

AilInventoryPro.com Acceptable Use Policy

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

Document ID: WF-SEC-013 | 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. All other requirements of version 1.1 are unchanged; earlier versions stay available at their own addresses.

Purpose and scope

This policy sets the rules for AilInventoryPro.com employees, contractors and anyone else who uses AilInventoryPro.com systems, accounts or customer data on AilInventoryPro.com's behalf. Customers' own users follow their company's rules and the Workspace Access Agreement.

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.

Accounts and passwords

Use only your own accounts. Never share passwords, verification codes or trusted devices. Use a password manager and unique strong passwords. Do not trust public or shared computers. Report lost devices, unexpected verification codes and suspected compromise immediately.

Customer data

Access customer workspaces only when a customer has granted support access or an approved operational task requires it, and only for that purpose. Do not copy customer data to personal accounts, personal devices, unapproved cloud services, chat tools or AI tools that are not approved for that data. Never browse customer data out of curiosity.

Devices

Devices used for AilInventoryPro.com work must have full-disk encryption, a screen lock, current security updates and malware protection, and must be locked when unattended. Do not install unapproved remote-access tools.

Prohibited activities and enforcement

Prohibited

1. Bypassing security controls, verification, logging or tenant boundaries.
2. Testing security against production systems without written approval.
3. Using AiInventoryPro.com systems for illegal activity, harassment or personal commercial purposes.
4. Sending customer data or credentials by unencrypted email or text message.
5. Disabling or tampering with logs.

Email and AI tools

Treat unexpected links and attachments with caution. Use only AI tools approved by management for AiInventoryPro.com work, and never enter customer secrets, credentials, payroll or banking details into tools that are not approved for that data.

Monitoring and enforcement

AiInventoryPro.com may monitor use of its systems to protect security, as permitted by law. Violations may lead to removal of access and disciplinary or contractual action. Everyone acknowledges this policy when they start and annually.

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-002, WF-SEC-014, WF-SEC-015.