



Security policy

The controls that support BooksAI accounting work, the responsibilities customers hold and the assurance commitments we can make today.

VERSION 1.0 | REVISED 13 SEPTEMBER 2026

Purpose and scope

BooksAI is a product of SumPulse Software Inc. This policy describes our public security approach for the BooksAI website, application and supported connections. It is intended for customers, administrators and people evaluating the service.

Security controls support an accountable accounting workflow. They do not remove the need for appropriate customer configuration, professional review or an agreement that addresses your requirements.

Access and account responsibility

BooksAI supports workspace roles and company-level access so users work within assigned permissions. Customer administrators should grant only the access needed for a role, review access when responsibilities change and remove departing users.

Protect the sign-in account used to access BooksAI. Use the available account-security protections, keep recovery information current and notify us if you suspect unauthorized access.

Controls around accounting actions

Source documents, prepared work, booking rules, review steps and approval or posting records help teams understand and control accounting actions. Eligible automation depends on the workflow, permissions and configured company rules.

Customers should check source records, coding, dates, amounts, tax treatment and company context. Duplicate indicators and other preparation checks help identify issues, but cannot guarantee that all mistakes or fraud will be detected.



Connections and sensitive information

BooksAI uses encrypted transport and protection for sensitive connection credentials. Establish connections through the authorized product setup; do not paste passwords, API keys or payment credentials into messages.

Connected accounting, AI, messaging and spreadsheet services have their own permissions and terms. Review what a connection can access and where exported or shared information will go. Use only the data needed for the task.

Reporting a concern

Report suspected unauthorized access, data exposure or a product vulnerability privately to Krishna@booksai.io. Start with a brief description and a way to contact you. Do not include secret keys or unrelated customer information.

We use reported information to assess the concern and determine appropriate next steps. Communication and any required notifications depend on the facts, applicable obligations and customer agreements. This policy does not promise a fixed response or resolution time.

Assurance and limitations

Our security and compliance program is in progress. Independent certifications and attestations have not yet been completed. We do not claim SOC 2 attestation or ISO 27001 certification. A service provider's certification is not certification of BooksAI.

No online service can prevent every incident. Using BooksAI does not, by itself, establish compliance with privacy, tax, accounting or industry rules. Confirm any required residency, retention, regulated-data, incident or service-level commitments with us in writing before onboarding.

Leaving and changes to this policy

Before leaving, export information you need, review connected services and request assistance with account or data closure. Disconnecting a service does not automatically delete previous records, audit history, backups or copies held by other services.

We may update this policy as the product and its security program develop. The version and revision date identify this edition. For privacy requests, contractual requirements or questions, contact SumPulse Software Inc. at Krishna@booksai.io.