

AilInventoryPro.com Secure Development and Change Management Policy

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

Document ID: WF-SEC-009 | 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 defines how changes to the AilInventoryPro.com application, its configuration and its servers are designed, built, tested, approved, released and reversed so that changes do not weaken security, tenant isolation or data integrity.

Domain scope: this policy applies to ainventorypro.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.

Security in design and code

1. Check every new feature against these policies; if a feature must differ from a policy, update the policy first and record the decision.
2. Enforce permissions on the server; validate input; use parameterized queries; escape output; protect state-changing requests against cross-site request forgery; never trust identifiers sent by the browser for tenant or record scope.
3. Keep secrets out of source code, logs and the browser (WF-SEC-007).
4. Prefer the framework's supported extension points over modifying framework code.

Testing

Test each change on a copy before release: the intended behavior, permission denials (including cross-tenant requests and direct API calls), and the effect on existing workspaces. Use test accounts and synthetic or practice data, not live customer data, wherever possible. Security-sensitive releases include automated checks that run after deployment and fail visibly.

Release and change control

Release procedure

1. Each release has a number, release notes and a list of changed files.
2. Before release: review the change, run the release checks on a copy, and take a backup of affected sites.
3. Production releases are deployed only with the owner's approval, to the named sites, never to every site at once without a decision to do so.
4. After release: run the release checks on each site, verify key pages, and watch the logs.
5. Every release has a rollback plan; if checks fail, roll back first and investigate after.

Configuration and server changes

Changes to server, DNS, mail, firewall, hosting control panel or security settings follow the same approval and record-keeping, with a backup of the previous configuration and a note of who changed what and why.

Emergency changes

An urgent change to stop an incident may be made before approval when waiting would cause harm. The person making it records it immediately and obtains retrospective approval by the next business day.

Records

Keep release notes, approvals, test and check results, and rollback records under the evidence retention schedule.

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-007, WF-SEC-012. OWASP Application Security Verification Standard; NIST SP 800-218 Secure Software Development Framework.