

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, ISO 9001, and ISO 14001 certifications, demonstrating compliance with government security standards.

Operating as a Data Processor under PIPEDA and Canadian privacy 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 within Canada (Canada Central and Canada East regions) on Microsoft Azure infrastructure. Authorized UK-based personnel may access data remotely for print file creation and support operations, with all data remaining on Canadian servers. All access is secured through encrypted connections, multi-factor authentication, and comprehensive logging, with personnel contractually bound to maintain PIPEDA-equivalent standards. This supports compliance with Government of Canada security 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

ISO 27001 certification demonstrates compliance with government security requirements for suppliers to public sector organizations, combined with ISO 9001, and ISO 14001 certifications.

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.

Document Name:	TCC07	Version No:	1	Date:	1 October 2025	Review Date:	1 October 2026
----------------	-------	-------------	---	-------	----------------	--------------	----------------

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 within Canada, 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 2-month processing retention for PIPEDA and Canadian privacy law 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 posing a real risk of significant harm are reported to the Office of the Privacy Commissioner of Canada as soon as feasible as required by PIPEDA and Canadian privacy laws. 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 Access to Information Act and Privacy Act requirements, and public accountability frameworks. Comprehensive incident logs enable pattern identification and continuous improvement.

Training

Staff receive annual security awareness training covering PIPEDA and Canadian privacy laws, 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 starters are subject to background checks before commencing employment, ensuring appropriate vetting for personnel who may access citizen and government data.

Document Name:	TCC07	Version No:	1	Date:	1 October 2025	Review Date:	1 October 2026
----------------	-------	-------------	---	-------	----------------	--------------	----------------