Information Security Policy Guide

Our Commitment

Stannp is committed to robust Information Security Management to ensure the confidentiality, integrity, and availability of all information. We protect data in accordance with applicable US privacy laws including HIPAA, CCPA, and state-specific regulations, as well as ISO 27001 standards, and maintain continuous improvement of our security practices.

Information Security Principles

Information is classified according to appropriate levels of confidentiality, integrity, and availability in line with legislative, regulatory, and contractual requirements. All data processed on behalf of our customers is classified as confidential and handled as such. For healthcare clients, Protected Health Information (PHI) is handled in accordance with HIPAA requirements. Access is based on least privilege and need-to-know principles. All users must handle information appropriately according to its classification level, and breaches must be reported. Information security provisions are regularly reviewed through annual internal audits and penetration testing.

Security Measures

We implement comprehensive technical and organizational measures including encryption of data in transit and at rest, regular system audits and penetration testing, strict access controls with mandatory multi-factor authentication for systems accessing PHI or sensitive data, and immediate breach response with notification to relevant parties as required by HIPAA and state breach notification laws.

Cloud Providers and Suppliers

All suppliers and cloud providers must meet our security standards or demonstrate equivalent protection. Cloud providers require risk assessment and approval by our Chief Technical Officer before use. For healthcare data, all vendors must execute Business Associate Agreements as required by HIPAA.

Third-Party Mail House Services

Where we engage third-party mail houses to print and post mail on behalf of our customers, these vendors must meet stringent security and compliance requirements. All third-party mail houses must demonstrate security standards that match or exceed our own internal security levels. For healthcare-related mailings containing Protected Health Information (PHI), mail house partners must be fully HIPAA compliant and execute Business Associate Agreements prior to processing any customer data. We conduct thorough due diligence on all mail house vendors, including security audits, compliance verification, and ongoing monitoring to ensure continuous adherence to our security standards and applicable regulatory requirements.

Stannp Inc.
250 Fillmore Street Suite
150 Denver 80206
www.stannp.com
1-888-321-2148

Roles and Responsibilities

All employees are responsible for information security and must act professionally while conducting Stannp operations. Our Compliance and Operations Director oversees privacy policy compliance, data protection, breach reporting to relevant authorities, IT infrastructure provision, physical security, and information security policies. Managers ensure policy implementation and maintain awareness of security risks within their areas.

Incident Reporting

We have comprehensive incident and data breach reporting policies and processes in place to ensure swift response and appropriate notification to affected parties, relevant authorities, and regulatory bodies as required by HIPAA and state privacy laws.

Stannp Inc.
250 Fillmore Street Suite
150 Denver 80206
www.stannp.com
1-888-321-2148