Asora Penetration Test Summary

Overview

An independent penetration test of the Asora Web and Mobile Application was conducted by Instil (CREST-certified testers), a recognised cybersecurity consultancy.

- Testing period: October 2025
- Retest completed: February 2026
- Scope: Web application, mobile application, APIs, and supporting infrastructure

Key Outcomes

The assessment identified a number of vulnerabilities across the application. These were addressed through a structured remediation programme and independently verified via retesting.

- All high severity vulnerabilities were successfully remediated and verified as closed
- The majority of medium-severity findings were remediated and closed
- Remaining findings are low to medium risk and do not present material risk to customer data or platform integrity

Remediation Summary

Asora follows a proactive security posture with rapid remediation and validation of findings:

- Critical and high-risk issues are prioritised and resolved immediately
- Fixes are verified through independent retesting
- Security improvements are incorporated into ongoing development processes

Remaining Findings (Non-Critical)

A small number of lower-risk findings remain open and are being addressed as part of ongoing development:

- Medium: Input handling in export functionality (formula injection risk)
- Low: HTTP security header consistency
- Informational: Input validation hardening opportunities

These findings do not expose sensitive data directly and are actively tracked and prioritised for resolution.

Security Assurance

The results of this assessment demonstrate that:

- The platform has no outstanding critical or high-risk vulnerabilities
- Identified issues are managed through a structured and effective remediation process
- Independent testing and verification form part of Asora's ongoing security programme

Additional Information

A full penetration test report is available under NDA upon request.