

POL-01: INFORMATION SECURITY POLICY

JOHN THOMAS FINTECH PRIVATE LIMITED

CIN: U62099KL2026PTC106017 | Doc ID: JT-ISMS-POL-001

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

ISO/IEC 27001:2022 Clause Mapping: Clause 5.2 (Policy), Clause 5.1 (Leadership & Commitment)

1. Purpose & Strategic Intent

JOHN THOMAS FINTECH PRIVATE LIMITED (the "Company") is committed to safeguarding the confidentiality, integrity, and availability (CIA triad) of all information assets, software platforms, customer financial transactions, proprietary algorithms, and supporting computing infrastructure against internal, external, accidental, or malicious security threats.

This Information Security Policy represents the foundational mandate established by the Board of Directors under Clause 5.2 of ISO/IEC 27001:2022. It directs the implementation, operation, monitoring, and continual improvement of our Information Security Management System (ISMS).

2. Policy Scope & Applicability

This policy applies without exception across:

- All organizational functions, including engineering, cloud operations, product design, quality assurance, finance, HR, and executive administration.
- All physical premises, primarily the registered office at **69/1854 A, A1, A2, SRM Road, Ernakulam North, Kochi, Ernakulam - 682018, Kerala, India**, as well as remote working environments authorized by the Company.
- All cloud environments (AWS, GCP, GitHub, Vercel, third-party SaaS tools).
- All employees, executive directors, contractors, consultants, interns, and vendors who access Company systems or client financial data.

3. Core Information Security Principles

The Company's security architecture is guided by the following tenets:

- Confidentiality:** Information is accessible only to authorized persons, systems, and processes on a strict "need-to-know" and "least-privilege" basis.

- **Integrity:** Information assets, financial ledgers, transactional logs, and source code are protected from unauthorized modification, tampering, or corruption.
 - **Availability:** Critical fintech services, APIs, and cloud services are resilient, backed up, and accessible when required by authorized clients and internal systems.
 - **Zero Trust Architecture:** Every access request is continuously verified, authenticated, and authorized regardless of user location or network perimeter.
 - **Privacy by Design:** Compliance with the **Digital Personal Data Protection (DPDP) Act 2023** is integrated into every stage of application development and data processing.
-

4. Top Management Commitments (Clause 5.1)

The Board of Directors and Executive Leadership commit to:

1. Ensuring the ISMS and security objectives align with the strategic direction of John Thomas Fintech Private Limited.
 2. Allocating necessary financial, technological, and human resources to establish and maintain ISO/IEC 27001:2022 controls.
 3. Communicating the importance of effective information security management across the organization.
 4. Ensuring compliance with all applicable statutory, regulatory, and contractual obligations, including:
 - The Companies Act, 2013
 - The Information Technology Act, 2000 and IT (Amendment) Act, 2008
 - The Indian Digital Personal Data Protection Act, 2023
 - CERT-In Directions on Cyber Security Incident Reporting (April 2022)
 - Relevant Reserve Bank of India (RBI) Cyber Security Guidelines for Fintechs and Payment Aggregators/Gateways.
 1. Conducting annual formal Management Reviews and ensuring continual improvement of the ISMS.
-

5. Information Security Objectives Framework (Clause 6.2)

The Company defines measurable, time-bound objectives:

1. **Service Availability:** Maintain at least 99.95% uptime for all client-facing fintech platforms and production APIs.
2. **Vulnerability Mitigation:** Remediate 100% of Critical vulnerabilities within 48 hours and High vulnerabilities within 7 calendar days of detection.
3. **Personnel Competence:** Achieve 100% annual information security awareness training completion for all active personnel.
4. **Data Protection:** Zero confirmed data breaches involving customer Personally Identifiable Information (PII) or financial transactions.

5. **Incident Response:** Acknowledge and contain P1 security incidents within 60 minutes and report relevant cyber incidents to CERT-In within 6 hours.

6. Key Security Domain Mandates

The Company has established formal subsidiary policies supporting this foundational policy:

- P0L-02 : Asset Management Policy
- P0L-03 : Data Classification and Handling Policy
- P0L-04 : Access Control and Identity Governance Policy
- P0L-05 : Cryptography and Key Management Policy
- P0L-06 : Physical and Environmental Security Policy
- P0L-07 : Acceptable Use of Assets Policy
- P0L-08 : Supplier and Third-Party Risk Management Policy
- P0L-09 : Secure Software Development Lifecycle (SSDLC) Policy
- P0L-10 : Vulnerability and Patch Management Policy
- P0L-11 : Clean Desk and Clean Screen Policy
- P0L-12 : Backup and Data Retention Policy

7. Compliance, Monitoring & Enforcement

- Compliance with this policy is mandatory. Periodic internal audits, automated posture scans, and third-party penetration tests will verify adherence.
- Any willful violation, unauthorized disclosure of sensitive financial data, bypass of security controls, or gross negligence constitutes disciplinary misconduct subject to disciplinary action, termination of employment, and civil/criminal prosecution under the Indian IT Act, 2000.

8. Document Governance & Approval

Version	Date	Description of Change	Prepared By	Approved By
1.0	14-Oct-2026	Initial ISO/IEC 27001:2022 Baseline Policy Release	CISO / Security Lead	Board of Directors

Signed for and on behalf of JOHN THOMAS FINTECH PRIVATE LIMITED:

John Thomas

Managing Director & Chief Executive Officer

