Stannp.com
The Direct Mail Platform

Secure Development Guide

Overview

Stannp implements comprehensive secure development practices to ensure information security and privacy are built into every application from the ground up. Our security-by-design approach follows industry-leading standards and guidelines, ensuring that customer data remains protected throughout the entire software development lifecycle.

Security by Design & Default

Information security and privacy are incorporated by design and default into all software development. Security is a fundamental requirement considered from the initial design phase through to production deployment. Our development practices follow the principle that secure systems are built through secure processes, with every stage of the development lifecycle incorporating security controls and validation. All software is developed in-house with no third-party development, maintaining complete control over security standards and quality throughout the development process.

Industry-Leading Standards

Software is designed and developed based on industry secure coding guidelines including the Open Web Application Security Project (OWASP) Top 10, NCSC government guidelines for secure development, and NIST guidance on mitigating software vulnerabilities. These internationally recognised frameworks ensure our development practices align with current security best practices and address the most critical security risks. Our adherence to these standards is regularly validated through security testing and external audits, demonstrating our commitment to maintaining the highest development security standards.

Environment Segregation

Development, test, and production environments are completely separated and do not share common components. Each environment operates on separate networks with segregation of administrative duties between development, test, and production teams. This separation ensures that development activities cannot impact production systems, test data never reaches production environments, and production data is never exposed to development or test environments. Network-based separation prevents any cross-contamination between environments whilst maintaining operational efficiency.

Secure Code Management

Development code is stored in secure code repositories that enforce version control and appropriate version archiving. Repositories meet access control policy requirements with segregation of duties, ensuring only authorised personnel can access or modify code. All code changes are tracked, auditable, and can be reverted if necessary, maintaining the integrity and stability of applications.

Industry-standard source code revision tools such as Git and GitHub provide comprehensive version management with complete audit trails of all modifications.

Code Review Process

All code is reviewed prior to release by skilled personnel other than the code author or developer. Code reviews are conducted against secure development coding guidelines, employing both manual and automated techniques to identify security vulnerabilities, coding errors, and deviations from standards. Peer review ensures that only secure, well-understood code reaches production systems. Code must be approved before being promoted into test or production environments, with formal approval processes ensuring appropriate oversight and accountability.

Comprehensive Testing

All pre-production testing occurs in dedicated test environments that mirror production environments as closely as possible. Application security testing is performed using manual and automated techniques, with testing conducted as a minimum for the OWASP Top 10 vulnerabilities including Security Scorecard vulnerability testing, cross-site scripting (XSS), and other common security threats. Continuous vulnerability scanning monitors systems and applications for security weaknesses, with identified issues promptly remediated. All public-facing web applications are tested using manual or automated vulnerability security tools at least annually or after significant changes.

Vulnerability Management

All vulnerabilities identified during testing, including penetration testing, are corrected prior to promotion to production or managed through our risk management process. Test results are reported to management teams for oversight and continuous improvement. Monthly web application vulnerability scans specifically test for SQL injection, XSS, and other threats. All penetration testing is conducted by external specialist companies, providing independent verification of security controls. Critical vulnerabilities are addressed immediately, with all findings tracked through to resolution.

Test Data Protection

All testing and development activities use synthetic data only—production data, cardholder data, and personal data are never used in non-production environments. If sensitive information is required as part of the testing process, it is sanitised, anonymised, or pseudonymised to protect confidentiality whilst enabling effective testing. This strict separation ensures customer data cannot be exposed through development or testing activities and maintains compliance with data protection regulations.

Change Control & Deployment

Code is promoted to production by approved personnel following documented change control processes. Production environments are backed up prior to code promotion to facilitate rollback for failed changes. Test data is removed before applications are promoted to production, with verification that no development files or test data are stored in production environments. Formal change management includes stakeholder approval, documentation, comprehensive testing in separate environments, and unit testing on all upgrades prior to rollout. We communicate significant platform updates that may affect service delivery to clients, ensuring transparency in operations.

Continuous Integration & Automation

Tests are automated through our Azure DevOps continuous integration pipeline. PHPUnit and PEST frameworks provide comprehensive unit testing coverage, enabling rapid identification and resolution of issues. Only well-tested code that passes all automated and manual tests is deployed to production. Automation reduces human error whilst maintaining rigorous quality standards and enables rapid response to security issues through automated testing and deployment pipelines.

Security Architecture

Our secure development practices integrate with broader security measures including input validation following OWASP guidelines, secure error handling preventing information disclosure, encryption at rest and in transit for all sensitive data, secure authentication and authorisation mechanisms, protection against common attack vectors, and regular security assessments validating control effectiveness. Architecture reviews ensure security is maintained as systems evolve and scale.

Compliance & Standards

Our secure development practices support compliance with ISO 27001 information security management requirements, PCI-DSS secure development standards for payment card systems, UK GDPR requirements for privacy by design and default, and industry best practices for software security. Regular audits verify ongoing compliance with these standards, with all practices documented and subject to continuous review and improvement.

Commitment to Secure Development

Our comprehensive secure development practices ensure that security is built into every application from the ground up. Through industry-leading standards, rigorous testing, complete environment segregation, peer code review, external penetration testing, and formal change control, we maintain the highest standards of software security whilst delivering reliable, feature-rich applications that protect customer data throughout its lifecycle.