3PINOS S.A.S. · 3 PINOS LLC

NIT 901.670.004

DATA RETENTION AND DISPOSAL POLICY

Field	Content
Issuing entities	3PINOS S.A.S. and its sister company 3 PINOS LLC (United States), jointly “3 Pinos” or “the Company”
NIT	901.670.004 (3PINOS S.A.S.)
Principal domicile	Villas del Campo L.59, El Retiro, Antioquia, Colombia
Legal representative	Mauricio Vásquez Barrera — C.C. 8.101.801
Document	Data Retention and Disposal Policy
Code	PL-SI-003
Version	1.1
Approval date	October 22, 2026
Approved by	Mauricio Vásquez Barrera — Legal Representative
Policy owner	Information Security Officer (ISO) — Mauricio Vásquez Barrera
Scope	All data held by the Company in the MyFitERP platform and its supporting systems, including consumer financial data received through Plaid, client accounting records, personal data and operational records
Review cycle	At least annually, and whenever applicable law, a vendor agreement or a data flow changes
Related documents	PL-SI-001 Information Security Policy and Procedures · PL-SI-002 Access Control Policy and Procedures · PL-CUM-011 Personal Data Processing Policy · MyFit ERP Privacy Policy (myfiterp.com/privacy)
Classification	Public — may be shared with clients, financial institutions, payment and data providers

1. Purpose

This Policy defines how long 3 Pinos keeps each category of data it holds, how that data is disposed of when it is no longer needed, and how requests for deletion are handled. It gives effect to the data minimization principle of PL-SI-001 and to the retention commitments made to clients, to the account holders whose financial data reaches the Company through Plaid, and to the authorities whose rules require certain records to be kept.

2. Scope

This Policy applies to every system where the Company stores data: the MyFitERP production database and file storage, backups, logging services, email and collaboration tools, endpoint devices and any

vendor that processes Company or client data (Annex C of PL-SI-001). It binds all personnel and contractors of 3PINOS S.A.S. and 3 PINOS LLC.

3. Principles

- **Retention is tied to purpose or to law.** Data is kept only while it serves the purpose for which it was collected or while a legal obligation requires it; whichever ends later determines the retention period.
- **Consumer financial data belongs to the account holder.** Data received through Plaid is kept only while the account holder's authorization is in force and is deleted promptly once it is withdrawn.
- **Disposal is irreversible and verifiable.** Deletion removes the data from active systems and lets it expire from backups; the action is recorded.
- **No local copies.** Restricted data is not downloaded to or kept on endpoint devices, email or personal storage beyond the immediate task.
- **Legal holds prevail.** When data is subject to an investigation, dispute or regulatory request, it is preserved until the hold is lifted, regardless of the schedule below.

4. Roles and Responsibilities

Role	Responsibilities
Legal Representative	Approves this Policy; decides on legal holds and on exceptions.
Information Security Officer (ISO)	Owns the retention schedule; receives and tracks deletion requests; verifies disposals; runs the periodic reviews of Annex B of PL-SI-001.
Technology Owner	Implements deletion in the platform, file storage and vendor integrations; keeps backup and log retention settings aligned with this Policy.
Client administrators (MyFitERP)	Request deletion of their company's data and of their users through the Company's channels.

5. Retention Schedule

Retention periods are maximums for active systems. Where a period is defined by law, the Company applies the longest period required in the jurisdictions where it operates (Colombia and the United States).

Data category	Examples	Retention in active systems	Disposal trigger
Consumer financial data received through Plaid	Plaid access tokens, account identifiers, balances, transactions	While the account holder's authorization and the client's contract are in force	Revocation of the connection, closure of the client account or a deletion request: the Plaid connection (Item) is removed and the associated data is deleted within 30 days, except bank transactions already reconciled or linked to an imported bank statement, which are retained in minimized form as accounting records (see Section 6).
Client accounting records	Journal entries, invoices, supporting documents, financial statements	For the period required by applicable law: ten (10) years in Colombia (Law 962 of 2005, art. 28; Commercial Code, art. 60) and the period required by United States federal and state law for United States clients	Expiry of the legal period, or earlier return or deletion at the client's request where the law allows
Client company and user account data	Company profile, user names and emails, roles, settings	For the duration of the client contract	Deleted or irreversibly anonymized within twelve (12) months after the contract ends, except data subject to a legal retention period
Personal data processed under PL-CUM-011	Contact data of clients, suppliers, employees and beneficiaries	As defined in PL-CUM-011 and the Privacy Policy	End of the purpose or exercise of the data subject's rights, subject to legal retention
Security, compliance and audit records	Access reviews, incident records, deletion logs, vendor reviews, screening evidence	Ten (10) years, aligned with PL-CUM-001 §15	Expiry of the period
Application, request and cloud audit logs	Infrastructure audit logs, application request logs	Retained under the cloud provider's logging retention (30 days by default), longer only when an incident investigation requires it	Automatic expiry

Data category	Examples	Retention in active systems	Disposal trigger
Database backups	Automated backups and point-in-time recovery logs	A limited rolling period of at least seven (7) days	Automatic expiry: data deleted from production leaves the backups when the rolling period elapses
Email and collaboration content	Corporate mailboxes, shared documents	Duration of the business need; Restricted data is never kept here (PL-SI-001 §5)	Deleted by the owner when no longer needed; mailboxes closed at offboarding

6. Disposal Procedures

- **Consumer financial data (Plaid).** The Technology Owner removes the Item through Plaid's API, deletes the access token and the stored account and transaction records from the production database, and records the action with the date and the requesting party. Bank transactions already reconciled or linked to an imported bank statement are not deleted: they are retained in minimized form (date, amount, description and reconciliation match only, with no access tokens or Plaid identifiers) as accounting support, for the accounting-records retention period set in Section 5. Connections that fail or are no longer used are identified and removed in the quarterly review of PL-SI-001, Annex B.
- **Database records and files.** Deletion is performed through the platform's own procedures so that related records, files in cloud storage and derived data are removed consistently. Deleted data expires from backups at the end of the rolling backup period and is not restored except to recover from a verified loss, in which case the deletion is re-applied.
- **Vendors.** When a vendor engagement ends, the Company requests deletion or return of the data held by the vendor and keeps the vendor's confirmation.
- **Physical media.** Production systems run on managed cloud infrastructure; media sanitization is performed by the cloud provider under its certified controls. Endpoint devices used for Company work are wiped before reuse, return or disposal.
- **Records of disposal.** Every disposal performed on request, and every periodic cleanup, is logged by the ISO with the data category, the trigger, the date and the person who executed it.

7. Deletion Requests

- Requests may come from a client administrator, from an account holder whose financial data was connected through Plaid, or from a data subject under PL-CUM-011. They are received at ethics@myfiterp.com or through the client's administrator in the platform.
- The ISO verifies the identity and authority of the requester before acting.
- Requests are fulfilled within thirty (30) days of verification. If a legal retention period or a legal hold prevents deletion of part of the data, the requester is informed of what is retained and why, and that data is restricted to the retention purpose only.
- The requester receives written confirmation when the deletion is complete.

8. Legal Holds and Exceptions

The Legal Representative may order a legal hold on specific data in connection with an investigation, a dispute, a regulatory or law-enforcement request, or an incident under PL-SI-001. Data under hold is excluded from scheduled disposal, its access is limited to the persons handling the matter, and the hold is reviewed at least every six months and lifted in writing. Any other exception to this Policy requires written approval from the ISO with a documented reason and an expiration date.

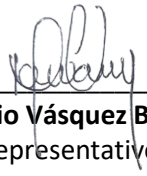
9. Monitoring and Review

- Compliance with the retention schedule is verified in the quarterly reviews of PL-SI-001, Annex B (Plaid connections, backup settings) and in the annual risk and policy review.
- Backup and log retention settings are checked against this Policy whenever infrastructure changes.
- This Policy is reviewed at least annually by the ISO and approved by the Legal Representative, and earlier when applicable law, a vendor agreement or a data flow changes.

10. Review and Approval

Version	Date	Description	Approved by
1.0	October 15, 2026	Initial issue	Legal Representative
1.1	October 22, 2026	Clarifies that bank transactions already reconciled or linked to an imported bank statement are retained in minimized form as accounting records after a Plaid disconnection (Sections 5 and 6).	Legal Representative

In witness of its approval, this document is signed in El Retiro, Antioquia, Colombia, on October 22, 2026.



_____

Mauricio Vásquez Barrera
Legal Representative and Information Security Officer
3PINOS S.A.S. — NIT 901.670.004 · 3 PINOS LLC
C.C. 8.101.801