ACCESS CONTROL POLICY – AFINCE

Effective Date: April 14, 2026

1. PURPOSE
This policy defines how access to systems, applications, and sensitive data is controlled and restricted to authorized users only.

2. SCOPE
This policy applies to all systems, infrastructure, and data managed by Afince, including backend services, databases, and third-party integrations.

3. ACCESS CONTROL PRINCIPLES
- Access is granted based on the principle of least privilege.
- Only authorized users can access production systems.
- Access is role-based and aligned with user responsibilities.

4. AUTHENTICATION
- All users must authenticate securely (e.g., Firebase Authentication).
- Strong passwords are required.
- Multi-factor authentication (MFA) is used where applicable.

5. AUTHORIZATION (RBAC)
- Role-Based Access Control (RBAC) is implemented.
- Users are assigned roles that determine permissions.
- Access is limited to only what is necessary.

6. DATA PROTECTION
- All data is transmitted using HTTPS encryption.
- Sensitive data is stored securely using trusted infrastructure.
- Access to financial data is restricted and monitored.

7. ACCESS MANAGEMENT
- Access is granted only when necessary.
- Access is revoked when no longer needed.
- Systems are managed through centralized identity services.

8. THIRD-PARTY SERVICES
- Third-party providers (e.g., Plaid) are used securely.
- Access to third-party data follows strict security controls.

9. MONITORING AND SECURITY
- Systems are monitored for unauthorized access.
- Security measures are continuously reviewed and improved.

10. COMPLIANCE
Afince follows industry best practices to protect user data and maintain secure access controls.

11. CONTACT
Email: support@afince.com
Website: https://afince.com