Security Assessment & Testing Guide

Introduction

Stannp maintains a rigorous security testing programme to validate the effectiveness of our security controls and identify vulnerabilities before they can be exploited. Our commitment to proactive security includes regular vulnerability scanning, automated monitoring, and independent third-party penetration testing across all systems that process customer data.

Vulnerability Scanning

We conduct comprehensive automated vulnerability scanning across our entire infrastructure:

- **Continuous automated scanning** of all systems that hold or process confidential information
- **Monthly vulnerability assessments** with automated alerting for any issues detected
- **Multi-layered scanning** covering open ports, code vulnerabilities, malware detection, version checking, and PCI DSS compliance
- **Industry-standard risk assessment** using CVSS (Common Vulnerability Scoring System) ratings

All discovered vulnerabilities are prioritized and remediated according to strict timeframes:

- Critical vulnerabilities: Resolved within 7 days
- High severity vulnerabilities: Resolved within 14 days
- Medium severity vulnerabilities: Resolved within 30 days
- Low severity vulnerabilities: Evaluated and addressed as appropriate

Penetration Testing

Independent external penetration testing provides real-world validation of our security posture:

- **Conducted by specialist third-party security firms** with expertise in identifying real-world attack vectors
- **Regular testing schedule** including pre-release testing for new applications and periodic testing of existing systems
- **Additional testing following significant changes** to validate security after major updates
- **Comprehensive testing scope** including our infrastructure and, where applicable, our cloud service providers

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

Application Security Testing

Our development and platform security includes:

- **Automated dependency scanning** via GitHub's vulnerability detection services
- **Code review processes** incorporating both manual and automated security testing techniques
- **Segregated testing environments** that mirror production for realistic security validation
- **Multi-tool security assessment** using Qualys for penetration and vulnerability scans, Azure Cloud Defender for infrastructure analysis, and Security Scorecard for monitoring our public-facing services

Network Security & Monitoring

Continuous protection through:

- **Firewall protection and application-level security controls** to validate requests, enforce authentication, and block unauthorised access.
- **Layered firewall protection** with network segregation based on data sensitivity
- **Intrusion detection systems** deployed across critical infrastructure
- **Web filtering** to block malicious and phishing content
- **Comprehensive logging and monitoring** of all security-relevant events

Patch Management

We maintain current security patches across all systems:

- **Automated patching** where available and appropriate
- **Monthly compliance verification** ensuring all systems remain up to date
- **Risk-based management** for any patching exceptions
- **Formal change control** for production system updates

Commitment to Continuous Improvement

Our security assessment programme is regularly reviewed and updated as part of our continual improvement process. All security measures are verified through internal audits, external assessments, and regular reporting to senior management.

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