Public Sector & Local Government Guide

Government Compliance & Data Protection

Public sector organizations operate under specific government security requirements with heightened accountability for citizen data protection. Stannp holds ISO 27001 and ISO 9001 certifications, demonstrating compliance with government security standards.

Operating under applicable US privacy regulations including state data protection laws, all citizen and government data receives confidential classification. Data is encrypted with 256-bit AES at rest and TLS 1.2/1.3 in transit, achieving an A+ SSL rating. Data hosting occurs exclusively in Ireland (EEA) on Microsoft Azure with no transfers outside the EEA, supporting compliance with government security classification requirements.

Department Access Controls

Public sector organizations 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 departmental segregation and public sector audit requirements.

Multi-factor authentication is available to enhance account security and meet government security standards. The platform operates continuous monitoring with 99%+ uptime SLA, ensuring citizen communications including statutory notifications and public service information remain accessible. Critical database services maintain RTO 30 minutes and RPO 6 hours, supporting continuity of public services.

Security Compliance

Regular vulnerability scans using Qualys and Security Scorecard identify potential security weaknesses. Security assessments validate the effectiveness of controls protecting citizen data.

OWASP Top 10 application security testing protects against common web application vulnerabilities. Automated GitHub vulnerability scanning monitors source code continuously. Azure Cloud Defender provides infrastructure analysis and threat detection capabilities. CVSS-based patching ensures critical vulnerabilities are addressed within 7 days, important within 14 days, and moderate within 30 days.

Data Management & Recovery

Critical citizen 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 essential public services.

Public sector organizations manage their own data retention policies within the platform, supporting compliance with varying statutory retention requirements. The system supports appropriate data retention periods in compliance with applicable privacy regulations. Business Continuity Plan covers

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

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

Incident Response & Breach Management

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.

Public sector organizations receive timely notification of incidents affecting citizen data, enabling them to meet their own notification obligations under Freedom of Information requirements and public accountability frameworks. Comprehensive incident logs enable pattern identification and continuous improvement.

Data Security & Training

All equipment is tracked throughout its lifecycle with hard drives physically removed and destroyed before disposal, complying with government disposal requirements. Staff receive annual security awareness training covering applicable US privacy regulations, phishing, social engineering, physical security, and incident reporting appropriate for handling citizen data. Technical personnel receive specialized training on secure coding practices and OWASP Top 10 guidelines.

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