Financial Services Guide

PCI-DSS Compliance & Data Protection

Stannp maintains PCI-DSS compliance alongside ISO 27001 and Cyber Essentials certifications. Operating as a Data Processor under UK GDPR (ICO: ZA134992), all customer and payment data is classified as confidential. Data is encrypted with 256-bit AES at rest and TLS 1.2/1.3 in transit, achieving an A+ SSL rating from Qualys. Hosted exclusively in Ireland (EEA) on Microsoft Azure with no data transfers outside the EEA.

High Availability & Access Control

The platform delivers 99%+ uptime SLA with RTO 30 minutes and RPO 6 hours for critical databases. Multi-factor authentication is mandatory for all internal systems with 2-hour session timeouts. Access follows role-based access control with least privilege and need-to-know principles. All user authentication is unique with no shared accounts.

Security Testing & Vulnerability Management

Comprehensive security programme includes:

- Monthly vulnerability scans using Qualys and Security Scorecard
- Monthly PCI-DSS compliance scans
- Annual penetration testing and security assessments
- OWASP Top 10 application security testing
- Automated GitHub vulnerability scanning
- CVSS-based patching: Critical 7 days, Important 14 days, Moderate 30 days

Monitoring & incident Response

24/7 SIEM monitoring with 12-month audit log retention and clock synchronisation ensures comprehensive security oversight. Data breaches are reported to the ICO within 72 hours. Incident classification by severity (Critical, Major, Minor) triggers structured response processes including detection, containment, investigation, eradication, recovery, and post-incident review. All incidents are logged for pattern identification.

Backup & Data Management

Critical data backups occur every 15 minutes with daily full backups retained for 30 days. All backups are encrypted and geographically separated within the EEA. Standard retention is 3 years (customisable) with 2-month processing retention, supporting GDPR erasure rights. Secure disposal includes physical destruction of hard drives before equipment disposal, complying with WEEE legislation.

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

Physical Security & Training

Facilities maintain 24/7 alarm monitoring and CCTV surveillance with controlled access and visitor accompaniment. Clean desk policy and locked cabinets protect confidential materials. All staff receive annual security awareness training covering UK GDPR, PCI-DSS requirements, phishing, social engineering, and incident reporting. Technical personnel receive specialised training on secure coding and OWASP Top 10 guidelines.