uncletimdigital@gmail.com | 08107198344
UNCLETIMTECH.COM

ACCESS MANAGEMENT AND MFA POLICY

Version 1.0 | Effective: 2 November 2026 | Owner: Director / DPO | Review: Annually or after any major change

1. Purpose

This policy governs how access to UNCLETIM systems, partner platforms (including 9PSB and Prembly dashboards and APIs), and customer data is requested, granted, reviewed, and withdrawn, and mandates multi-factor authentication (MFA).

2. Principles

- Least privilege: users receive only the access their role requires.
- Unique identity: every user has an individual account; shared or generic accounts are prohibited.
- Segregation: administrative accounts are separate from day-to-day accounts and used only for administration.

3. Access lifecycle

Stage	Requirement
Request and approval	Access is requested in writing (email) and approved by the Director before provisioning.
Provisioning	Accounts are created with role-based permissions; MFA enrolment is completed at first sign-in.
Change of role	Permissions are adjusted within one (1) business day of a role change; unnecessary rights are removed.
Exit / termination	All access is revoked on or before the individual’s last working day, and API keys they could access are rotated.
Review	The Director reviews all user and privileged access quarterly and removes dormant or excessive rights. Dormant accounts are disabled after 30 days of inactivity.

4. Authentication and MFA

- MFA is mandatory for: all cloud and email accounts, all partner/banking platforms, remote access, administrative consoles, and the credential vault. Authenticator-app or hardware-backed factors are preferred; SMS is a fallback only.
- Passwords must be at least 12 characters, unique per system, and stored in the Company credential vault; password sharing is prohibited.
- API keys and secrets: issued per environment, stored only in the credential vault, never in code or email; rotated at least every 90 days and immediately upon suspected compromise or staff exit.

5. Monitoring and enforcement

Sign-in and administrative activity is logged and retained for at least two (2) years. Repeated failed sign-ins trigger account lockout and review. Non-compliance with this policy may lead to access suspension and disciplinary action.

Approved and signed:



Olamide Timilehin Adedayo
Director, Uncletim Digital Solutions LTD
Date: 2 November 2026