

AilInventoryPro.com Data Retention and Deletion Policy

Applies to aiiinventorypro.com and all of its subdomains

Document ID: WF-SEC-004 | Version: 1.2 | October 16, 2026

Status: Controlled policy | Owner: Designated AilInventoryPro.com Security and Privacy Owner

Policy review: At least annually; retention and deletion controls: Quarterly

Purpose and scope

AilInventoryPro.com must retain personal and business data only for an authorized purpose and an approved period, and securely dispose of it when that purpose or period ends. This policy applies to the workspace, platform portal, Plaid integration, production systems, exports, logs, backups, and service providers handling data on AilInventoryPro.com's behalf. It supplements WF-SEC-001, WF-SEC-002, and WF-SEC-003.

Domain scope: this policy applies to aiiinventorypro.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.

Required compliance and accountability

Management designates a Security and Privacy Owner and approves the retention register, exceptions, and resources for enforcement. The Owner identifies applicable privacy, tax, accounting, employment, contractual, and record-preservation obligations with qualified advice where necessary. Requirements must be assessed for each jurisdiction and processing role; a single universal retention period must not be substituted for that assessment.

Engineering and system operators must enforce the approved schedule through permission-checked services, scheduled disposal, restricted archives, and monitored exception handling. Tenant Admins authorize tenant requests within their authority. Staff and suppliers follow the same purpose, access, and disposal limits. Policy requirements must have dated configuration and operating evidence; publication alone does not establish enforcement.

Retention register and collection limits

Before collecting a data category, record its owner, purpose, applicable legal basis, controller or processor role, data subjects, systems and suppliers, jurisdiction, retention trigger, period, legal justification, and disposal method. Collect only necessary data. Minimize raw financial payloads and avoid unnecessary copies. A new use or longer period requires documented review and approval.

Policy retention schedule

The following are AilInventoryPro.com default maximum periods, subject to a shorter applicable legal requirement or a documented lawful obligation. Mandatory business records use the jurisdiction-specific period in the approved register. A legal hold suspends deletion only for its defined scope. No data category may have indefinite retention without a documented lawful justification and recurring review.

Transient Plaid or integration payloads: Delete within 30 days after successful processing unless an approved, necessary record purpose is registered. Derived business records follow their own approved schedule.

Temporary exports and processing files: Delete within 7 days after creation; approved customer-delivered copies are governed by the customer's responsibilities.

Security event logs: Retain for 90 days; access-review and security audit evidence for 12 months. Exclude passwords, live codes, and access tokens from logs.

Retention periods and deletion procedures

Account, business record, and backup periods

Closed workspaces: Allow up to 90 days after contract termination for authorized export and closure, then delete remaining data unless the approved register requires lawful retention. A valid erasure request or shorter applicable deadline takes precedence.

Accounting, tax, payroll, and transaction records: Retain for the applicable statutory or contractual period documented in the register. Preserve submitted records, revision history, and native financial integrity during that period; restrict archived records to the required purpose.

Integration credentials: Revoke provider access promptly when authorization ends or compromise is identified, and remove credentials from active storage when revocation completes. Do not retain live credentials for archival purposes.

Backups: Use a rolling expiry of no more than 35 days unless a separately approved recovery or preservation requirement is registered.

Payroll and tax records: pay runs, pay slips, employee tax profiles (such as Forms W-4 and TD1), year-end forms and filing and remittance records are customer records kept in the customer's workspace under the customer's control. The customer sets and meets its legal record-keeping periods (for example, at least four years for United States employment tax records and six years from the end of the last tax year for Canadian payroll records) and must export these records before a workspace is closed. Tax rates published by the WindFire Tax Service are reference information; AilInventoryPro.com is not responsible for them and each tenant must verify them.

Deletion triggers and request handling

Deletion must be triggered by schedule expiry, termination, withdrawn authorization where applicable, an approved erasure request, or removal of an unnecessary purpose. Verify identity and authority proportionately without collecting unnecessary sensitive evidence. Determine whether AilInventoryPro.com acts as controller or processor; route customer-controlled requests to the responsible customer and assist within contractual obligations.

Log the request date, scope, responsible owner, legal assessment, applicable deadline, systems, suppliers, and outcome. AilInventoryPro.com's internal target is completion within 30 calendar days, or sooner when required by law. Any lawful extension must be documented and communicated within the applicable deadline. Explain any permitted refusal or partial retention and available escalation. Handle correction, restriction, or objection requests through the same accountable process where relevant.

Execute and verify securely

Inventory affected records, relationships, attachments, indexes, caches, exports, and supplier copies. Confirm tenant and record permissions on the server. Use supported application and provider services; revoke an integration separately from any decision to delete related business records. Never bypass native transaction validation, approvals, legal holds, or another tenant's boundaries.

Make deletion jobs repeatable without duplicate effects. Record accurate pending, failed, and completed states; alert an assigned owner to failures and overdue work. Retry safely and verify the result before reporting completion. Delete or securely sanitize active copies, or irreversibly anonymize them where approved. Pseudonymization alone is not deletion. Retain minimal disposition evidence without reproducing the deleted data.

Suppliers and independent providers

Contracts must specify retention, deletion, assistance, and confirmation responsibilities for processors. Send authorized disposal instructions and obtain confirmation or track an exception. Provider-held data subject to a provider's independent legal role must be handled under its applicable process; removing an AIInventoryPro.com connection must not be represented as deleting every record held independently by Plaid or a financial institution.

Exceptions, enforcement, and periodic review

Legal holds and lawful retention

Only authorized management, with legal review where required, may establish a hold or retention exception. Document its legal basis, exact data scope, approver, access restrictions, start date, expiry or release condition, and next review date. Preserve required records securely and prohibit unrelated use. Review holds quarterly and release them promptly when the basis ends; apply the ordinary disposal schedule after release.

Backups and restoration

Deleted active data may remain in isolated recovery backups until their approved expiry. Restrict backup access, prohibit ordinary use, and document the final expiry in the deletion record. When restoring a backup, reapply the deletion and restriction ledger before restored data becomes available for normal service. Verify backup expiry and restoration handling; do not claim immediate removal from immutable backups unless the method has been verified.

Monitoring and enforcement

The Owner maintains a deletion ledger and monitors scheduled jobs, overdue requests, failed disposal, unsupported data categories, supplier confirmations, and exceptions. Engineering must address failures with an assigned owner and target date. Enforce access limits throughout retention and quarantine data that has no approved continuing purpose while its disposition is resolved. Violations follow the incident and corrective-action procedures in WF-SEC-001.

Quarterly control review

At least quarterly, review the retention register, holds and exceptions, overdue requests, disposal failures, supplier results, and backup expiry. Sample completed deletions and check active storage, attachments, indexes, and restored-copy handling. Test permission denial, cross-tenant rejection, retries, partial failures, and preservation of legally required records. Record findings, accountable owners, corrective dates, and closure evidence.

Annual policy review and change control

Review and approve this policy at least annually and after material privacy-law, service, integration, supplier, data-category, or incident changes. Assess applicable legal requirements and shorten retention when continued storage is unnecessary. Record the reviewer, date, decision, version, and next review. Train responsible personnel and update procedures and technical controls before the revised policy takes effect.

Version 1.1 (October 4, 2026) names AiInventoryPro.com as the organization responsible for this policy and states the domain scope: this policy applies to aiinventorypro.com and all of its subdomains. No other requirement changed. Version 1.0 remains at /security-policies/WF-SEC-004-v1.0.pdf.

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. It also adds a paragraph that applies this policy to these services. It states that AiInventoryPro.com is not responsible for the tax rates and tax information published by the WindFire Tax Service and that each tenant must verify them. No other requirement changed. Earlier versions remain available at their own addresses under /security-policies/.

Policy administration

Legal operating entity: _____

Security and Privacy Owner / backup: _____

Approved retention register location: _____

Deletion ledger and enforcement evidence: _____

Management approval / effective date: _____

Last review / next review: _____

Reference basis

The periods above are AiInventoryPro.com policy requirements. Applicable obligations are recorded by jurisdiction and processing role. Supporting guidance: FTC, Protecting Personal Information: A Guide for Business; Plaid Developer Policy. This policy defines required controls and does not certify compliance in every jurisdiction.