

Financial Services Guide

Payment Security & Regulatory Compliance

Financial institutions require robust security controls that meet stringent regulatory standards. Stannp maintains PCI-DSS compliance alongside ISO 27001 certification, providing the security framework necessary for processing customer communications containing payment card and financial data.

Operating as a Data Processor under PIPEDA and Canadian privacy laws, we implement bank-grade security measures throughout our infrastructure. 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. 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 ensures compliance with data residency requirements.

PCI-DSS Compliance Program

Our PCI-DSS compliance program includes regular compliance scans and the security testing required to achieve and maintain PCI-DSS certification. All systems operate under strict security controls including network segmentation, access restrictions, and comprehensive logging.

Regular PCI-DSS compliance scans ensure continued adherence to payment card industry security standards, with identified issues remediated according to our vulnerability management procedures.

Operational Resilience for Financial Institutions

The platform architecture supports Canadian financial sector operational resilience requirements with 99%+ uptime SLA and rapid recovery capabilities. Critical database services maintain RTO 30 minutes and RPO 6 hours, ensuring financial communications continue without material disruption during incidents.

Financial organizations manage their own user accounts and access controls within the platform, implementing role-based access control with least privilege and need-to-know principles appropriate to their regulatory obligations. Multi-factor authentication is available to enhance account security, supporting institutions in meeting regulatory requirements for strong customer authentication and operational resilience.

Document Name:	TCC03	Version No:	1	Date:	1 October 2025	Review Date:	1 October 2026
----------------	-------	-------------	---	-------	----------------	--------------	----------------

Continuous Security Monitoring

Our Security Information and Event Management (SIEM) system provides continuous monitoring and real-time threat detection across all infrastructure components. All security incidents undergo classification by severity level—Critical, Major, or Minor—triggering appropriate response procedures. Our structured incident response includes detection, containment, investigation, eradication, recovery, and post-incident review phases. Comprehensive incident logging enables pattern identification and continuous improvement, while ensuring financial institutions receive timely notification of any events affecting their data.

Vulnerability & Patch Management

Our vulnerability management program combines automated scanning with independent security assessment. Regular vulnerability scans using Qualys and Security Scorecard identify potential security weaknesses across infrastructure and applications.

OWASP Top 10 application security testing protects against common web application vulnerabilities including injection attacks, broken authentication, and security misconfigurations. Automated GitHub vulnerability scanning monitors source code continuously, identifying security issues during development before they reach production systems.

CVSS-based patch management ensures timely remediation with critical vulnerabilities addressed within 7 days, important vulnerabilities within 14 days, and moderate vulnerabilities within 30 days. This risk-based approach prioritizes patches according to severity and exploitability, maintaining security while minimizing operational disruption.

Data Protection & Backup Procedures

Critical financial data receives backup every 15 minutes with daily full backups retained for 30 days. All backup data is encrypted using the same standards as production data and stored in zonally separated locations within Canada, ensuring recovery capability while maintaining data sovereignty.

Organizations manage their own data retention policies within the platform. The system supports 2-month processing retention for PIPEDA and Canadian privacy law erasure rights. Secure disposal procedures include physical destruction of hard drives before equipment disposal.

Personnel Controls

All personnel receive annual security awareness training covering PIPEDA and Canadian privacy laws, PCI-DSS requirements, phishing recognition, social engineering awareness, and incident reporting procedures. Technical personnel receive additional specialized training on secure coding practices and OWASP Top 10 guidelines, ensuring security considerations integrate throughout the development lifecycle. This comprehensive training program supports our security culture and ensures staff understand their role in protecting financial institution data.

Document Name:	TCC03	Version No:	1	Date:	1 October 2025	Review Date:	1 October 2026
----------------	-------	-------------	---	-------	----------------	--------------	----------------



Stannp.com

The Communications Platform

All new starters are subject to background checks before commencing employment, ensuring appropriate vetting for personnel who may access financial institution data.

Document Name:	TCC03	Version No:	1	Date:	1 October 2025	Review Date:	1 October 2026
----------------	-------	-------------	---	-------	----------------	--------------	----------------

www.stannp.com



Stannp Inc.

2727 Steeles Avenue West, Suite 1032,
North York, Ontario, M3J3G9, Canada



www.stannp.com



+1 437 295 0300