# Vulnerability Assessment and Patch Management Policy Guide

## Overview

Our vulnerability assessment and patch management policy ensures comprehensive controls are in place to detect vulnerabilities and ensure operating systems, application software, and firmware are updated to address known security vulnerabilities in a timely manner. This proactive approach protects customer data and maintains system integrity.

## Vulnerability Assessment Process

**Mandatory Security Scanning** Mandatory vulnerability scans are implemented for all systems that hold or process confidential customer information. Scans are configured on appropriate schedules based on the classification of information held or processed.

**Comprehensive Scanning Coverage** Our vulnerability scans include port scans for unneeded open ports, code vulnerability tests, PC virus and malware scans, PCI DSS compliance scans, and version checking for common software. This comprehensive approach ensures all potential security weaknesses are identified.

**Trusted Security Tools** We utilise approved third-party security vendors including Qualys for penetration and vulnerability scanning, GitHub automated vulnerability scanning for source code and dependencies, Azure Cloud Defender for infrastructure analysis, and Security Scorecard for public-facing web services.

**Regular Security Testing Schedule** Monthly vulnerability scans are conducted using Qualys and Security Scorecard. Monthly web application vulnerability scans test for SQL injection, XSS, and other common threats, with continuous monitoring through SIEM systems.

## Vulnerability Report Analysis

**Structured Review Process** All vulnerability scans produce detailed reports which are processed and analysed to determine the level of risk each vulnerability presents. Action plans are defined to address vulnerabilities according to severity rating timeframes.

**Risk Assessment** Each identified vulnerability undergoes assessment to understand the risk and business impact if exploited. This ensures resources are appropriately allocated to address the most critical security concerns first.



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

## Severity-Based Patch Management

We follow Microsoft's severity rating system with defined timeframes for patch deployment:

**Critical Vulnerabilities** Vulnerabilities allowing code execution without user interaction, including self-propagating malware or unavoidable scenarios, are patched immediately but no later than 7 days. These represent the highest security risk and receive immediate priority.

**Important (High) Vulnerabilities** Vulnerabilities that could compromise confidentiality, integrity, or availability of user data or processing resources are patched immediately but no later than 14 days.

**Moderate (Medium) Vulnerabilities** Vulnerabilities with mitigated impact due to authentication requirements or non-default configurations are patched immediately but no later than 30 days.

**Low Severity Vulnerabilities** Comprehensively mitigated vulnerabilities are evaluated and patched based on risk assessment and operational requirements.

## Patch Management Controls

**Automated Patching** Automated patching is deployed where available and appropriate, ensuring timely updates with minimal manual intervention.

**Regular Compliance Monitoring** The patching status of all endpoint devices and production systems is checked every 30 days. Automatic tracking with alerting and reporting identifies non-compliant devices requiring remedial action.

**Change Management Integration** Patching of production systems follows our standard change management process, ensuring updates are properly tested and documented before deployment.

**Risk-Based Patching Schedule** Patches are applied following our risk-based schedule with 14-28 days for application patches and 30 days for infrastructure updates as detailed in our Application Security Policy. Critical security patches are prioritised and applied as soon as testing is complete.

## Exception Management

**Controlled Exceptions** An exception list is maintained, managed, and reported via the Management Review Team. Where patches cannot be applied due to operational requirements or other valid reasons, the device is added to the risk register and managed through our risk management process.

**Continual Improvement Tracking** Exceptions are reported and tracked through the management review team meeting process, ensuring continuous improvement and eventual resolution of patching constraints.

## Compliance and Verification

**Multi-Method Compliance Verification** The information security management team verifies compliance through business tool reports, internal and external audits, and feedback mechanisms. This ensures adherence to policy requirements and identifies areas for improvement.



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

**Regular Policy Review** The policy is updated and reviewed as part of our continual improvement process, incorporating lessons learned, industry best practices, and changes in the threat landscape.

## Data Protection Assurance

Our comprehensive vulnerability assessment and patch management policy ensures that all systems processing customer data are regularly scanned for vulnerabilities and promptly patched according to risk-based priorities. This proactive approach minimises security risks and maintains the highest standards of data protection.