Data Encryption Standards Guide

Overview

Our cryptography policy provides comprehensive guidelines to secure data transfer and storage through encryption. Encryption helps prevent unauthorised access to sensitive customer and company data, protecting information from ever-growing potential threats.

Encryption Standards

Industry-Leading Encryption Stannp employs approved encryption solutions following industry-recognised standards to control access to and preserve the integrity and confidentiality of all data classified as "confidential".

256-bit AES Encryption for Data at Rest All stored data is protected using 256-bit AES encryption, providing the highest level of security for data in storage, within file systems, and within databases. This ensures that even if physical storage is compromised, the data remains unreadable without proper decryption keys.

TLS 1.2/TLS 1.3 for Data in Transit All data transmitted to, from, and within Stannp systems is protected using TLS 1.2/TLS 1.3 protocols. This applies to data both inside and outside company boundaries, ensuring continuous protection during transfer.

SSL/TLS Excellence

A+ Rated Security Our SSL encryption for public-facing web services maintains consistently high standards. All connections are rated A+ by Qualys SSL Labs, representing the highest achievable security rating for web encryption.

Regular Standards Review Encryption ciphers and protocols are configured following recommendations from trusted third-party information security experts including Qualys and OWASP. We regularly review and update our encryption standards to ensure we use current secure hashing functions and ciphers.

Comprehensive Encryption Coverage

Our cryptography policy ensures encryption techniques are implemented across all critical processes and situations:

Cloud Storage Protection All data stored in cloud environments is encrypted to protect against unauthorised access, ensuring customer data remains secure even within third-party infrastructure.

Password Security Passwords are stored using strong cryptographic hashing, never in plain text, protecting credentials even in the event of a database breach.

Remote Access Security All remote access connections are encrypted to protect data and authentication credentials during transmission.

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

Payment Card Data Processing and transmitting cardholder data over any network is protected with strong cryptography in accordance with PCI-DSS requirements, ensuring compliance with payment card industry standards.

Web Application Transactions HTTPS is enforced for all web application transactions, ensuring that user interactions with our platform remain encrypted and secure.

Wireless Network Security Wireless networks are secured using strong encryption protocols to prevent interception of data transmitted over wireless connections.

Cryptographic Key Management

Secure Key Storage Cryptographic keys are securely stored in Azure Key Vault, protecting them from modification, loss, destruction, and unauthorised disclosure. This centralised, secure key management system ensures keys remain protected throughout their lifecycle.

SSH Key Security Private keys generated for SSH authentication are unique per person and machine. Keys are never transferred or copied between systems and are refreshed at least annually to maintain security.

Key Protection All cryptographic keys are protected with strict access controls, ensuring only authorised systems and personnel can access them for legitimate encryption and decryption operations.

Compliance and Standards

Regular Security Assessments Our encryption implementations are regularly tested as part of our monthly vulnerability scans and annual penetration testing to ensure they remain effective against emerging threats.

Industry Best Practices We follow guidance from trusted information security experts including Qualys, OWASP, and industry standards bodies to ensure our cryptographic practices remain current and effective.

Continuous Monitoring Encryption standards and implementations are continuously monitored by our Compliance team to ensure ongoing adherence to policy requirements and industry best practices.

Data Protection Assurance

Our comprehensive cryptography policy ensures that customer data is protected with the strongest available encryption methods, both when stored and during transmission. Combined with secure key management and regular security assessments, these measures provide robust protection for all sensitive information processed through our platform.

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