

POL-07: ACCEPTABLE USE OF ASSETS POLICY (AUP)

JOHN THOMAS FINTECH PRIVATE LIMITED

CIN: U62099KL2026PTC106017 | **Doc ID:** JT-ISMS-POL-007

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

ISO/IEC 27001:2022 Controls: 5.10 (Acceptable use of assets), 6.7 (Remote working), 8.1 (User endpoint devices)

1. Purpose & Scope

This policy defines the acceptable and responsible conduct expected of all employees, directors, and contractors when utilizing computer systems, communication networks, mobile devices, internet connectivity, and cloud resources provided by JOHN THOMAS FINTECH PRIVATE LIMITED.

2. General Use & Ownership

- All company-issued laptops, email accounts, cloud workspaces, and generated code remain the exclusive property of the Company.
- Personnel should have no expectation of privacy regarding personal activities conducted on company systems. The Company reserves the right to monitor network traffic, application usage, and system logs in compliance with law.

3. Prohibited Activities

Users must strictly refrain from:

- Installing unlicensed, pirated, peer-to-peer (P2P), or unauthorized third-party software on company endpoints.
- Utilizing public cloud file-sharing services (e.g., personal Google Drive, Dropbox, Mega) to upload company code, contracts, or customer data.
- Pasting proprietary source code, credentials, or customer financial records into public AI generative tools without verified enterprise data confidentiality agreements.
- Attempting to bypass security controls, disabling antivirus/EDR, tampering with MDM configurations, or running unauthorized network vulnerability scanners.
- Conducting commercial activities or hosting external projects on company infrastructure.

4. Remote & Hybrid Working Security (Control 6.7)

1. Remote employees must connect to corporate resources exclusively via approved VPNs or secure Zero Trust Network Access (ZTNA).
2. Connecting company laptops to unsecured public Wi-Fi networks (e.g., airports, cafes) without active VPN encryption is strictly prohibited.
3. Family members or unauthorized third parties are strictly forbidden from viewing, touching, or using company-issued devices.