

# AiInventoryPro.com Multifactor Authentication Policy

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

Document ID: WF-SEC-003 | Version: 1.3 | 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 1.3

Version 1.3 (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 1.2 are unchanged; earlier versions stay available at their own addresses.

## Purpose and scope

AiInventoryPro.com requires a second authentication step for interactive access to customer workspaces and the platform portal. This policy defines password authentication followed by an emailed verification code, together with enrollment, trusted devices, recovery, monitoring and verification. It supplements WF-SEC-001 and WF-SEC-002.

Coverage: every human account with Desk access (System User) on the platform site and on every customer workspace, including the original Tenant Admin, delegated administrators and the platform Administrator. Each sign-in route is inventoried separately (see Authentication inventory). Machine credentials (API keys) are governed by WF-SEC-002 and must not become a human sign-in route.

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.

## Approved method

The approved method is a password followed by a six-digit code delivered by email to the address recorded for the person. Codes are sent by AiInventoryPro.com's system mail relay, independent of the customer's own mail settings, so a customer mail problem cannot stop sign-in. SMS delivery is not offered. Email codes can be phished; this policy makes no claim of NIST assurance level compliance. Phishing-resistant methods should be preferred for privileged access when they become available.

## Code requirements

Codes are cryptographically random, six digits, bound to the person and to the sign-in attempt, and stored only as a keyed hash. A code expires after five minutes, is accepted once, and allows at most five attempts per challenge. A new code may be requested after 60 seconds, at most three times per sign-in and six times in 15 minutes per person; a resend replaces the earlier code. After five failed password attempts the account waits five minutes before another attempt. Errors before sign-in do not reveal whether an account or address exists. No session exists until the right code is entered.

## **Trusted devices**

After entering a correct code, a person may choose Trust this device on their own computer or phone. That browser may then sign in with the password alone for 30 days. At most five devices are trusted per person. Trust is stored as a random token (only its hash is kept on the server), is tied to the person, and ends when it expires, when the person or the original Tenant Admin forgets the device, or when the person's password or email address changes. A trusted-device sign-in never counts as a recent confirmation: sensitive changes still require a fresh code. People must not trust shared or public computers.

## **Confirmation before sensitive changes**

Adding people or changing their access, roles or sign-in address; changing where codes are sent; creating API keys; granting AiInventoryPro.com support access; changing mail relay, payment or sign-in settings; signing agreements and taking a workspace live require a code confirmed within the previous ten minutes. The request stops with Confirm it's you until the person enters a fresh code.

# Enrollment, recovery and inventory

## Enrollment

A person is enrolled at their first successful code. Codes go to the account's email address unless an administrator records another destination. Changing the destination requires a fresh confirmation by the administrator, a recorded reason, notice to both the old and new address, and ends the person's sessions and trusted devices.

## Recovery

For a lost mailbox or suspected takeover, the original Tenant Admin (or, for a workspace whose owner is locked out, AiInventoryPro.com support after verifying identity through a documented process) changes where codes go. A password or security question alone never authorizes factor replacement. AiInventoryPro.com operators may issue a one-time eight-digit emergency code through the server console for an owner who cannot receive email; each use is recorded in the security log, and the code works once.

## Authentication inventory

Covered: the sign-in page; Frappe's own sign-in address, which is refused for covered people; password reset, after which a code is required before anything opens; sessions that existed before 2-step verification, which are held until a code is entered; trusted devices (above). Off: sign-in by email link. Separate control: API keys (WF-SEC-002). Covered through the platform: AiInventoryPro.com support sign-in, a one-time link issued by the workspace only while the customer grants support access, used by staff who passed 2-step verification on the platform.

Documented exception: Tracker worker sign-in. Shop-floor workers without a workspace account sign in to the time clock only, with their own credentials and a fresh device location. They have no access to workspace records. This exception requires management approval and quarterly review. Not in scope: customer and supplier portal accounts, which have no access to the workspace.

## Monitoring and verification

The security log records codes sent (with masked addresses), failed and successful sign-ins, lockouts, trusted-device events, destination changes, confirmations and emergency codes. It never stores passwords, codes or tokens, and it cannot be edited. The original Tenant Admin can read and export the workspace's log. The Security Owner reviews privileged coverage and exceptions monthly and all covered accounts quarterly, consistent with WF-SEC-002, and after authentication changes or incidents.

Before representing this control as operating, retain dated evidence that: native sign-in is refused; wrong, expired and reused codes fail; resend limits and lockout work; held sessions cannot reach data; trusted devices skip only the sign-in code and are revoked on password change; sensitive changes ask for a fresh code; and failed authentication never creates a session.

## 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: \_\_\_\_\_  
Approved method by login surface: \_\_\_\_\_  
Approved exceptions (Tracker worker sign-in) and review date: \_\_\_\_\_  
\_\_\_\_\_  
Implementation and verification date: \_\_\_\_\_  
Evidence register location: \_\_\_\_\_  
Management approval and effective date: \_\_\_\_\_

**Related documents and reference basis**

WF-SEC-001 Information Security Policy and Program; WF-SEC-002 Access Control Policy; WF-SEC-010 Logging and Monitoring Policy. Version 1.0 of this policy (October 2, 2026) remains at /security-policies/WF-SEC-003-v1.0.pdf. NIST guidance explains that OTP methods can be phished: NIST Multi-Factor Authentication. Review this policy at least annually and after material authentication changes.