

AiInventoryPro.com Access Control Policy

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

Document ID: WF-SEC-002 | Version: 1.3 | 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 1.3

Version 1.3 (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. It also adds a paragraph that applies this policy to these services. All other requirements of version 1.2 are unchanged; earlier versions stay available at their own addresses.

Purpose and scope

AiInventoryPro.com limits access to information and systems to authorized people and services with a documented business need. This policy defines how access is requested, approved, granted, protected, monitored, reviewed and revoked. It supports WF-SEC-001. It applies to employees, contractors, suppliers, administrators, service accounts, APIs and automation accessing AiInventoryPro.com production or supporting environments, and to customer records, financial and payroll information, Plaid credentials and tokens, source repositories, hosting systems, databases, backups and security logs.

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.

Core access requirements

Deny access unless an authorized role or explicit permission permits it. Grant the minimum functions, records, tenant scope and duration needed. Use named individual accounts for people and separately owned service accounts for automation; shared human accounts are prohibited. Enforce permissions on the server for every protected request, including searches, downloads, exports, background jobs and related records. Hiding a control in the interface is not an authorization control.

Visual editors and flow charts (WindFire Blueprint, WindFire Job Flow and WindFire Order Flow) change real records and enforce the same server-side permissions as the forms they replace: a person cannot do through a flow chart what the person's role does not allow in the form. WindFire Blueprint is limited to the tenant administrator and approved administrators. Payroll records, employee tax profiles and payroll tax settings are limited to people with payroll roles, and the WindFire Tax Service publishing console is limited to authorized AiInventoryPro.com platform staff.

Separation of duties

Nobody approves their own new privileges or grants themselves higher authority. Approval, provisioning and review are separated where staffing permits; otherwise management documents the conflict and requires compensating review. Financial and payroll permissions must preserve native approvals and must not arise from integration or support access.

Tenant and owner boundaries

Platform Super Admin controls the platform across tenants; Tenant Admin authority is limited to one customer workspace. Matching email addresses, role names or browser selections never grant access to another tenant. The original Tenant Admin is identified from the subscription configuration; delegates must not modify, disable or restrict the owner or the owner's privileges. Support access to customer information requires the customer's time-limited grant, a documented purpose, an authorized scope and an audit trail.

Sign-in protection and sessions

Passwords and attempts

Passwords must reach a strength score of at least 3 of 4 (zxcvbn) and may not be reused across systems or shared. After five failed password attempts an account waits five minutes. Sign-in by email link is off. Multifactor authentication is required for every human workspace and platform account as defined in WF-SEC-003.

Session limits

Workspaces: a session ends after eight hours without activity and in any case 14 hours after sign-in. Platform portal: two hours without activity and 12 hours after sign-in. Sessions end, and trusted devices are forgotten, when a password or sign-in address changes. An administrator can sign a person out everywhere. Tokens are never placed in URLs or browser storage.

Re-authentication for sensitive actions

Changes to people, roles, access, sign-in destinations, API keys, mail relay, payment settings and security settings, signing agreements and taking a workspace live require a verification code confirmed within the previous ten minutes (WF-SEC-003).

Agreements before access

A customer workspace opens only after its original Tenant Admin has signed the Customer Agreement and the schedule for each subscribed module. Every other person accepts the Workspace Access Agreement, which explains that the company controls the workspace, their access and their personal information, and links to these policies. Updated agreements must be accepted within ten days, with daily reminders; after that, the agreement stands between sign-in and the workspace. Each signature is kept permanently with the exact text, a SHA-256 fingerprint and a PDF copy, and AilInventoryPro.com keeps a copy.

New workspaces and going live

A new workspace opens only after the original Tenant Admin gives the account details (identity, title, legal name, address, phone, email, time zone). Until the workspace goes live, nothing reaches customers or suppliers: outside email is held, payment links and the payment page are off and portal sign-in is refused. Going live requires a complete company profile and the company's own mail relay tested with a code sent through it, and only the original Tenant Admin may take the workspace live, with a fresh confirmation.

Account lifecycle and access review procedures

Request and approve access

1. Record the person or service, manager or owner, business purpose, systems, role, tenant and data scope, start date and end date for temporary access.
2. The system or data owner validates need and conflicts; the Security Owner or management approves privileged, production financial data or external support access. Keep the decision and approver.
3. The administrator verifies identity, provisions only the approved scope, confirms 2-step verification enrollment, and tests intended access and relevant denials.

Change or end access

1. On a change of role, reassess the whole role set and remove obsolete permissions; increased authority is a new request.
2. At departure, disable the account at the effective time; for suspected compromise, suspend immediately under WF-SEC-006.
3. Revoke sessions, trusted devices and API keys, remove memberships, and rotate shared secrets the person could reach.
4. Transfer record ownership and scheduled work without deleting required records or audit history; verify and document completion.

Review access regularly

The Security Owner coordinates monthly reviews of privileged accounts, Plaid Dashboard permissions and production integration credentials, and quarterly reviews of all other user and service access, using a dated export as the baseline. Record each retain, remove or modify decision, assign corrections an owner and deadline, and keep the evidence.

Emergency and third-party access

Emergency access is used only for a documented incident or urgent recovery, with individual accountability, logging, prompt retrospective review and removal after use. Third parties need a named sponsor, approved purpose, confidentiality obligations, least privilege and an explicit expiry.

Logging, exceptions and records

Record account creation, privilege changes, approvals, sensitive administrative actions, authentication failures and revocations (WF-SEC-010) without passwords, codes, tokens or unnecessary financial data. Document each exception with its risk, compensating measures, owner, approver and expiry; review active exceptions at least quarterly. Maintain an access register with owner, account type, system, role, scope, approval, provisioning date, expiry, last review and revocation status.

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 Information Security Policy and Program; WF-SEC-003 Multifactor Authentication Policy; WF-SEC-006 Incident Response Policy; WF-SEC-010 Logging and Monitoring Policy. Version 1.0 (October 2, 2026) remains at /security-policies/WF-SEC-002-v1.0.pdf. Plaid Developer Policy, Account Use and Access and Security sections: <https://plaid.com/developer-policy/>.