

AiInventoryPro.com Security Awareness and Training Policy

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

Document ID: WF-SEC-015 | Version: 1.2 | Prepared: October 16, 2026
Status: Prepared for management approval | Effective date: Upon approval
Policy owner: Designated AiInventoryPro.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

People are the first line of defense. This policy ensures that everyone who works on AiInventoryPro.com knows how to protect accounts and data and how to report problems, and that customers have clear guidance for their own users.

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.

Staff and contractors

Before receiving access to production systems or customer data, and at least annually after that, everyone completes security awareness training covering: these policies; phishing and social engineering; passwords, verification codes and trusted devices; protecting customer, financial and payroll data; secure use of AI tools; device security; and how to report incidents. Completion is recorded.

Role-based training

Engineers receive secure development training covering WF-SEC-009, including authorization, tenant isolation, input handling and secrets. Administrators and support staff receive training on access approvals, support access, recovery procedures and incident response. Training is refreshed after significant incidents or policy changes.

Phishing exercises

AiInventoryPro.com may run simulated phishing exercises with management approval; results are used for coaching, not punishment.

Customer guidance and records

Customer users

AIInventoryPro.com provides in-product lessons and help articles, in six languages, on signing in with 2-step verification, trusting devices, the security page, agreements and going live. The Workspace Access Agreement and the public security policies page explain what each user's access means.

Records

Keep training materials, attendance and completion records, and acknowledgments of the Acceptable Use Policy under the evidence retention schedule. The Security Owner reports completion to management at least 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-006, WF-SEC-009, WF-SEC-013. NIST SP 800-50 Building an Information Technology Security Awareness and Training Program.