

POL-04: ACCESS CONTROL AND IDENTITY GOVERNANCE POLICY

JOHN THOMAS FINTECH PRIVATE LIMITED

CIN: U62099KL2026PTC106017 | Doc ID: JT-ISMS-POL-004

Version: 1.0 | Effective Date: 14-Oct-2026 | Review Cycle: Annual

ISO/IEC 27001:2022 Controls: 5.15 (Access control), 5.16 (Identity management), 5.17 (Authentication information), 5.18 (Access rights), 8.2 (Privileged access rights), 8.3 (Information access restriction)

1. Principles of Access Control

Access to systems and data at JOHN THOMAS FINTECH PRIVATE LIMITED operates under two inviolable tenets:

- 1. Principle of Least Privilege (PoLP):** Users and systems are granted only the minimum permissions necessary to execute authorized job duties.
- 2. Need-to-Know:** Access is strictly bounded by specific business necessity.

2. Identity & Authentication Standards

- 1. Unique Identification:** Every individual is provisioned a distinct, individual user account through the centralized Identity Provider (Google Workspace / Okta SSO). Shared accounts are strictly prohibited.
- 2. Multi-Factor Authentication (MFA):**
 - MFA is **mandatory** for all corporate email accounts, cloud consoles (AWS/GCP), GitHub Enterprise, VPNs, and production infrastructure.
 - Hardware security keys (FIDO2/WebAuthn) or time-based one-time password (TOTP) authenticator apps are required. SMS-based OTP is prohibited for administrative access.
- 1. Password Complexity Standard:**
 - Minimum length: 14 characters.
 - Complexity: Must contain uppercase, lowercase, numbers, and symbols.
 - Screen lock timeout: Endpoints lock after 5 minutes of inactivity.

3. Privileged Access Management (PAM - Control 8.2)

1. **Root Account Security:** AWS root accounts must have hardware MFA enabled and stored securely in an executive safe. Root credentials must never be used for daily operational tasks.
2. **Just-in-Time (JIT) Elevation:** Production database access and administrative cloud permissions are granted on a temporary, time-bound JIT basis and automatically expire after completion of approved maintenance windows.
3. **Session Auditing:** All privileged shell sessions and administrative queries are logged with immutable audit trails.

4. User Access Lifecycle & Periodic Reviews (Control 5.18)

1. **Onboarding:** Access is provisioned upon HR ticket and manager approval based on predefined role templates (PRO-06).
2. **Quarterly Access Review:** The CISO and DevOps leads conduct quarterly audits of all active accounts across AWS, GitHub, databases, and SaaS tools to identify and purge orphaned permissions.
3. **Immediate Revocation:** Upon employee resignation or termination, all account access is revoked within **60 minutes** of the official offboarding notification.