Retail & E-Commerce Guide

Customer Data Protection & Payment Security

Retail and e-commerce businesses process high volumes of customer data and payment information requiring robust security controls and scalable infrastructure. Stannp operates under applicable US privacy regulations including state data protection laws, providing the security framework necessary for retail customer communications.

All customer and payment data receives confidential classification with 256-bit AES encryption at rest and TLS 1.2/1.3 in transit, achieving an A+ SSL rating from Qualys. ISO 27001 and PCI-DSS certifications ensure retail sector compliance.

High Availability & Scalability

The platform delivers 99%+ uptime SLA supporting high-volume processing requirements essential for peak trading periods including Black Friday, Christmas, and January sales. Critical database services maintain RTO 30 minutes and RPO 6 hours, ensuring customer communications including order confirmations and delivery notifications continue during peak demand.

Retail businesses manage their own user accounts and access controls, enabling role-based access control with least privilege principles for customer service, marketing, and operations teams. Multi-factor authentication is available to enhance account security for teams accessing customer data and payment information.

Payment Security & Compliance

PCI-DSS compliance ensures adherence to payment card industry security standards throughout customer communication processing. Regular PCI-DSS compliance scans validate ongoing compliance with security requirements for systems handling payment-related communications.

Monthly vulnerability scans using Qualys and Security Scorecard assess security posture across retail systems. Security assessments validate the effectiveness of controls protecting customer and payment data.

OWASP Top 10 application security testing protects against common web application vulnerabilities that could compromise customer information. 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 during peak trading periods.

Customer Data Protection & Backup

Critical customer 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 trading periods.

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

Retail 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.

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.

Business Continuity Plan includes periodic recovery scenario testing and staff training exercises, ensuring continuity during peak trading periods. Retail businesses receive timely notification of incidents affecting customer data.

Data Security & Staff Training

All equipment is tracked throughout its lifecycle with secure disposal procedures. Staff receive annual security awareness training covering applicable US privacy regulations, PCI-DSS requirements, phishing, social engineering, and incident reporting appropriate for retail environments. Technical personnel receive specialized training on secure coding practices and OWASP Top 10 guidelines, ensuring security throughout the development lifecycle for retail systems.

All new employees are subject to background checks before commencing employment, ensuring appropriate vetting for personnel who may access customer and payment data.