

AilInventoryPro.com Vendor and Third-Party Risk Policy

Applies to aiinventorypro.com and all of its subdomains
Policy and operating procedures

Document ID: WF-SEC-008 | Version: 1.2 | Prepared: October 16, 2026
Status: Prepared for management approval | Effective date: Upon approval
Policy owner: Designated AilInventoryPro.com Security Owner | Review: At least annually

What changed in version 1.2

Version 1.2 (October 16, 2026) adds the services in scope: every WindFire module and service operated on these domains, including WindFire Blueprint, WindFire Job Flow, the WindFire Order Flow flow chart, vendor-managed inventory, Payroll with the WindFire Tax Service for the United States and Canada, and bank feeds through Plaid or Stripe Financial Connections. It also adds a paragraph that applies this policy to these services. It states that AilInventoryPro.com is not responsible for the tax rates and tax information published by the WindFire Tax Service and that each tenant must verify them. All other requirements of version 1.1 are unchanged; earlier versions stay available at their own addresses.

Purpose and scope

AilInventoryPro.com relies on service providers for hosting, DNS, email, payment processing, bank connections, AI features, address lookup and support tools. This policy ensures that providers who store, process or can access AilInventoryPro.com or customer data protect it to a standard consistent with AilInventoryPro.com's own policies.

Domain scope: this policy applies to aiinventorypro.com and to all of its subdomains, including subdomains added in the future.

Services in scope: this policy covers every WindFire module and service operated on these domains, including inventory, parts and products, sales, purchasing, shipping and receiving, fleet and vendor-managed inventory; Production and Scheduling with WindFire Job Flow; WindFire Blueprint; the WindFire Order Flow flow chart; Quality, WindFire QMS and standard operating procedures; Time Card Manager; Accounting & Finance; Payroll with the WindFire Tax Service for the United States and Canada; bank feeds through Plaid or Stripe Financial Connections; WindFire AI; Projects and Advanced Reporting; the help, training, sales and support desks; and the platform administration portal.

Vendor register

The Security Owner maintains a register of each provider: service, data it can access (none, metadata, customer business data, personal data, financial or payroll data, credentials), where data is stored, the contract and its security terms, the business owner, risk tier, last review date and how to end the service. Typical entries include the hosting provider and control panel, the mail server, payment processors, Plaid, AI model providers and the address lookup service.

Providers for the services in scope include Plaid and Stripe (Stripe Financial Connections) for bank connections. Government websites, calculators and payment portals, such as those of the Internal Revenue Service, state and local tax agencies and the Canada Revenue Agency (including its Payroll Deductions Online Calculator), are public sources for the WindFire Tax Service, not contracted vendors: they receive only synthetic test amounts, never customer data, and their information is treated as reference data that AilInventoryPro.com does not warrant and that each tenant must verify.

Risk tiers

High: providers that store or can access customer financial, payroll, banking or personal data, or credentials.
Medium: providers with access to business data or that the service depends on. Low: providers with no access to customer data.

Due diligence, contracts and review

Before use

1. Define the business need and the minimum data the provider needs.
2. Review the provider's security information (for example a SOC 2 report, ISO 27001 certificate, published security documentation or a questionnaire) proportionate to its tier.
3. Confirm encryption, access controls, incident notification, data location, sub-processors, retention and deletion on termination.
4. For high-tier providers, obtain management approval before production use.

Contract terms

Contracts or accepted terms for high-tier providers should include confidentiality, use of data only to provide the service, appropriate security safeguards, prompt notice of security incidents affecting AiInventoryPro.com data, cooperation in investigations, return or deletion of data at the end of the service, and flow-down of these duties to sub-processors. Where a provider handles customer personal information on AiInventoryPro.com's behalf, the terms must allow AiInventoryPro.com and its customers to meet the notification duties in WF-SEC-006.

Ongoing review

Review high-tier providers annually and medium-tier providers every two years, and after a provider incident or a material change in the service. Track findings to closure. Remove access and confirm data deletion when a provider is retired.

Customer-chosen providers

Customers may connect their own providers, such as their own mail server or payment account. Those relationships are between the customer and the provider; AiInventoryPro.com protects the stored credentials under WF-SEC-007 and limits use to the customer's instructions.

Policy status

Requirements become effective when management approves this document. It does not certify that each control is already operating. Management must verify implementation and supporting records before representing this policy as an operational control to Plaid, a customer or another reviewer. Record implementation gaps with an owner and target date.

Approval and operational confirmation

Legal operating entity: _____
 Security Owner and backup: _____
 Accountable executive and title: _____
 Evidence register location: _____
 Management approval signature and date: _____
 Effective date and next annual review: _____

Related documents and reference basis

WF-SEC-001, WF-SEC-006, WF-SEC-007, WF-SEC-014. FTC Safeguards Rule (16 CFR Part 314), service provider oversight, where applicable. Plaid Developer Policy.