptime SLA, ensuring property communications including viewing confirmations, offer notifications, and tenancy communications remain accessible. Critical database services maintain RTO 30 minutes and RPO 6 hours, supporting business continuity during critical transaction periods.

Security Standards

ISO 27001 and PCI-DSS certifications demonstrate compliance with security standards expected by professional bodies. Our security measures support property businesses in meeting their professional obligations for client data protection.

Monthly vulnerability scans using Qualys and Security Scorecard assess security posture across systems handling property transaction data. Security assessments validate the effectiveness of controls protecting client and property information.

OWASP Top 10 application security testing protects against common web application vulnerabilities. Automated GitHub vulnerability scanning monitors source code continuously. Critical patches are applied within 7 days, important patches within 14 days, and moderate patches within 30 days.

Transaction Data Protection & Backup

Critical transaction 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 during critical completion periods.

Property businesses manage their own data retention policies within the platform. The system supports appropriate data retention periods in compliance with applicable privacy regulations. Secure disposal procedures include physical destruction of hard drives before equipment disposal.

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

Incident Response & Business Continuity

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, classification, containment, investigation, eradication, recovery, and post-incident review.

Property businesses receive timely notification of incidents affecting client data. Comprehensive incident logs enable pattern identification and continuous improvement of security controls protecting property transaction information.

Data Security & Staff Training

All equipment is tracked throughout its lifecycle with secure disposal procedures ensuring property transaction data cannot be recovered from disposed equipment. Staff receive annual security awareness training covering applicable US privacy regulations, data handling, phishing, social engineering, physical security protocols, and incident reporting procedures appropriate for the property sector.

All new employees are subject to background checks before commencing employment, providing appropriate vetting for personnel handling sensitive property transaction data.