Terms of Service

Effective: November 8, 2026 • **Version:** 2026-11-08 • **Service:** SpendLeak

This document describes the conditions under which SpendLeak is offered and should be read together with the other policies published through the Service. The actual service operator and monitored legal contact are identified on SpendLeak's legal information page.

Contents

1. Agreement and parties
2. Eligibility and organizational authority
3. What the Service actually provides
4. Accounts and credentials
5. Customer data and ownership
6. Import and information quality
7. Findings, estimates and recovery entries
8. Artificial intelligence and automated outputs
9. Demo and test data
10. Permitted use
11. Prohibited use and misuse
12. Supplier and third-party services
13. Subscription, fees and taxes
14. Confidentiality
15. Data handling and retention
16. Security responsibilities
17. Availability, updates and maintenance
18. Intellectual property and feedback
19. Accuracy warranties and disclaimers
20. Allocation of financial risk
21. Liability limitations
22. Customer indemnity
23. Suspension and emergency restrictions
24. Ending use and account closure
25. Privacy and individual requests
26. Notices and changes to Terms
27. Disputes and governing law
28. General interpretation

1. Agreement and parties

These Terms of Service (the “Terms”) are the agreement governing access to SpendLeak’s website, account features, financial-data workspaces, invoice review tools, reports and optional artificial-intelligence assistance (the “Service”). “SpendLeak,” “we,” “us” and “our” identify the operator disclosed in the Service’s legal information. “Customer” means the business or other entity for which an authorized user opens or administers a workspace; “you” means both the Customer and the individual using the Service as the context requires. If you use SpendLeak for an organization, you affirm that you have authority to accept these Terms for it, and that the organization is responsible for its authorized users. A person who lacks legal capacity to form this agreement must not purport to bind an organization.

These Terms apply alongside the Privacy Policy, Acceptable Use Policy and, where separately executed, any Data Processing Addendum or written order. A signed negotiated agreement controls only to the extent it expressly overrides a conflicting provision. Any promotional summary or interface copy is informational and does not replace these Terms. Nothing here displaces statutory rights that cannot lawfully be waived.

2. Eligibility and organizational authority

The Service is intended for authorized business use by people capable of entering binding agreements. You must not create an account for a business without permission or submit records you have no right to disclose. You are responsible for verifying whether your business is legally permitted to use cloud services and to send particular records to external processors. An employee's technical access to a file does not, by itself, establish a legal right to upload it.

SpendLeak is not designed for children to create independent business-financial accounts. If an account holder's legal capacity or authority is uncertain, the operator may request clarification, restrict use or direct the organization to designate an authorized adult representative. If you manage accounts for others, you must communicate relevant policies and ensure permissions reflect each user's role. A user's acceptance of these Terms does not transfer an organization's pre-existing legal responsibilities to SpendLeak.

3. What the Service actually provides

SpendLeak offers software to import supported records, compare invoices and related documents, surface potential discrepancies, organize evidence, record user-supplied recovery information and assist investigation. Supported imports and features change as the product develops. CSV import is available for structured records; a reference to QuickBooks, Xero, NetSuite, a bank, a payment platform or a similar service may describe an export workflow, not a direct connection. A feature is “connected” only when the interface expressly indicates that a live integration is active and authorized.

Findings are leads for investigation, not certified audit conclusions. A result may be wrong, incomplete, duplicated, stale or based on unreliable inputs. “Potential,” “estimated” and similar labels are deliberate. The Service does not independently verify banking settlements, issue refunds, collect accounts receivable, undertake recovery action or guarantee any savings unless a separate expressly documented feature does so. The operator may modify features, impose fair-use limits, suspend malfunctioning functionality or retire integrations with reasonable notice when appropriate.

4. Accounts and credentials

You must supply accurate registration details and safeguard account credentials. Accounts may use supported email/password or third-party authentication. An OAuth sign-in identity may be a separate account from an email/password identity even where the visible email address matches; do not assume data will merge automatically. Never share passwords, session links, recovery codes or API keys. Notify the operator through the published support channel if you suspect unauthorized access.

The operator may enforce password rules, lockouts, rate limits and risk-based session controls, and may deny suspicious login attempts. Email confirmation, password reset and multi-factor authentication must not be assumed available until visible and functioning in the Service. Your organization should apply its own access policies and end employee access promptly when roles change. The absence of an optional protection does not reduce your obligation to protect accounts reasonably.

5. Customer data and ownership

Between you and SpendLeak, you retain your rights in invoices, contracts, payment records, business names, notes, uploaded materials and other data you submit (“Customer Data”). You grant the operator and contracted service providers a limited, non-exclusive right to host, process, transform, display and transmit Customer Data only as reasonably needed to supply requested functions, maintain security, comply with law and perform the purposes explained in the Privacy Policy. This permission does not transfer ownership to us.

You represent that you have all permissions and legal grounds needed to provide Customer Data, including information concerning employees, supplier representatives and customers. You must avoid uploading unnecessary personal information, passwords, card numbers, health information or other sensitive records outside the product's intended scope. You remain responsible for copies, accurate classification, lawful collection, retention decisions and providing required notices to affected individuals.

6. Import and information quality

Imports can contain missing fields, unusual numbering, foreign currencies, inconsistent taxes, stale rate schedules, duplicate records and manipulated files. SpendLeak may reject, flag or normalize data, but its validation is not comprehensive. Before relying on findings you must compare them against authoritative source documents, payment records, contract amendments, signed approvals and supplier communications. Review field mappings and preview screens carefully; an automatically inferred mapping is only a suggestion.

Where currency conversion is not explicitly performed using a documented date and source, totals must remain in their original currencies. Do not add unlike currencies or treat a historical anomaly as a paid overcharge. Supporting attachments, annotations and exports may be incomplete; retain originals and verify exported reports. The Service does not replace a professional accountant, procurement specialist, licensed auditor, legal adviser or your own financial controls.

7. Findings, estimates and recovery entries

A “finding” is a candidate discrepancy generated by one or more rules or analytical methods. It is not proof of fraud, contractual breach, supplier fault, overpayment or a recoverable legal claim. Findings may overlap, and adding all candidate amounts may exaggerate the actual financial exposure. A recorded refund, credit or recovery is a statement entered by a user unless the interface explicitly shows separately verified matching evidence. Partial recoveries and open amounts require careful reconciliation.

You decide whether to contact a supplier, change a payable, initiate a dispute, submit a tax adjustment or take other action. You must not use an unverified result to accuse someone of misconduct or withhold legitimate payment. Financial decisions should be based on full evidence, human review and advice suitable to the risk. SpendLeak gives no promise that a supplier will accept a claim or that a potential discrepancy can legally be recovered.

8. Artificial intelligence and automated outputs

If the optional AI assistant is enabled, relevant workspace summaries and user questions may be sent to an external model provider to produce explanatory text. Responses can omit facts, misread contracts, fabricate citations, overstate confidence or misunderstand instructions embedded in user content. AI responses are not independent legal, accounting, audit, tax, banking or investment advice. They must be checked against the original evidence and calculations before use. The assistant is not authorized to execute payments, send supplier correspondence or finalize claims on your behalf by default.

Do not put material into the assistant unless your organization has approved such processing and reviewed the Privacy Policy and provider details. Never rely on the AI alone for fraud allegations,

employment decisions, tax filings, creditor disputes or financial reporting. Model availability, policies, retention and geographic processing may change; we will update disclosures when material provider practices change. We do not warrant the accuracy or uniqueness of AI-generated text.

9. Demo and test data

The public demonstration and any sample files contain invented names, invoice amounts, supplier records and recovery scenarios for evaluation only. They are intentionally fictional, even when formatted like realistic business documents. They are not verified examples of real clients, actual money recovered, endorsements or performance statistics. Real cloud workspaces should not be silently populated with sample transactions. You must clearly identify demonstration or test information before sharing reports externally.

Do not upload confidential production records into demo or browser-only modes unless you fully understand where they are stored and whether the data is transmitted to third-party services. Browser storage may be cleared, lost or exposed through the local device; it is not a substitute for managed organizational records. Tests must not be treated as an accounting ledger or evidence of supplier conduct.

10. Permitted use

Use the Service only for legitimate internal review, authorized import, investigation and reporting consistent with applicable laws and these Terms. You may view, export or use outputs for your internal business purposes subject to third-party intellectual property rights and provider restrictions. You may not misrepresent an automated finding as a verified audit opinion, claim SpendLeak has endorsed your recovery demand or attribute independently unverified accuracy statistics to the Service.

You are responsible for verifying exported communications before they are sent. The Service may be used to support review of invoices belonging to your organization or clients when your professional engagement and applicable law allow it. You must follow reasonable security instructions, respect rate limits and protect third-party confidentiality.

11. Prohibited use and misuse

You must not use SpendLeak to process stolen records, gain access to another tenant, test third-party credentials, introduce malicious code, evade authentication, scrape restricted endpoints, overload infrastructure, manipulate financial results deceptively or infringe intellectual property or privacy rights. You must not reverse engineer protected portions of the Service beyond rights that law expressly preserves, resell unauthorized access, impersonate another entity or use outputs to harass individuals.

Security research must use prior written authorization and a defined scope. The operator may investigate credible abuse, temporarily restrict affected access and preserve necessary records when reasonably needed to protect users, comply with law or investigate incidents. Enforcement will be proportionate to severity and applicable contractual and legal obligations.

12. Supplier and third-party services

SpendLeak uses independent hosting, database, sign-in and optional AI infrastructure. Third parties have their own terms, security practices and operational limits. A label mentioning an accounting product does not imply endorsement, partnership or a live API integration. If you separately authorize a future connector, you are responsible for reviewing the requested scope and ensuring account permissions remain appropriate.

Disruptions at a provider can affect availability and timing. We will use reasonable care when selecting and administering providers, but we cannot guarantee that third-party networks never fail. Changes affecting material processing practices should be reflected in published disclosures or appropriate customer notices. The operator is responsible for its own contractual duties to customers; a third party's involvement does not automatically eliminate those duties.

13. Subscription, fees and taxes

Unless a separate written order specifies charges, the currently offered Service is made available on the terms presented in the interface, without a commitment to paid enterprise capacity. If the operator later offers fees, subscriptions, trials or usage-based plans, pricing, renewal terms, cancellation instructions and any applicable taxes must be clearly presented before an authorized purchase. No payment obligation arises solely because you view a public demo or create a free account.

A future subscription or service-level agreement may include additional commercial terms; it must be accepted in the required manner before it applies. Nothing in these Terms authorizes charges that have not been disclosed and consented to. The operator may impose reasonable limits on free access or discontinue a free feature with notice where feasible.

14. Confidentiality

Each party receiving the other's non-public business information will use reasonable care to protect it and will use it only for authorized purposes. “Confidential Information” includes non-public contracts, vendor rates, financial records, account access information, technical information and commercial plans that a reasonable recipient would understand as confidential. It does not include information independently developed without misuse, already lawfully known, publicly available without breach or rightfully received from another source.

Access may be given to personnel and service providers who need it to operate the Service, subject to appropriate confidentiality and security obligations. Legally compelled disclosure should be limited to what law requires, with notice where lawful and practical. These provisions supplement and do not replace obligations under privacy law or a separately negotiated confidentiality agreement.

15. Data handling and retention

The Privacy Policy describes categories of information, purposes, providers and individual rights. Customer Data may be stored in a hosted database and limited records may be retained for security, audit, legal compliance and continuity. Not all deletions are instantaneous or universal: backups, legal holds, incident records and provider retention rules may require limited additional storage. Retention schedules and deletion controls must be evaluated against actual system configuration, not an assumption that data disappears as soon as a user signs out.

Keep your own exports and source documents. If a customer requests deletion or access, the operator will assess identity, applicable law, contractual obligations and the technical capability to complete the request. A workspace deletion is not necessarily the same as deleting an authentication account or provider-side logs. See the Privacy Policy for request channels and limitations.

16. Security responsibilities

SpendLeak and the Customer share responsibility for secure operation. The operator will use reasonable safeguards proportionate to the nature of the information and its service design; the Customer must apply authentication hygiene, user permissions, device security, file classification and verification procedures. Security measures reduce risk but do not make any internet service invulnerable. No statement on the site is a certification of SOC 2, ISO 27001, PCI DSS or a completed penetration test unless independent verification is actually available.

Report a suspected security incident through the published support channel as soon as practicable and avoid public disclosure of credentials or personal records. We may require verification before providing details or restoring account access. Incident notification obligations are governed by applicable law and contracts, not an unconditional promise of any particular response deadline absent a signed commitment.

17. Availability, updates and maintenance

The Service may be unavailable because of maintenance, software updates, internet outages, provider incidents, security controls, quota limits or other operational circumstances. Unless expressly set out in a separately signed service-level agreement, no percentage uptime, response time, processing capacity, uninterrupted access or fixed recovery time is guaranteed. Reasonable efforts may be made to communicate significant planned disruptions where practical.

Updates may change interfaces, calculations, detection rules or availability. The operator should record algorithm versions and materially changed financial methods where technically practical. You must reevaluate findings if relevant imports, contracts, calculation rules or currencies change. A prior report should not be assumed current after data changes.

18. Intellectual property and feedback

The software, interface, design, marks and original documentation are owned or licensed by the operator, subject to applicable third-party rights. You receive a limited, non-exclusive, revocable right to use the hosted Service during the applicable term in accordance with these Terms. You receive no ownership in the software source code, infrastructure or model technology. Customer Data remains yours as described above.

If you submit feature requests or product feedback, the operator may consider and incorporate general ideas without obligation to compensate you, but this does not authorize us to publish your confidential financial records. Use of third-party names or trademarks in export instructions is descriptive and does not imply affiliation.

19. Accuracy warranties and disclaimers

To the maximum extent permitted by law, the Service is provided on an “as available” and “as is” basis without a warranty that detection is complete, that every candidate discrepancy is correct, that files are error-free or that any financial amount is recoverable. We do not warrant uninterrupted or completely secure operation. This disclaimer does not exclude express commitments in a signed agreement or rights and remedies that cannot legally be excluded.

We are responsible for meeting applicable legal duties and any expressly agreed promises; the phrase “as is” does not excuse unlawful conduct. You should perform independent reconciliation, human review and appropriate professional consultation for any materially consequential use of the results. The Service is a review aid and not a substitute for your internal controls.

20. Allocation of financial risk

You remain responsible for payment authorization, contract interpretation, tax treatment, recording accounting entries, supplier negotiations, financial reporting and final business decisions. A discrepancy that SpendLeak does not find is not automatically proof of negligent service, and a finding that SpendLeak does find is not automatically a valid recovery claim. You should preserve source records, validate calculations and maintain appropriate approval controls before money is moved or external representations are made.

If an error is suspected, stop the affected action and contact the operator with enough non-sensitive detail to allow investigation. Depending on applicable law and any negotiated agreement, potential

remedies may include correction of an error, reasonable assistance, a refund of relevant service fees if any, or other legally required relief.

21. Liability limitations

To the extent permitted by applicable law, neither party is responsible to the other for indirect, incidental, consequential, special or punitive losses, or for lost profits or business opportunities arising solely from use of the Service, even if warned such losses were possible. This limitation does not override liability that cannot legally be excluded, including liability arising from fraud, intentional wrongdoing, or other matters for which an exclusion is prohibited by law.

For claims not within an exception required by law or a separate signed agreement, the operator's aggregate contractual liability arising from the Service will be limited, where enforceable, to the greater of CAD $100 or fees actually paid by the Customer for the Service in the 12 months preceding the event giving rise to the claim. This limit applies only where valid under applicable law and does not limit rights, claims or remedies that cannot legally be excluded.

22. Customer indemnity

To the extent law permits, you agree to defend or reimburse the operator for third-party claims, reasonable liabilities and costs directly arising from your unlawful provision of data, knowing infringement of a third party's rights, deliberate misuse of the Service or material breach of the Acceptable Use Policy. This does not apply to the extent a claim results from the operator's own breach, negligence where liability cannot lawfully be excluded, intentional wrongdoing or failure to meet statutory obligations.

An indemnified party should give reasonable notice, cooperate in the defense and not settle a claim imposing an admission or non-monetary duty on the other party without appropriate consent. These provisions are subject to mandatory law and do not require an individual to surrender rights they cannot legally waive.

23. Suspension and emergency restrictions

The operator may restrict an account or specific function when reasonably necessary to address suspected compromise, prohibited content, severe service disruption, non-compliance with law or credible harm to other users. Where reasonable and lawful, we will explain the reason and give an opportunity to resolve the problem. In urgent cases, restrictions may be immediate, but they should be no broader or longer than reasonably necessary.

Temporary suspension does not automatically authorize deletion of Customer Data or the disclosure of unrelated records. Any continued access, preservation or return of information remains subject to applicable law, security needs, retention requirements and any separate data-processing obligations.

24. Ending use and account closure

You may stop using the Service and request closure of your account or deletion of workspace information through the published contact route, subject to identity verification and legal retention requirements. If a self-service deletion feature is not available, a request must be handled manually; no policy should imply an automated button exists when it does not. The operator may end access for material misuse or discontinue the Service with reasonable notice when practical.

Before closure, export records you need to retain. The operator does not guarantee indefinite access after termination. Surviving provisions include confidentiality, ownership, outstanding payment obligations where valid, limitations permitted by law, privacy-related duties and dispute-resolution terms to the extent they logically continue.

25. Privacy and individual requests

Information about identifiable people may appear in business records even where the workspace is primarily financial. You must provide necessary notices, collect only authorized information and respond appropriately when your personnel or suppliers exercise applicable privacy rights. The operator will assess requests for access, correction, deletion and complaint handling under relevant law, the Privacy Policy and the parties' roles.

When acting as a processor or service provider on behalf of a Customer, we may direct a request involving Customer-controlled records to the relevant Customer unless law requires us to act directly. Where legally required, we will provide reasonable assistance, subject to verifying authority and avoiding disclosure of another user's information.

26. Notices and changes to Terms

These Terms carry a version and effective date. Material changes affecting existing users should be communicated through reasonable channels such as an in-product notice or registered email where available. Continued access should not be treated as blanket consent to a material change when law requires a fresh affirmative agreement; the operator may instead require renewed acceptance before access to the cloud workspace.

The previous acceptance record should remain distinguishable from a later version. Legal notices to the operator should use the verified contact details shown in the Service. Providing an email address does not itself authorize promotional emails; marketing preferences are separate and governed by applicable anti-spam law.

27. Disputes and governing law

The parties should first attempt to resolve disputes in good faith through the published legal contact, describing the issue and desired remedy without unnecessarily disclosing confidential data. Subject to mandatory consumer, employment, privacy or other laws, these Terms are governed by the laws of Ontario and applicable federal Canadian law. Courts with competent jurisdiction may hear disputes, subject to rules that cannot be contracted away.

These Terms do not require secret arbitration, forbid lawful complaints to regulators, prevent access to small claims procedures or waive statutory class-action rights where such waivers are prohibited. No compulsory arbitration term is imposed by these Terms. Nothing limits a regulator's authority to investigate or enforce applicable law.

28. General interpretation

If one provision is invalid or unenforceable, the remaining provisions continue to the extent they can operate independently and law permits. A failure to enforce a right immediately is not a permanent waiver. Neither party may assign its material obligations in a way that materially reduces the other's protections without following applicable law or an express agreement. Headings are for convenience and do not alter interpretation.

These Terms, the referenced policies and expressly applicable signed documents form the stated agreement about the Service. They do not create a partnership, fiduciary relationship, audit engagement or agency authority to bind a supplier. In case of a genuine inconsistency, mandatory law prevails. Questions about scope, rights or complaints should be directed to the verified legal contact identified in the Service.

Contact and version control

This document is issued under SpendLeak policy version 2026-11-08. Questions, complaints and authorized requests should be addressed through the legal or privacy contact shown on the deployed Service. The operator must ensure that its public legal identity and monitored contact details are accurate before public use.