

AiInventoryPro.com Vulnerability and Patch Management Policy

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

Document ID: WF-SEC-012 | 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

This policy defines how AiInventoryPro.com finds and fixes security weaknesses in its servers, operating systems, containers, the Frappe and ERPNext framework, third-party libraries and its own code.

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.

Inventory

Keep an inventory of servers, containers, framework and application versions, and major libraries, so that announcements can be matched to what AiInventoryPro.com runs.

Sources

Follow security announcements for the operating system, the hosting control panel, Docker, Frappe and ERPNext, Python and JavaScript libraries, and the database. Run dependency and vulnerability scans at least monthly and before major releases. Review the results of any external testing.

Remediation deadlines

Fix or mitigate confirmed vulnerabilities in production within: critical, 7 days (or sooner when actively exploited); high, 30 days; medium, 90 days; low, at the next planned maintenance. Apply operating system security updates at least monthly. When a fix cannot meet the deadline, document an exception with compensating controls under WF-SEC-001.

Testing and disclosure

Applying updates

Updates follow WF-SEC-009: test on a copy, back up, deploy with approval, run checks and keep a rollback path. Emergency security updates may use the emergency change procedure.

Security testing

Perform an internal security review of authentication, authorization and tenant isolation for every security-sensitive release, and arrange an independent penetration test when the customer base or contracts require it, at least annually once AiInventoryPro.com handles production financial data at scale.

Responsible disclosure

People who believe they have found a vulnerability can report it to info@aiinventorypro.com. AiInventoryPro.com acknowledges reports, investigates, fixes confirmed issues under these deadlines, and does not take action against good-faith researchers who avoid harming data or service.

Records

Keep scan results, tickets, fixes and exceptions, and report open high and critical items to management monthly.

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. CISA Known Exploited Vulnerabilities Catalog; CVSS v3.1 for severity.