

AiInventoryPro.com Business Continuity and Disaster Recovery Policy

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

Document ID: WF-SEC-011 | 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 keeps the service available and restores it after a serious disruption, such as a server failure, data corruption, ransomware, a hosting provider outage, loss of a key person or a hurricane affecting AiInventoryPro.com's Florida operations. Customer-selected workspace backups are governed by WF-SEC-005; this policy covers the platform as a whole.

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.

Recovery objectives

Target recovery time (RTO): restore the platform and customer workspaces within 24 hours of a declared disaster. Target recovery point (RPO): lose no more than 24 hours of data. Management may set tighter targets for specific customers by contract. Targets are proposed values until verified by a restore test.

Platform backups

Each production database and its files are backed up at least daily. At least one copy is kept off the production server, encrypted (WF-SEC-007), in a different location or provider. Backups are retained under WF-SEC-004 and protected from deletion by a compromised production account where practicable. Configuration, deployment scripts and the application source needed to rebuild the service are kept in version control and backed up.

Plans, testing and communication

Recovery plan

1. Declare a disaster (Security Owner or management) and start the incident record under WF-SEC-006 when security is involved.
2. Decide whether to repair in place, restore to the same server, or rebuild on a new server or provider.
3. Restore the platform site first, then customer workspaces in priority order, verifying integrity and the release checks for each.
4. Rotate credentials if compromise is possible; confirm mail relays, payments and bank connections work.
5. Communicate status to customers until service is restored; record the timeline and lessons learned.

Florida weather readiness

Before and during hurricane season, confirm that backups are current and off-site, that at least two people can reach the hosting and registrar accounts from outside the affected area, and that customer contact lists and status channels work. AiInventoryPro.com's production servers are hosted in a data center; the plan must not depend on any single office or person.

Key people and access

At least two authorized people must be able to administer the hosting, domain, DNS and mail accounts, each with multifactor authentication. Recovery credentials are stored securely (WF-SEC-007) and their location is recorded.

Testing

Restore at least one production backup to a test environment every quarter and a full platform recovery exercise at least annually. Record the time taken and any problems, and fix gaps.

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: _____
Disaster declaration authority: _____
Off-site backup location and provider: _____
Last restore test date and result: _____
Management approval signature and date: _____

Related documents and reference basis

WF-SEC-001, WF-SEC-004, WF-SEC-005, WF-SEC-006, WF-SEC-007. NIST SP 800-34 Contingency Planning Guide.