3PINOS S.A.S. · 3 PINOS LLC

NIT 901.670.004

ACCESS CONTROL 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	Access Control Policy and Procedures
Code	PL-SI-002
Version	1.0
Approval date	October 15, 2026
Approved by	Mauricio Vásquez Barrera — Legal Representative
Policy owner	Information Security Officer (ISO) — Mauricio Vásquez Barrera
Scope	Logical access to all Company systems and data, including the MyFitERP platform, its authentication services, cloud infrastructure, source code, corporate tools and consumer financial data received through Plaid
Review cycle	At least annually, and after any significant incident or change in systems
Related documents	PL-SI-001 Information Security Policy and Procedures · PL-CUM-001 Fraud and Corruption Prevention Policy · PL-CUM-011 Personal Data Processing Policy
Classification	Public — may be shared with clients, financial institutions, payment and data providers

1. Purpose

This Policy defines how 3 Pinos grants, uses, reviews and revokes access to its information systems and data, so that only authorized persons and services can access information, and only to the extent required for their role. It develops Section 7.1 of the Information Security Policy (PL-SI-001).

2. Scope

This Policy applies to every account that can access Company or client information:

- Personnel and contractors of 3PINOS S.A.S. and 3 PINOS LLC.
- Client users of the MyFitERP platform.
- Service accounts, API keys and integration credentials, including those used with Plaid and Stripe.
- Vendors with access to Company systems.

- AI-assisted development and operations tools used by authorized personnel.

It covers: cloud infrastructure (Google Cloud Platform), the MyFitERP application and database, the MyFitERP authentication services (central login service and Auth0), source code repositories (GitHub), corporate email and collaboration (Microsoft 365, Google Workspace), and the administrative dashboards of payment and data providers (Stripe, Plaid).

3. Principles

- **Least privilege.** Each account receives the minimum permissions required for its role and task.
- **Need to know.** Access to Restricted data (as defined in PL-SI-001) requires a documented business need.
- **Unique identity.** Every person and service uses its own account; shared or generic accounts are prohibited for production systems.
- **Default deny.** Access not expressly granted is denied.
- **Accountability.** Every access grant has a named approver and is recorded.
- **Segregation of duties.** Where the size of the Company prevents full segregation, the compensating controls in Section 10 apply.

4. Roles and Responsibilities

Role	Responsibilities
Legal Representative	Approves this Policy; approves privileged access and exceptions.
Information Security Officer (ISO)	Approves and records access requests; performs quarterly access reviews; revokes access; maintains the access matrix (Annex A) and access records (Annex B).
System administrators	Implement approved grants and revocations; never self-approve their own access.
Client administrators (MyFitERP)	Request, approve and revoke access for their own company's users within the roles the platform allows.
All users	Protect their credentials; do not share accounts; report suspected misuse immediately.

5. Authentication Requirements

- **Centralized identity.** MyFitERP keeps a single directory of user identities. Users sign in through the Company's central login service (salted password hashes or Google sign-in), which issues signed, time-limited access tokens. API, analytics and AI-assisted access is authenticated through Auth0 (OAuth 2.0 and OpenID Connect) and mapped to the same user identity. Personnel access to cloud infrastructure uses Company-managed Google identities.
- **Token validation.** The MyFitERP backend must validate the signature and expiry of every access token (and the issuer and audience of tokens issued by Auth0), and must reject requests from accounts that have been disabled, even before their tokens expire.
- **Multi-factor authentication (MFA)** is mandatory for: the cloud console, source code repositories, corporate email, the database administrative access path, the Auth0 administrative console, the Stripe and Plaid dashboards, and every user of the MyFitERP application (enforced by the MyFitERP authentication service).

- **Non-human authentication.** Service-to-service and integration access uses OAuth 2.0 client credentials or provider-issued API keys, always over TLS.
- Passwords must be at least 12 characters, unique per system, and stored only in an approved password manager. Passwords are never shared, written down or sent by email or chat.
- Default credentials are changed before any system goes into use.
- Credentials suspected of compromise are changed immediately and the event is handled under the incident response procedure of PL-SI-001.

6. Authorization Model

6.1 Internal systems

Internal access is assigned by role according to the access matrix in Annex A. Administrative (privileged) roles are limited to the persons named by the Legal Representative. Cloud infrastructure permissions must be granted to Company-managed groups rather than to individual accounts, so that disabling a person's identity removes their infrastructure access.

6.2 MyFitERP platform (client data)

- Access is role-based and scoped per client company (tenant). Every request is authorized against explicit permissions of the user's roles in the companies assigned to them; a user cannot read or modify data of a company to which they are not assigned. Authorization must never be based on role names alone.
- Menus, functions and actions available to each user are controlled by role assignments stored in the platform.
- Company personnel access a client's data only to provide the contracted service or support, with the client's authorization.
- Plaid-connected bank data is visible only to users of the client company that authorized the connection.

6.3 Service accounts and API credentials

- Service accounts are created for a specific system or integration, with the minimum permissions needed, and are not used interactively by people.
- API keys and tokens (including Plaid and Stripe credentials) must be stored only in managed secret storage or encrypted server-side fields, and are rotated when personnel with knowledge of them leave or when compromise is suspected.

6.4 AI-assisted tools

AI-assisted development and operations tools operate only on authorized Company workstations, under the identity, permissions and supervision of the authorized person who uses them. Every change they prepare is reviewed and approved by a human before it is merged or deployed.

7. Access Lifecycle Procedures

Procedure	Steps	Timing
Request and grant	1) Requester or manager submits the request stating system, role and justification. 2) ISO approves (privileged access also requires Legal Representative approval). 3) Administrator grants the access. 4) Grant is recorded in the access log (Annex B).	Before access is used
Change of role	Access no longer needed is removed and new access follows the request-and-grant procedure.	Within 1 business day of the change
Revocation (offboarding)	Execute the deprovisioning procedure (Section 7.1), recover devices, and rotate any shared secret the person knew. Record the revocation.	Within 1 business day; immediately for termination for cause
Vendor access	Granted for a defined purpose and period, with least privilege; removed when the engagement ends.	At engagement end
Client user access (MyFitERP)	Created at the request of the client's authorized administrator; removed at their request or when the client relationship ends.	Within 1 business day of request

7.1 Deprovisioning procedure

Revocation is executed as a single recorded action that covers every production asset:

- **MyFitERP:** the account is disabled in the authentication services (central login service and Auth0), its active sessions are revoked, its role assignments are removed in every client company, and the action is written to the application audit log.
- **Cloud infrastructure:** the person's Company-managed identity is disabled or removed from the groups that carry infrastructure permissions.
- **Source code repositories:** the person is removed as a collaborator from every repository.
- **Systems without a team-management interface** (such as the Stripe and Plaid dashboards and Microsoft 365): the procedure produces a checklist that the administrator completes and records in Annex B.

8. Privileged Access

- Privileged accounts (cloud owner/administrator, database administrator, identity provider administrator, repository owner, payment and data provider administrator) are held only by persons named by the Legal Representative.
- Privileged access always requires MFA and is used only for administrative tasks.
- Administrative actions on cloud infrastructure are recorded in the provider's audit logs, which cannot be altered by the administrator.
- Emergency (break-glass) access, if ever used, is recorded and reviewed by the Legal Representative within 2 business days.

9. Access Reviews

- The ISO reviews all user, privileged and service accounts in every system of Annex A quarterly, confirming that each account is still needed, correctly scoped and protected by MFA where required.
- Inactive accounts (no use for 90 days) are disabled unless justified.
- The result of each review, and any access removed, is recorded and signed by the ISO (Annex B).
- MyFitERP client administrators are reminded at least annually to review their own users.

10. Segregation of Duties and Compensating Controls

Because the Company is small, the same person may approve and administer access. In that case the following compensating controls apply: immutable cloud audit logs; version-controlled history of all code and configuration changes; quarterly reviews documented in writing and reported to the Legal Representative; and no person may approve access for themselves outside the privileged-access rules of Section 8.

11. Monitoring and Logging

Access events are logged by the cloud provider, the identity providers and the MyFitERP application. Automated alerts are investigated promptly, and the ISO reviews access anomalies and failed authentication patterns at least quarterly.

12. Exceptions and Violations

Exceptions require written approval from the ISO, a documented risk assessment and an expiration date. Violations of this Policy, including account sharing or unauthorized access, may result in disciplinary or contractual measures and in the immediate suspension of access.

13. Review and Approval

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

Annex A — Access Matrix

Roles authorized per system. Named assignments are kept in the access log maintained by the ISO.

System	Roles / access levels	Who may hold privileged access	Authentication	Review
Google Cloud Platform	Owner/Admin; Developer; service accounts per service	Persons named by the Legal Representative	Google identity + MFA; permissions granted through groups	Quarterly
Cloud SQL (MyFitERP database)	Administrator; application service identity	Technology Owner	Cloud SQL Auth Proxy (IAM) + MFA on the Google identity	Quarterly

System	Roles / access levels	Who may hold privileged access	Authentication	Review
Auth0 (identity provider)	Tenant administrator; machine-to-machine applications (server-side only)	Persons named by the Legal Representative	MFA; client secrets in managed secret storage	Quarterly
MyFitERP application	Platform administrator; client administrator; client user roles per tenant	Platform administrators named by the Legal Representative	Central login service (password or Google sign-in) + MFA; Auth0 (OAuth 2.0 / OpenID Connect) for API and AI access; signed access tokens	Quarterly (internal); annually (client)
GitHub	Owner; Collaborator (write); read-only	Repository owner	MFA	Quarterly
Microsoft 365 / Google Workspace	Global admin; user	Legal Representative	MFA	Quarterly
Stripe	Administrator; Developer; View-only	Legal Representative	MFA	Quarterly
Plaid dashboard and API	Administrator; Developer; API credentials (server-side only)	Legal Representative	MFA; secret storage for keys	Quarterly

Annex B — Access Request and Review Record (template)

Each grant, change, revocation and quarterly review is recorded with at least the following fields:

Date	Type (grant / change / revoke / review)	System	Account	Role / scope	MFA verified	Justification / result	Approved by	Executed by

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