

AiInventoryPro.com Information Security Policy and Program

Applies to aiinventorypro.com and all of its subdomains

Policy and operating procedures for Plaid onboarding review

Document ID: WF-SEC-001 | 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

Purpose and policy

AiInventoryPro.com protects the confidentiality, integrity, and availability of customer information and the systems that process it. This document defines security responsibilities, required safeguards, operating procedures, and a recurring improvement process for the AiInventoryPro.com service and its planned or enabled Plaid integration.

Personnel and service providers with access to AiInventoryPro.com systems or information must follow this policy. Management must resource the program, assign accountable owners, track control performance, and resolve or formally accept documented risks. Requirements below become effective on approval; this document does not itself attest that each control has already been implemented or exercised.

Scope

The program covers production and supporting infrastructure, source code, deployment processes, administrator endpoints, customer and employee information, third party services, Plaid Dashboard access, API credentials, integration tokens, and financial information received through Plaid. Applicable safeguards extend to backups, logs, exports, and development or test environments. Only approved Plaid products and authorized data uses are permitted.

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.

Accountability

AiInventoryPro.com management approves the policy, appoints the Security Owner and a backup, and decides material risk exceptions. The Security Owner maintains the risk register, coordinates incident response, reviews evidence, and reports progress. Engineering and operations implement and test controls. Personnel protect credentials, complete training, and promptly report suspected incidents.

Platform Super Admin authority is separate from tenant authority. Tenant Admins manage only their own tenant within assigned permissions. Security oversight does not authorize unrestricted access to customer records or bypass native transaction approvals.

Document control

The Security Owner retains approved versions, change history, acknowledgments, and supporting evidence in a restricted repository. Changes require management approval. Review this policy at least annually and after

material incidents, changes to the integration, or significant changes in risk. Version 1.0 is the initial document prepared for approval.

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-001-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. It states that AiInventoryPro.com is not responsible for the tax rates and tax information published by the WindFire Tax Service and that each tenant must verify them. No other requirement changed. Earlier versions remain available at their own addresses under /security-policies/.

Required security safeguards

Identity and tenant isolation

Use individual accounts, least privilege, and multifactor authentication for privileged access and the Plaid Dashboard. Restrict service accounts to their documented purpose. Enforce tenant, company, location, and record permissions on the server for reads, writes, exports, and background jobs. Browser state, email identity, and client supplied tenant identifiers must not grant cross tenant access. Protect original tenant owner accounts and prevent delegated administrators from increasing their own privileges.

Plaid credentials and financial information

Keep production secrets and long lived integration tokens in approved encrypted server side storage. Limit retrieval to authorized services and personnel. Do not place them in browser storage, source code, URLs, analytics, support tickets, or logs. Keep sandbox and production credentials separate. Revoke or rotate credentials when exposed or when access changes warrant it. Use the approved Plaid Link flow; AiInventoryPro.com must not collect or retain bank login credentials.

Encrypt sensitive information in transit and at rest, including backups and exports. Engineering must document the encryption configuration, key custody, and authorized access. Map each Plaid connection to its authorized tenant and user, validate that association on every request, and limit collected data to the approved product and user purpose. Verify incoming integration messages using the applicable Plaid mechanism before acting on them.

WindFire Tax Service: the tax rates, wage bases, thresholds, tables and formulas, deadlines, form templates and agency and payment links published by the WindFire Tax Service are reference information prepared from public sources. Values found by its research tools stay drafts until a Platform Super Admin reviews and publishes them, and the research uses synthetic test amounts only, never customer data. AiInventoryPro.com is not responsible for the rates and tax information it publishes: each tenant must verify every rate with the issuing tax authority or a qualified professional before relying on it, as stated in Section 3.8 of the Customer Agreement and in the Payroll Schedule. This policy protects that information while it is stored and transmitted; it does not warrant that the information is correct.

Data handling and retention

Classify secrets and financial information as restricted; other customer records as confidential unless approved for disclosure. Maintain an inventory of collected fields, purpose, storage location, recipients, retention period, and deletion method. The Security Owner must approve this schedule before production collection. Honor authorized disconnection and deletion requests, subject to documented retention obligations; restrict retained records and record the reason. Never silently delete native financial or business records to satisfy a technical cleanup request.

Infrastructure and personnel

Restrict administrative interfaces and network access, remove unused services, maintain supported software, and protect workstations with device encryption, screen locks, and timely updates. Personnel must not copy restricted information to unmanaged devices or unapproved services. Require confidentiality commitments and security training before sensitive access and at least annually afterward. Review physical security responsibilities with hosting providers and protect any local equipment or printed records.

Third party and AI access

Before onboarding a supplier with sensitive access, assess its intended data access, security practices, incident contacts, retention arrangements, and contractual responsibilities. Review material suppliers annually and after significant changes. Do not send Plaid credentials or financial information to an AI service without an approved purpose and data review. Wia actions must retain named permission checked services, explicit confirmation for supported writes, and auditable results.

Access and change procedures

Grant change and remove access

1. The requester identifies the person or service, business need, tenant scope, permissions, and required duration. The responsible manager or system owner approves the request before access is granted. No person approves their own privilege increase.
2. The administrator verifies identity, assigns only approved roles, enables required authentication safeguards, and records the approver, scope, grant date, and expiry when applicable. Test that unauthorized tenants and functions remain inaccessible.
3. The Security Owner reviews privileged and Plaid access monthly and all remaining access quarterly. Remove unnecessary access and record the review decision, reviewer, date, and remediation evidence.
4. On departure, reassignment, suspected misuse, or expiry, promptly remove unneeded access, invalidate active sessions and tokens where supported, and rotate shared credentials if exposure is possible. Record completion and verify that access no longer works.

Assess vulnerabilities and release changes

1. Engineering maintains an inventory of systems and dependencies, monitors relevant security advisories, and reviews vulnerability results at least monthly and before material releases. Use authorized testing against AiInventoryPro.com assets only.
2. Record each finding with affected assets, impact, likelihood, severity, owner, target date, and mitigating controls. Escalate active exploitation, credential exposure, and tenant isolation failures immediately to incident response. Other remediation dates must reflect severity and exposure and be approved by the Security Owner.
3. For a proposed change, identify affected services, data, permission boundaries, tests, backups, and rollback steps. Review security sensitive changes before release. Prefer additive migrations and preserve native Frappe and ERPNext validation, transaction integrity, and audit history.
4. Test normal use, denied permissions, tenant separation, invalid inputs, retries, and partial failures as applicable. Use synthetic or approved deidentified test data. Keep production information and credentials out of routine development fixtures.
5. Obtain authorized release approval, deploy to explicitly named sites, verify operation and security controls, and retain release evidence. Emergency changes require a recorded reason and prompt retrospective review. Close vulnerabilities only after verification.

Safe business operations

Plaid connectivity must not silently initiate payments, submit accounting transactions, or grant new financial permissions. Any such workflow requires separate design authorization, current permissions, applicable approvals, and native validation. Protect retries against duplicate effects and retain an accurate record of partial completion.

Monitoring incident response and recovery

Monitor and investigate

Operations must capture relevant authentication failures, privileged changes, sensitive access, integration errors, and events suggesting unauthorized use. Protect logs against unauthorized changes, restrict access, synchronize timestamps, and apply the approved retention schedule. Exclude credentials and unnecessary financial payloads. Configure alerts for material security events and review security alerts and backup failures each business day, with an assigned escalation route for urgent events outside normal hours.

Respond to an incident

1. Report suspected credential exposure, unauthorized financial data access, tenant boundary violations, malware, or service compromise immediately to the designated Security Owner through the approved incident channel. The backup owner acts when the primary owner is unavailable.
2. Open an incident record. Record discovery time, affected systems and tenants, known facts, uncertainty, severity, and the response lead. Preserve relevant logs and evidence with restricted access and a record of handling.
3. Contain the event using authorized measures such as disabling compromised accounts, revoking exposed tokens, isolating affected services, or suspending the integration. Preserve evidence and avoid unnecessary destruction of customer data.
4. Assess the data and users affected. The response lead coordinates management, relevant providers, and qualified advisers as needed. Notify Plaid promptly at security@plaid.com of a security breach or unauthorized use of the Plaid account or End User Data, as required by the Plaid Developer Policy. Track applicable contractual and legal notices; do not wait for a completed root cause analysis to make a required notification.
5. Remove the cause, restore trusted configurations and credentials, test security boundaries, and obtain approval to resume affected processing. Record recovery decisions and monitor for recurrence.
6. Complete a post incident review with causes, impact, response timing, corrective actions, accountable owners, and target dates. Update procedures and training and verify that corrective actions worked.

Back up and recover

Operations must define backup frequency, retention, encryption, isolation, recovery priorities, and responsible owners for critical systems. Management must approve recovery time and acceptable data loss targets before production reliance on the Plaid integration. Review backup failures each business day and perform a documented restore exercise at least quarterly and after material recovery architecture changes.

Recover into an appropriately isolated environment, verify record integrity and permissions, reconcile integration state, and confirm that retrying operations cannot duplicate business effects. Preserve activity recorded after a backup; do not overwrite newer transactions casually. Record actual recovery time, data loss, defects, and follow up actions. Exercise the incident response procedure at least annually.

Program review and management approval

Continuous improvement

The Security Owner maintains a risk and improvement register containing each issue, source, affected asset or process, severity, owner, target date, status, and closure evidence. Inputs include access reviews, vulnerability checks, incidents, restore exercises, supplier reviews, employee feedback, and changes in Plaid requirements. Known permission defects remain open until remediation has been verified.

Management reviews the program quarterly. Review overdue risks, privileged access exceptions, vulnerability age, incident response performance, restore results, training completion, and supplier changes. Select measurable improvements, assign resources and deadlines, and verify outcomes at the next review. Track control status as planned, implemented, tested, or requiring correction so documentation does not overstate operational maturity.

Exceptions and evidence

An exception must identify the unmet requirement, business reason, exposure, compensating controls, owner, expiry, and management approval. Review exceptions at least quarterly and before expiry. Exceptions must not override binding obligations or authorize cross tenant disclosure. Retain evidence of policy approval, access reviews, training, risk decisions, changes, incidents, backups, restore tests, and corrective action closure under the approved retention schedule.

Plaid onboarding statement

The requested questionnaire response is: "Yes — We have a documented policy, procedures, and an operational information security program that is continuously matured." Management should use that response only after confirming that the documented program is operating and that supporting records are available. Creating this policy alone does not establish operational effectiveness, certification, or Plaid approval.

Approval and operational confirmation

Before external submission, management must complete the fields below, approve the requirements and review cadence, confirm actual implementation, and record any gaps in the risk register. Validate the Plaid use case, data inventory, encryption and credential controls, incident contact, access review records, and recovery evidence. This document covers the quoted question; other questionnaire items may need separate evidence.

Legal operating entity: _____
 Accountable executive and title: _____
 Security Owner and backup: _____
 Incident reporting email or channel: _____
 Approval signature and date: _____
 Effective date and next annual review: _____
 Evidence register location: _____

Reference basis

Prepared using AiInventoryPro.com project security and tenant requirements and the current project handoff. Those records establish requirements and reported work, not a comprehensive operating control assessment. External references were reviewed October 2, 2026. The cadence and procedures in this document are proposed AiInventoryPro.com policy requirements.

Plaid Developer Policy — security, access, and data handling obligations
<https://plaid.com/developer-policy/>
 Plaid Launch Checklist — integration readiness guidance
<https://plaid.com/docs/launch-checklist/>