Acceptable Use Policy

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.

1. Purpose and authorized data

Use SpendLeak to review financial records you are legally entitled to process. Never submit stolen documents, unrelated personal datasets, account passwords, full payment-card information, government identifiers or material for which your organization has not established lawful authority. Confirm that the people managing the workspace are authorized and that the records are appropriately classified.

2. Honest financial representations

Do not present fictional demo records as a real customer's transactions, alter supporting records deceptively or label potential findings as verified recovery without evidence. Do not use generated findings to fabricate allegations of fraud, pressure suppliers unlawfully or falsely claim that SpendLeak has certified a conclusion. All external financial communications require human review.

3. System and access integrity

Do not bypass authentication or authorization, probe accounts or APIs without permission, distribute malware, overload endpoints, perform automated scraping contrary to access limits or attempt to obtain another customer's records. Do not submit malicious formulas or scripts disguised as invoice data. Responsible security disclosure requires a prior agreed scope for intrusive testing.

4. AI misuse

Do not use the assistant to exfiltrate personal information, override other users' instructions, impersonate legal counsel or accountants, or automate adverse financial decisions without required review. Imported notes, contract text and prompts must be treated as untrusted sources, not as authority to bypass account rules.

5. Enforcement and reporting

The operator may investigate credible misuse and apply proportionate restrictions when reasonably necessary to protect users, infrastructure and legal rights. Report suspected misuse through the

published contact. No enforcement action automatically excuses applicable privacy, retention or notification obligations. Customers remain responsible for their authorized users and lawful instructions.