

AilInventoryPro.com Encryption and Key Management Policy

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

Document ID: WF-SEC-007 | 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. It also adds a paragraph that applies this policy to these services. 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 protects information with encryption and how cryptographic keys, passwords, API keys and access tokens are created, stored, used, rotated and destroyed. It covers the platform, customer workspaces, databases, backups, mail relays, payment and banking integrations (including Plaid) and administrative access to servers.

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.

Encryption in transit

All web traffic to AilInventoryPro.com uses HTTPS with TLS 1.2 or later and certificates from a trusted authority; plain HTTP must redirect to HTTPS. Cookies that carry sessions or trusted-device tokens must be Secure and HttpOnly. Outgoing mail relays use STARTTLS or TLS. Connections to payment processors, Plaid and other APIs use TLS with certificate validation. Administrative server access uses SSH with keys, not passwords.

Encryption at rest

Secrets stored in workspace databases (mail passwords, payment and integration keys, bank and Plaid access tokens, tax identifiers) are encrypted with the site encryption key using Frappe's encrypted password storage and are never sent back to the browser. Backups that leave the server must be encrypted before upload. Laptops and phones used for AilInventoryPro.com administration must use full-disk encryption and a screen lock.

Employee identifiers used for payroll, such as Social Security numbers and Social Insurance Numbers, are encrypted in the browser before they are stored; no key or decryption for them exists on the server. Bank-connection tokens and account identifiers for Plaid and Stripe Financial Connections are stored encrypted on the server or held by the platform and are never shown to users.

Passwords and verification codes

User passwords are stored only as salted one-way hashes. Verification codes, trusted-device tokens and agreement fingerprints are stored only as keyed hashes (HMAC-SHA-256) or SHA-256 digests. Passwords, codes and tokens are never written to logs, URLs, browser storage or support tickets.

Key management

Ownership and storage

Each key or secret has a named owner and purpose recorded in the key register (without the secret itself). Server-level secrets (site encryption keys, the global mail relay password, database passwords) are kept in files readable only by root (permissions 0600) or in the application's encrypted configuration, never in source control, tenant databases, chat or documents. Production and sandbox keys are kept separate.

Generation

Keys, tokens and passwords for services are generated with a cryptographically secure random generator and have at least 128 bits of strength (for example 32 random characters from a 62-character alphabet).

Rotation and revocation

1. Rotate service passwords and API keys at least annually, when a person with access leaves, and immediately when exposure is suspected.
2. Revoke Plaid access tokens and payment webhooks for a customer when the customer disconnects the service or ends the subscription.
3. Site encryption keys are not rotated casually: rotating one requires re-encrypting stored secrets and is planned, tested on a copy and approved as a change under WF-SEC-009.
4. Record each rotation or revocation with the date, reason and person, without the secret.

Destruction

When a key or secret is retired, delete it from configuration and secrets stores, and ensure backups that contain it are retained or destroyed under WF-SEC-004. Securely erase or destroy storage media before disposal.

Exceptions

Any system that cannot meet these requirements is documented with its risk, compensating controls, owner and expiry, and approved by management.

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, WF-SEC-002, WF-SEC-004, WF-SEC-005, WF-SEC-009. NIST SP 800-57 Recommendation for Key Management; NIST SP 800-52 Guidelines for TLS Implementations. Plaid Developer Policy, Security section.