Public Sector & Local Government Guide

Government Compliance & Data Protection

Stannp holds Cyber Essentials certification alongside ISO 27001, ISO 9001, and ISO 14001 certifications. Operating as a Data Processor under UK GDPR and Data Protection Act 2018 (ICO: ZA134992), all citizen and government 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. Hosted exclusively in Ireland (EEA) on Microsoft Azure with no data transfers outside the EEA.

Security Architecture & Access Control

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, ensuring unique user authentication with no shared accounts. The platform operates 24/7 SIEM monitoring with 12-month audit log retention and clock synchronisation. Critical services maintain 99%+ uptime SLA with RTO 30 minutes and RPO 6 hours for databases.

Security Testing & Vulnerability Management

Comprehensive security programme includes:

- Monthly vulnerability scans using Qualys and Security Scorecard
- Annual penetration testing and security assessments
- OWASP Top 10 application security testing
- Automated GitHub vulnerability scanning for source code
- Azure Cloud Defender for infrastructure analysis
- CVSS-based patching: Critical 7 days, Important 14 days, Moderate 30 days

Data Management & Recovery

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. Business Continuity Plan covers all facilities with regular testing through recovery scenarios, staff training exercises, and tabletop simulations.

Incident Response & Breach Management

Data breaches are reported to the ICO within 72 hours as required by UK GDPR. Incident management framework classifies incidents by severity (Critical, Major, Minor) with structured response processes: detection, classification, containment, investigation, eradication, recovery, and

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

post-incident review. Comprehensive incident logs enable pattern identification and continuous improvement.

Physical Security & Training

Facilities maintain 24/7 alarm monitoring and CCTV surveillance with controlled access, visitor registration, and staff accompaniment. Clean desk policy and locked cabinets protect confidential materials. Network equipment is housed in protected cabinets with restricted access. All equipment is tracked throughout its lifecycle with hard drives physically removed and destroyed before disposal, complying with WEEE legislation. Staff receive annual security awareness training covering UK GDPR, phishing, social engineering, physical security, and incident reporting. Technical personnel receive specialised training on secure coding practices and OWASP Top 10 guidelines.