

AilInventoryPro.com Logging and Monitoring Policy

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

Document ID: WF-SEC-010 | 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

Logs make it possible to detect misuse, investigate incidents and show that controls work. This policy defines which events AilInventoryPro.com records, how logs are protected and how they are reviewed. It applies to the application, the platform, customer workspaces and supporting servers.

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.

Events recorded

At minimum: sign-ins, failed sign-ins, lockouts and verification codes sent (with masked addresses); trusted-device, destination and confirmation events; account creation, role and access changes; agreement signatures; support access grants and use; changes to mail, payment, banking and security settings; workspace go-live; API key creation; release deployments; and server administrative access. Each record has a time, the person, the actor if different, the source address where available and a short description.

What is never logged

Passwords, verification codes, trusted-device tokens, API keys, access tokens, full bank or card numbers, tax identifiers and message bodies are never written to logs.

Protection

The AilInventoryPro.com security log is append-only in the application: entries cannot be edited or deleted through the application. Access is limited to the original Tenant Admin for their workspace and to authorized platform operators. Server logs must be readable only by administrators, and server clocks must be synchronized.

Review, alerting and retention

Review

The Security Owner reviews privileged activity and authentication events monthly, and all security log trends quarterly, together with the access reviews in WF-SEC-002. Reviews look for repeated failures, lockouts, unusual destinations, support access, new administrators and setting changes. Findings are tracked to closure.

Alerting

People are notified directly of events that may indicate account takeover, such as a change to where their codes are sent or to their sign-in address. Platform operators monitor server health, mail delivery and failed jobs. Additional automated alerting is added as the service grows and recorded in the evidence register.

Retention

Security logs are retained for at least one year, and longer when needed for an investigation, legal hold or contract, under WF-SEC-004. Customers can export their workspace security log.

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-003, WF-SEC-004, WF-SEC-006. NIST SP 800-92 Guide to Computer Security Log Management.