D20 INVOICE AI

# Security

Last updated 11 June 2026 · How D20 protects your invoices, credentials and accounting connections.

## 1. Architecture

- Each customer has an isolated workspace; every database query is scoped to the workspace so one customer can never read another's data.
- All traffic is encrypted in transit with TLS 1.2+; data is encrypted at rest by our hosting provider.
- Accounting OAuth tokens are additionally encrypted at the application layer with a key held only in server configuration, and are refreshed under lock to prevent token replay.
- Original invoice files, extracted data and the audit trail live in a managed database with rolling 30-day backups.

## 2. Authentication

- Passwords are hashed with bcrypt and never stored or logged in plain text.
- Sessions use short-lived access tokens (15 minutes) with 7-day refresh tokens in HttpOnly, Secure, SameSite cookies.
- Five failed sign-ins lock the account for 15 minutes.
- Users are emailed whenever their password changes and whenever their account signs in from a new device or country, with a one-click reset if it wasn't them.
- Password-reset links expire after one hour and can be used once.

## 3. Access control

- Two roles: admins (billing, team, integrations, rules) and reviewers (process invoices). Admin-only actions are enforced server-side.
- Invitations are single-use, expire after 7 days and can be revoked.
- Every approval, recode, payment, sync and settings change is written to an immutable audit trail with who, when and what.

## 4. AI and third parties

- Documents are processed by the AI provider under API terms that prohibit training on customer data.
- We request the minimum OAuth scopes needed for each accounting system (bills, contacts, payments, attachments) and you can disconnect at any time from Settings; disconnecting deletes the stored tokens.
- Inbound email is accepted only from your team, your connected mailbox or senders you have trusted; everything else is quarantined for review.
- Payment card data never touches D20 — Stripe handles checkout and card storage (PCI DSS Level 1).

## 5. Operations

- Infrastructure is hosted in ISO 27001-certified data centres with network isolation, automated patching and monitoring.
- Dependencies are reviewed regularly and security patches applied promptly.
- Production configuration and secrets are stored in an encrypted secret store, never in source code.
- Access to production systems is restricted to named engineers with multi-factor authentication.

## 6. Incident response and disclosure

If we become aware of a personal-data breach affecting your workspace we will notify your admins without undue delay and in any case within 72 hours, with what happened, what data was involved and what we are doing. Security researchers can report vulnerabilities to privacy@d20invoice.com; we acknowledge reports within 2 business days and do not pursue good-faith research.

Generated 15 Nov 2026 10:27 UTC from the published version at d20invoice.com/legal/security. The online version is authoritative.
Questions: privacy@d20invoice.com.