

AilInventoryPro.com Security Incident Response Policy

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

Document ID: WF-SEC-006 | 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

This policy defines how AilInventoryPro.com detects, reports, contains, investigates, communicates and learns from security incidents affecting the AilInventoryPro.com platform, customer workspaces, customer data (including accounting, payroll, banking and personal information), Plaid data, hosting systems, backups and service providers. It implements the incident response requirements of WF-SEC-001.

Domain scope: this policy applies to ainventorypro.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.

Definitions

A security event is an observable occurrence that may affect security, such as repeated failed sign-ins. A security incident is an event that actually or likely compromises the confidentiality, integrity or availability of information or systems, including unauthorized access, data disclosure, ransomware, account takeover, credential exposure, or loss of a device holding unencrypted data. A breach of security is unauthorized access to data in electronic form containing personal information as defined by applicable law.

Roles

The Security Owner leads incident response and may appoint an incident lead. Management approves external notifications, customer communications and decisions with legal or contractual effect, with counsel where needed. Engineering contains, preserves evidence and restores service. Everyone who works on AilInventoryPro.com must report suspected incidents immediately and must not investigate on their own in ways that destroy evidence.

Reporting

Report suspected incidents at once to the Security Owner through the incident channel recorded below, and to info@ailinventorypro.com if the channel is unavailable. Customers report suspected incidents to AilInventoryPro.com support. Reports are accepted at any time; there is no penalty for a good-faith report that turns out to be harmless.

Response procedure

Steps

1. Triage: record the time, reporter, systems, tenants and data types involved; assign a severity (critical, high, medium, low) based on data sensitivity, number of tenants or people affected and whether the incident is ongoing.
2. Contain: revoke or rotate exposed credentials, keys and tokens; end affected sessions and trusted devices; suspend affected accounts or integrations; isolate affected systems; block malicious sources. Prefer containment that preserves evidence.
3. Preserve evidence: keep security logs, server logs, database snapshots and a timeline. Record who did what and when. Do not alter logs.
4. Investigate: determine the cause, entry point, duration, accounts, tenants and records affected, and whether personal or financial information was accessed or acquired.
5. Eradicate and recover: remove the cause, patch, restore from known-good backups under WF-SEC-005 and WF-SEC-011, verify integrity, and monitor closely after restoration.
6. Notify: decide notification duties promptly (see below) and communicate accurately, without speculation.
7. Close and learn: within ten business days of closure, review what happened, what worked, what did not, and assign corrective actions with owners and dates. Update policies, monitoring and training.

Customer notification

AiInventoryPro.com notifies each affected customer without unreasonable delay after determining that its workspace data was or is reasonably believed to have been accessed without authorization, and in any case within the period required by law or by the customer agreement. The notice describes what happened, the data involved, what AiInventoryPro.com has done and what the customer should do. Customers remain responsible for notices they owe to their own employees, customers and regulators, and AiInventoryPro.com provides reasonable information to support them.

Regulatory notification

Florida: under the Florida Information Protection Act of 2014, section 501.171, Florida Statutes, notice to affected individuals is required no later than 30 days after a breach is determined or reasonably believed to have occurred; notice to the Florida Department of Legal Affairs is required within 30 days when 500 or more Florida residents are affected; consumer reporting agencies must be notified when more than 1,000 individuals are notified at once; and a third-party agent must notify the covered entity within 10 days. Where AiInventoryPro.com acts as a service provider to a customer, it notifies that customer so the customer can meet its duties. Other states, the FTC Safeguards Rule for financial institutions, Plaid's requirements and contracts may impose additional or shorter deadlines. Management confirms each notification decision with counsel and records it.

Plaid and service providers

Incidents involving Plaid credentials, access tokens or Plaid-derived data are reported to Plaid as its policies and agreements require, and the affected tokens are revoked or rotated. Service providers must notify AiInventoryPro.com of incidents affecting AiInventoryPro.com data under WF-SEC-008.

Exercises and records

Test this procedure at least annually with a tabletop exercise (for example: a stolen administrator password, a lost mailbox used for verification codes, or ransomware on the server). Keep an incident register with each event, severity, timeline, decisions, notifications and corrective actions, under the approved evidence retention schedule.

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: _____
Incident reporting channel (phone and email): _____
Legal counsel contact: _____
Accountable executive and title: _____
Incident register location: _____
Management approval signature and date: _____

Related documents and reference basis

WF-SEC-001, WF-SEC-002, WF-SEC-005, WF-SEC-008, WF-SEC-010, WF-SEC-011. Florida Information Protection Act of 2014, section 501.171, Florida Statutes: Florida Statutes 501.171. NIST SP 800-61 Computer Security Incident Handling Guide. This summary of legal duties is not legal advice; management confirms obligations with counsel.