3PINOS S.A.S. · 3 PINOS LLC

NIT 901.670.004

INFORMATION SECURITY POLICY AND PROCEDURES

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	Information Security Policy and Procedures
Code	PL-SI-001
Version	1.0
Approval date	October 15, 2026
Approved by	Mauricio Vásquez Barrera — Legal Representative
Information Security Officer	Mauricio Vásquez Barrera
Scope	All information, systems, personnel and third parties of 3 Pinos, including the MyFitERP platform operated by the Company and any consumer financial data received through Plaid
Review cycle	At least annually, and after any significant incident or change in systems or regulation
Related documents	PL-SI-002 Access Control Policy and Procedures · PL-CUM-001 Fraud and Corruption Prevention Policy · PL-CUM-008 Control List Screening Procedure · PL-CUM-011 Personal Data Processing Policy
Classification	Public — may be shared with clients, financial institutions, payment and data providers

1. Purpose

This Policy establishes how 3 Pinos identifies, mitigates and monitors information security risks relevant to its business. It defines the principles, roles, minimum controls and operating procedures that protect the confidentiality, integrity and availability of the information the Company handles: its own, its clients’, and the financial data that clients and their end users entrust to the MyFitERP platform, including bank account and transaction data obtained through Plaid.

2. Scope

This Policy is mandatory for:

- Shareholders, legal representatives, employees and contractors of 3PINOS S.A.S. and 3 PINOS LLC.

- All systems used to store, process or transmit Company or client information: the MyFitERP application (backend, frontends, database and integration services), its authentication services, the corporate website, cloud infrastructure, source code repositories, email and collaboration tools, and endpoint devices.
- Third-party service providers that access, host or process Company or client information.
- AI-assisted development and operations tools used by authorized personnel.

3. Principles

- **Least privilege.** Access is granted only to the extent required for a defined role and task.
- **Defense in depth.** No single control is relied upon; identity, network, application and data controls overlap.
- **Data minimization.** The Company collects and retains only the data needed to deliver the contracted service.
- **Human accountability.** Every change to production systems has a named human owner who approves it, including changes prepared with AI-assisted tools.
- **Risk-based approach.** Controls are prioritized according to the risk assessment in Section 6 and Annex A.
- **Continuous monitoring.** Controls are verified on a defined schedule (Annex B) and evidence is retained.

4. Governance and Roles

Role	Responsibilities
Legal Representative	Approves this Policy and its updates; allocates resources; receives security reports; ultimate accountability for information security.
Information Security Officer (ISO)	Maintains this Policy, the risk register and the asset inventory; runs access reviews and control monitoring; leads incident response; manages vendor security; reports to the Legal Representative at least quarterly.
Technology Owner	Approves every change deployed to production; manages cloud configuration, secrets, backups and vulnerability remediation.
Personnel and contractors	Comply with this Policy; protect credentials and devices; report suspected incidents immediately to the ISO.

Given the size of the Company, a single person may hold more than one role. Where segregation of duties is not possible, compensating controls apply: immutable audit logs in the cloud provider, version-controlled change history, automated alerts, and the periodic reviews in Annex B.

5. Information Classification

Level	Examples	Minimum handling
Restricted	Plaid access tokens, API keys, credentials, encryption keys, bank account and transaction data, client financial records, identity documents	Must be encrypted in transit and at rest; stored only in approved systems; access limited to named roles; never sent by email or chat; never placed in source code.

Level	Examples	Minimum handling
Confidential	Client contracts, internal financial reports, source code, system configuration	Access on a need-to-know basis; stored only in approved Company systems.
Internal	Procedures, internal communications	Not shared outside the Company without approval.
Public	Website content, published policies	No restriction.

6. Risk Management

The Company identifies, assesses and treats information security risks through the following procedure:

- **Identify.** The ISO maintains an inventory of information assets and systems (Annex C) and a risk register (Annex A) covering threats to confidentiality, integrity and availability.
- **Assess.** Each risk is rated by likelihood and impact (High / Medium / Low). Risks involving Restricted data are rated at least Medium impact.
- **Mitigate.** Each risk is assigned controls, an owner and a treatment decision (mitigate, transfer, avoid or accept). Residual High risks require Legal Representative approval.
- **Monitor.** Controls are verified on the schedule in Annex B. The risk register is reviewed at least annually and whenever a new system, vendor, integration or significant incident occurs.

7. Security Controls

7.1 Identity and access management

- Every user has a unique, named account. Shared accounts are not permitted for production systems.
- Multi-factor authentication (MFA) is required for the cloud console, source code repositories, corporate email, the identity provider's administrative console, and the administrative dashboards of payment and data providers. MFA is also required for every user of the MyFitERP application and is enforced by the MyFitERP authentication service.
- MyFitERP keeps a single directory of user identities. Users sign in through the Company's central login service, which verifies their credentials (salted password hashes or Google sign-in) and issues signed, time-limited access tokens; API, analytics and AI-assisted access is authenticated through Auth0 using OAuth 2.0 and OpenID Connect and is mapped to the same user identity. Access within the application is governed by role-based permissions scoped per client company (tenant): a user can only access data of the companies to which they are assigned. Access to cloud infrastructure uses Company-managed Google identities.
- Access is granted on request with ISO approval, reviewed quarterly, and revoked within one business day of a role change or termination through the deprovisioning procedure of PL-SI-002.
- Service accounts use the minimum permissions needed and are reviewed with user access.

7.2 Data protection and encryption

- All traffic to Company applications must be served over HTTPS (TLS 1.2 or higher). Unencrypted HTTP is not accepted.
- Databases, file storage and backups must be encrypted at rest (AES-256 or equivalent provided by the cloud provider).

- Secrets, API keys and Plaid access tokens must be kept server-side only, in managed secret storage or encrypted database fields, and must never be exposed to browsers, logs or source code repositories.
- File downloads containing Restricted or Confidential data must be delivered through authenticated, time-limited access.

7.3 Infrastructure and network security

- Production systems run on managed cloud services (Google Cloud Platform) and inherit the provider's physical, environmental and network security controls. Production data must be hosted in the United States region.
- Database access is restricted to authorized service identities and authenticated administrative connections; the database must not be exposed to anonymous access.
- Access to production systems is permitted only from devices and identities that are authorized and controlled by the Company.

7.4 Secure development and change management

- All source code is stored in private, access-controlled repositories with full version history.
- Every change to production must be traceable to a commit, approved by the Technology Owner before deployment, and deployed through an automated build process.
- AI-assisted development and operations tools operate only on authorized Company workstations, under the identity and supervision of the authorized person who uses them. Every change they prepare requires human approval before it is merged or deployed.
- AI providers that may process Restricted data must be bound, by contract or by account configuration, not to use that data to train their models.
- Database schema changes are applied through versioned, sequential migrations with a recorded risk level.
- Automated dependency vulnerability alerts must be enabled on all source code repositories; third-party dependencies are kept within supported versions and updated when security advisories are published.

7.5 Vulnerability and patch management

- Critical and high-severity vulnerabilities in Company systems or dependencies are remediated within 15 and 30 days respectively of identification; others in the next scheduled update.
- Automated vulnerability scanning must run on production container images and on endpoint devices used for Company work.
- Managed services are kept on supported versions; endpoint operating systems and browsers have automatic updates enabled.

7.6 Logging and monitoring

- Cloud audit logs record administrative activity on infrastructure; application request logs are retained in the cloud provider's logging service.
- Automated alerts are investigated promptly. The ISO reviews security-relevant events, deployment history and access anomalies at least quarterly and records the review.

7.7 Endpoint security

- Devices used for Company work must have full-disk encryption, a screen lock, automatic updates and active anti-malware protection.

- Lost or stolen devices are reported to the ISO immediately; associated sessions and credentials are revoked.

7.8 Business continuity and backups

- Production databases must have automated daily backups with point-in-time recovery, retained for at least 7 days.
- Source code is replicated in the hosted repository and on authorized workstations.
- A restore test is performed at least annually and its result documented.

8. Consumer Financial Data (Plaid)

Data obtained through Plaid is Restricted information and is handled under the following additional rules:

- It is collected only with the explicit consent of the account holder, through Plaid's own interface, and used solely to provide the service the client requested (such as bank reconciliation and accounting).
- Plaid access tokens must be stored server-side, encrypted, and associated with the client company that authorized them.
- The data is never sold, shared with third parties for marketing, or used for purposes the account holder did not authorize.
- When a client revokes access, closes its account or requests deletion, the Company must remove the Plaid connection (item) and delete the associated consumer data within 30 days, except where retention is required by law.
- Connections that fail or are no longer in use are identified and removed as part of quarterly monitoring.

9. Third-Party and Vendor Management

- Before engaging a vendor that will access or host Restricted or Confidential data, the ISO verifies its security posture (for example, SOC 2 or ISO 27001 reports) and its data processing terms.
- Approved vendors are listed in Annex C and reviewed annually. A new vendor is added to Annex C before it receives Company or client data.
- Vendors receive only the access needed for their service, and their access is removed when the engagement ends.

10. Incident Response Procedure

Step	Action
1. Detect and report	Anyone who suspects an incident reports it to the ISO immediately (ethics@3pinos.com or directly to the Legal Representative).
2. Triage	The ISO confirms the incident, classifies its severity and records it in the incident log.
3. Contain	Revoke compromised credentials or tokens, isolate affected services, rotate secrets.
4. Eradicate and recover	Remove the cause, restore from clean backups if required, verify integrity.

Step	Action
5. Notify	Notify affected clients, Plaid and other affected partners without undue delay, and no later than 72 hours after confirming an incident involving their data; notify authorities where the law requires (including the Superintendencia de Industria y Comercio in Colombia).
6. Learn	Document root cause and corrective actions within 15 days; update the risk register and controls.

11. Personnel Security and Awareness

- New personnel and contractors acknowledge this Policy in writing before receiving access.
- Everyone with access to Company systems completes security awareness training at onboarding and annually, covering phishing, credential protection, data handling and incident reporting.
- Confidentiality obligations are included in employment and service contracts and survive their termination.

12. Compliance and Exceptions

Breaches of this Policy may result in disciplinary or contractual measures. Exceptions require written approval from the ISO, a documented risk assessment and an expiration date. The Company complies with applicable data protection law, including Colombian Law 1581 of 2012 and United States federal and state requirements applicable to its operations.

13. Review and Approval

This Policy is reviewed at least annually by the ISO and approved by the Legal Representative. Version history is kept in the table below.

Version	Date	Description	Approved by
1.0	October 15, 2026	Initial issue	Legal Representative

Annex A — Information Security Risk Register (summary)

L = likelihood, I = impact (H/M/L). Full register maintained by the ISO and reviewed at least annually.

#	Risk	L/I	Key controls	Monitoring	Owner
R1	Account takeover of cloud, repository, identity provider or email accounts	M/H	MFA on all critical accounts; unique accounts; prompt revocation	Quarterly access review; audit log review	ISO
R2	Leakage of secrets or Plaid access tokens	M/H	Server-side secret storage; no secrets in code or logs; rotation on suspicion	Quarterly review; rotation after incidents	Tech Owner
R3	Cross-tenant data exposure in MyFitERP	L/H	Tenant-scoped authorization on every request; role-based permissions	Review on every access-control change	Tech Owner

#	Risk	L/I	Key controls	Monitoring	Owner
R4	Unreviewed or faulty change deployed to production	M/M	Human approval of every change; versioned migrations; automated builds	Quarterly deployment history review	Tech Owner
R5	Vulnerable third-party dependency	M/M	Automated dependency alerts; supported versions; remediation SLAs (Section 7.5)	Monthly triage of automated alerts	Tech Owner
R6	Data loss or extended outage	L/H	Automated daily backups with point-in-time recovery; managed infrastructure	Quarterly backup status; annual restore test	Tech Owner
R7	Phishing or social engineering	M/M	Awareness training; MFA; out-of-band confirmation of payment changes	Annual training record	ISO
R8	Lost or stolen device	L/M	Full-disk encryption; screen lock; remote session revocation	Quarterly device check	ISO
R9	Vendor security failure	L/H	Vendor due diligence; least-privilege vendor access	Annual vendor review	ISO
R10	Retention of consumer data beyond need	L/M	Deletion within 30 days of revocation; removal of unused Plaid items	Quarterly review of Plaid connections	ISO

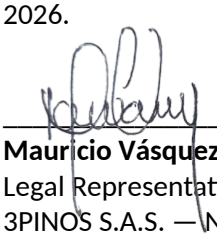
Annex B — Control Monitoring Schedule

Control	Frequency	Evidence retained
Triage of automated dependency and security alerts	Monthly	Remediation tickets / commits
User and service-account access review (all critical systems)	Quarterly	Signed review record (PL-SI-002, Annex B)
MFA enforcement check on critical accounts	Quarterly	Screenshot or export of account settings
Audit log and access-anomaly review	Quarterly	Review note in security log
Deployment and change history review	Quarterly	Repository and build history
Backup status verification	Quarterly	Backup console record
Plaid connection review and removal of unused items	Quarterly	Connection list and removal log
Backup restore test	Annually	Test report
Security awareness training	Onboarding and annually	Training acknowledgment
Vendor security review	Annually	Vendor review record
Risk register and Policy review	Annually	Approved new version

Annex C — Systems and Critical Vendors

System / vendor	Use	Data level
Google Cloud Platform (Cloud Run, Cloud SQL, Cloud Storage, Secret Manager, Cloud Build, Cloud Logging)	Hosting, database, file storage, secrets, builds and logs for MyFitERP and the corporate website	Restricted
Auth0 (Okta)	Identity provider for API, analytics and AI-assisted access to MyFitERP (OAuth 2.0 / OpenID Connect)	Restricted
Plaid	Bank account connectivity authorized by clients	Restricted
Stripe	Invoice payment processing	Restricted
Anthropic (Claude)	AI-assisted development and operations under human supervision, including access to client financial records on behalf of an authorized user	Restricted
MATIAS	Electronic invoicing and support documents before the Colombian tax authority (DIAN)	Confidential
Notion	Synchronization of selected client records (such as investor directories) to client workspaces, at the client's request	Confidential
GitHub	Private source code repositories	Confidential
Microsoft 365	Corporate email and scheduling (3 Pinos)	Confidential
Google Workspace	Email and collaboration (MyFitERP)	Confidential

In witness of its approval, this document is signed in El Retiro, Antioquia, Colombia, on October 15, 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