

AiInventoryPro.com Workspace Backup and Recovery Policy

Applies to aiinventorypro.com and all of its subdomains

Document ID: WF-SEC-005 | Version: 1.2 | October 16, 2026

Status: Controlled policy | Owner: Designated AiInventoryPro.com Operations and Security Owner

Control review: Quarterly | Policy review: At least annually

Purpose and service scope

This policy defines AiInventoryPro.com's routine workspace backups, optional paid cloud backup storage, customer-selected schedules and contents, and authorized recovery. It protects customer information and AiInventoryPro.com through clear responsibilities, secure storage, verified results, and bounded restoration procedures. It applies to production workspace data, files, backup jobs, storage connections, operators, and processors.

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.

Weekly routine workspace backups

AiInventoryPro.com requires one routine backup of each active, eligible customer workspace every week. The routine backup includes workspace database data and the workspace's public and private uploaded files needed for recovery. Operations assigns a weekly window and records the workspace, start and completion time, included contents, encryption and integrity results, storage location, and expiry. A queued job or uploaded partial archive must not be reported as a successful backup.

Routine backups provide a recovery safety net at the last successfully completed backup point. They do not continuously capture changes between runs. A weekly schedule normally leaves up to seven days of changes after the latest completed point; failures or missed runs can increase that gap and must be disclosed through accurate job status. Customers needing more frequent recovery points must select an appropriate additional schedule and verify completion.

Routine retention and protection

AiInventoryPro.com-managed recovery backups use a rolling maximum retention of 35 days under WF-SEC-004 unless an approved, lawful recovery or preservation exception applies. Rotation must not remove the last usable copy before a replacement has been verified without escalation to the Owner. Longer retention requires an approved exception; if a replacement fails near expiry, Operations must escalate rather than silently retain indefinitely or silently remove the only recovery copy.

Routine backups are stored separately from the working workspace with access restricted to authorized operations personnel and services. Encrypt backup archives and transmission, protect recovery keys separately, and use isolation or immutability where supported. Maintain a separate recovery copy protected from ordinary workspace credential compromise. Backups must not expose another tenant's data.

Completion, failures, and notifications

Verify archive creation, expected scope, database readability, file manifests, checksums, and successful storage before marking completion. Monitor overdue, interrupted, corrupted, and failed jobs. Alert the responsible operator and affected Tenant Admin when their recovery coverage is impaired, show the latest successful backup time, and track retries and resolution. Backups do not replace application access controls, incident response, or customer retention obligations.

Optional paid cloud backups and customer choices

Cloud storage option

Customers may connect a supported cloud storage destination through the optional paid backup offering and schedule additional backups. This option supplements routine AiInventoryPro.com backups. Supported providers, eligible plans, limits, storage regions, and charges must be shown before activation.

Customer-owned provider charges and any AiInventoryPro.com backup-service charges must be identified separately. No provider, price, capacity, frequency, or recovery service is promised beyond the applicable published plan or accepted agreement.

Authorized connection and custody

Only the protected tenant owner or a specifically authorized Tenant Admin may configure the tenant's destination and schedule within existing permission boundaries. Verify account control and tenant ownership before use. Use scoped provider authorization or restricted credentials, protect secrets server-side, and exclude them from browser navigation, logs, ordinary exports, and support screenshots. Never allow a tenant connection to select another tenant's source data or cloud destination.

Before activation, show the destination account/container, storage region, selected contents, frequency, time zone, retention, expected costs, and responsible contact. Require explicit authorization for the connection and any payment or contractual terms. Validate write/read permissions and storage availability. Do not silently change the customer's selections or use a broader credential scope than needed.

Selectable backup contents

Data only: A consistent workspace database backup containing records, relationships, configuration, and native history required for data recovery. Uploaded attachment bytes are excluded; attachment references may remain and will require matching file archives to restore those files.

Data and files: A consistent database backup plus public and private uploaded workspace files, packaged with a matching manifest. This is the preferred selection for a complete workspace recovery.

Files only or selected file categories: May be offered where supported. The selection must clearly identify included files and exclusions. File archives alone are not a complete database or workspace backup.

Selective data exports, if offered, must be labeled as exports and identify their limitations; they must not be represented as fully restorable database backups. Product software, another tenant's data, external bank records, independently held supplier data, and integration secrets are not customer backup contents. Secure internal recovery configuration must be managed separately when needed to decrypt or operate the restored workspace.

Schedules, retention, and customer responsibility

Customers select supported daily, weekly, or other offered schedules, the time zone, contents, and retention settings. Display the next run and most recent successful backup. Prevent overlap, duplicate jobs, and unsafe load; disclose plan limits and schedule delays. Customer cloud retention must comply with WF-SEC-004 and applicable obligations; longer periods require a documented lawful purpose. Customers maintain their cloud account, capacity, payment, permissions, authorized contacts, and any customer-held encryption keys.

Backup operations and controlled recovery

Consistent and auditable execution

Use named, permission-checked backend services and native database/file backup mechanisms. Record the software/schema version and backup scope. Coordinate database and file capture so records and attachments correspond to a defined recovery point. Use bounded, tenant-scoped jobs with safe retries, locking or concurrency controls, timeouts, and accurate partial state. An interrupted run must remain failed or incomplete until all required verification finishes.

Retain minimal job evidence and a signed or integrity-protected manifest where supported. Protect archives and keys from unauthorized access and tampering. Do not include live MFA codes, unnecessary secrets, or unrelated customer information in backup metadata. Delete temporary staging copies within the approved retention period after verified transfer. A provider success response alone is insufficient if the final object is incomplete or unreadable.

Cloud failures, revocation, and suspension

Detect expired authorization, insufficient capacity, unpaid provider service, unavailable regions, rate limits, and failed transfers. Preserve the last successful backup, report the failure and its recovery-point effect, and retry within safe limits. A disconnected cloud account stops future customer-cloud jobs and revokes AiInventoryPro.com's connection credentials; it does not itself delete existing objects or business records. Explain separately how existing copies and provider charges are handled.

Suspension, termination, or failed payment must follow the applicable agreement and WF-SEC-004. Notify the responsible customer of affected jobs and any available export or retrieval window. Never promise indefinite storage after termination. Existing customer-owned cloud copies remain subject to the customer's provider permissions, retention, and deletion responsibilities unless a separately authorized disposal process applies.

Restore authorization and safeguards

A backup is not an instruction to overwrite the live workspace. Verify the requester and tenant authority, assess the backup date, scope, legal holds, native record integrity, software compatibility, and available encryption keys. Explain data that will be replaced, changes made since the recovery point, expected disruption, and file exclusions. Obtain explicit authorization for consequential restoration and preserve a verified rollback copy of affected live data before overwrite.

Restore into an isolated validation environment first where feasible. Verify database integrity, expected record counts, tenant/company boundaries, representative attachments, permissions, and application function. Reapply the deletion/restriction ledger required by WF-SEC-004 before normal access. Review or revoke restored credentials and sessions; do not reactivate withdrawn financial connections or replay payroll, accounting, stock, or external payments. Restore through supported mechanisms and preserve native validations.

Recovery expectations and testing

Recovery depends on the last usable backup, archive scope, encryption keys, platform compatibility, incident conditions, and available capacity. Operations assesses timing and communicates progress; this policy does not establish a guaranteed recovery time, zero data loss, or a contractual service credit. Any agreed recovery point or time objective must appear in the applicable service agreement. Test representative data-only and data-and-files restoration at least quarterly and after material backup changes; record results and corrective actions.

Responsibilities and service limits

AilInventoryPro.com responsibilities

AilInventoryPro.com Operations owns routine schedules, job monitoring, access protection, integrity checks, controlled recovery, and incident escalation. The Security Owner reviews tenant isolation, credential scope, encryption, retention, disposal, suppliers, and restore testing. Maintain current procedures, named backups for responsible personnel, and evidence of completed weekly runs and reviewed failures. Engineering implements the optional scheduling and scope controls in shared services, with permissions enforced server-side.

Customer responsibilities

Customers select schedules and contents suitable for their business, check completion and notifications, protect cloud accounts and keys, maintain sufficient paid storage, and keep contact and authority information current. Customers identify their legal preservation requirements and provide authorized restoration instructions. A data-only choice excludes attachment bytes. Losing a customer-held key, deleting customer-cloud copies, changing provider access, or ignoring failed jobs may prevent recovery; AilInventoryPro.com must report known limitations accurately.

Service limitations and protection of AilInventoryPro.com

Backup storage and recovery are bounded by the subscribed service, supported integrations, lawful retention, and the applicable agreement. Customer selections, independent cloud-provider failures, missing keys, unsupported or corrupted archives, compromise, and changes made after the last successful backup can limit restoration. A backup copy is not a guarantee of error-free service, continuous availability, complete recovery, archival compliance, or prevention of every loss.

This policy does not amend an executed service agreement or create a separate warranty, indemnity, liability cap, service-level guarantee, or automatic entitlement to refunds. Contractual remedies and allocations of liability are governed by the applicable agreement and mandatory law. AilInventoryPro.com retains its responsibilities under that agreement and applicable law; customer or provider responsibilities must not be used to conceal AilInventoryPro.com's own failures. Additional restoration work or optional services may be charged only under disclosed, accepted terms.

Privacy, deletion, and storage regions

Limit backup access and use to recovery, security, and approved lawful preservation. Assess provider security and cross-border transfer requirements before enabling a region. Publish accurate subprocessor and privacy information where required. Customer-requested deletion may age out through the approved backup cycle; isolate retained copies and reapply restrictions on restoration. Permanent disposal and customer-cloud deletion require the applicable authority and verification, not merely removal of a connection.

Policy governance and review

Periodic review and evidence

Review backup coverage, failed and overdue jobs, permissions, provider connections, costs/limits, expiry, exceptions, and restore-test results quarterly. Review this policy annually and after material platform, provider, privacy-law, or incident changes. Track issues with owners, dates, and closure evidence. Verify retries, incomplete archives, denied access, cross-tenant rejection, revoked connections, cloud capacity failures, and matching database/file recovery. Retain audit evidence under WF-SEC-004.

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-005-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. No other requirement changed. Earlier versions remain available at their own addresses under /security-policies/.

Policy administration and reference basis

Management approval / effective date: _____

Operations Owner / backup: _____

Approved weekly window and recovery storage: _____

Supported paid cloud option / plan terms: _____

Job evidence and quarterly restore-test register: _____

Last review / next review: _____

Related policies: WF-SEC-001 through WF-SEC-004. Supporting guidance: CISA #StopRansomware Guide recommends protected, encrypted backups and regular recovery testing. Weekly service frequency, selectable contents, and the service responsibilities above are AiInventoryPro.com policy requirements, not claims of independently verified implementation.