



Vulnerability reporting policy

A clear, private route to report a suspected vulnerability or security concern without putting customer information at risk.

VERSION 1.0 | REVISED 13 SEPTEMBER 2026

Where to report

Send a concise report to Krishna@booksai.io with "BooksAI security report" in the subject. This is the public contact for SumPulse Software Inc.'s BooksAI security concerns.

Use the first message to describe the issue, affected BooksAI page or feature, potential impact and a way to reach you. If evidence contains sensitive information, request a suitable private exchange before sending it.

Useful information

Where safe, include the steps that led to the observation, the approximate time, expected versus observed behavior, and a minimal redacted screenshot or example. Use fictional data or accounts you control.

Do not send passwords, API keys, full authentication tokens, bank details or records belonging to another customer. Stop if you unexpectedly encounter information you are not authorized to access. Do not download, retain or share it beyond what is strictly needed to report the concern.

Boundaries for reporting

This policy welcomes reports; it does not authorize access to another person's account or data, bypassing permissions, or intrusive testing of production systems. Request written authorization before testing outside normal use of your own account.

Do not disrupt availability, run denial-of-service or high-volume automated scans, use social engineering, install malware, alter records or make accounting transactions to demonstrate an issue. Third-party services are outside our authorization.

How reports are handled

We review the information provided to assess the issue and determine appropriate next steps. We may ask for clarification or a safer reproduction. Resolution and communication depend on impact, evidence and the systems involved.

This policy does not promise a fixed response time, a fix date, payment, a bug bounty or a legal safe-harbor arrangement. Any separately agreed testing terms must be confirmed in writing.

Coordinating disclosure

Please keep suspected vulnerabilities and sensitive evidence private while we assess the report. Discuss any proposed public disclosure with us first so customer protection and remediation can be considered.

We may update this reporting policy as the program develops. The version and revision date identify this edition. For ordinary product questions or early access, use the BooksAI contact form instead.