

ISO/IEC 27001:2022 INFORMATION SECURITY MANAGEMENT SYSTEM (ISMS)

Master Documentation Toolkit & Audit Package

JOHN THOMAS FINTECH PRIVATE LIMITED

- **Corporate Identification Number (CIN):** U62099KL2026PTC106017
- **Date of Incorporation:** 01 September 2026
- **Permanent Account Number (PAN):** AAHCJ5884B | **TAN:** CHNJ05481A
- **Goods & Services Tax (GSTIN):** 32AAHCJ5884B1ZN
- **Registered Office:** 69/1854 A, A1, A2, SRM Road, Ernakulam North, Kochi, Ernakulam - 682018, Kerala, India
- **Reference MOA:** [17878067411002_INC-33_1-27156774214_MOA.pdf](#)
- **Standard Baseline:** ISO/IEC 27001:2022 & ISO/IEC 27002:2022

Complete Document Directory & Clickable Index

00. Executive Governance & Implementation Roadmap

- [00_EXECUTIVE_SUMMARY_AND_ROADMAP/ISMS Executive Summary and Implementation Roadmap.md](#)
- Executive summary, corporate background, 12-week certification roadmap, and document hierarchy.

01. ISMS Manual & Governance (Clauses 4, 5 & 6)

- [01_MANUAL_AND_GOVERNANCE/POL-01 Information Security Policy.md](#) — *Clause 5.2 Top-level Board policy*
- [01_MANUAL_AND_GOVERNANCE/DOC-01 ISMS Scope and Context of Organization.md](#) — *Clause 4 Context, PESTLE, Interested Parties & Scope*
- [01_MANUAL_AND_GOVERNANCE/DOC-02 ISMS Roles Responsibilities RACI.md](#) — *Clause 5.3 Governance & RACI Matrix*
- [01_MANUAL_AND_GOVERNANCE/DOC-03 ISMS Objectives and Metrics.md](#) — *Clause 6.2 & 9.1 Quantified KPIs & Performance Metrics*

02. Risk Management & Statement of Applicability (SoA)

- [02_RISK_MANAGEMENT_AND_SOA/PRO-01 Risk Assessment and Treatment Methodology.md](#) — *Clause 6.1.2 5x5 Risk Methodology*

- [02_RISK_MANAGEMENT_AND_SOA/REG-01_Information_Security_Risk_Register_and_RTP.md](#) — *Clause 6.1.3 & 8.3 Risk Register & Treatment Plan*
- [02_RISK_MANAGEMENT_AND_SOA/REG-02_Statement_of_Applicability_SoA_IS027001_2022.md](#) — *Clause 6.1.3(d) All 93 Controls across 4 Themes*

03. Domain Policies & Technical Standards (Annex A Alignment)

- [03_POLICIES_AND_STANDARDS/POL-02_Asset_Management_Policy.md](#) — *Controls 5.9, 5.10, 7.10, 7.14*
- [03_POLICIES_AND_STANDARDS/POL-03_Data_Classification_and_Handling_Policy.md](#) — *Controls 5.12, 5.13, 8.11, 8.12 (DPDP Act)*
- [03_POLICIES_AND_STANDARDS/POL-04_Access_Control_Policy.md](#) — *Controls 5.15-5.18, 8.2-8.5 (PoLP, MFA, SSO)*
- [03_POLICIES_AND_STANDARDS/POL-05_Cryptography_and_Key_Management_Policy.md](#) — *Control 8.24 (AES-256, TLS 1.3, KMS)*
- [03_POLICIES_AND_STANDARDS/POL-06_Physical_and_Environmental_Security_Policy.md](#) — *Controls 7.1-7.14 (Kochi Office, Biometrics, CCTV)*
- [03_POLICIES_AND_STANDARDS/POL-07_Acceptable_Use_Policy.md](#) — *Control 5.10 (Hardware, Cloud, Remote Work)*
- [03_POLICIES_AND_STANDARDS/POL-08_Supplier_and_Vendor_Security_Policy.md](#) — *Controls 5.19-5.23 (AWS/GCP, SaaS Due Diligence)*
- [03_POLICIES_AND_STANDARDS/POL-09_Secure_Development_Lifecycle_SSDLC_Policy.md](#) — *Controls 8.25-8.33 (OWASP, CI/CD, SAST, Env Segregation)*
- [03_POLICIES_AND_STANDARDS/POL-10_Vulnerability_and_Patch_Management_Policy.md](#) — *Controls 8.8, 8.19 (VAPT, 48h Critical SLA)*
- [03_POLICIES_AND_STANDARDS/POL-11_Clean_Desk_and_Clean_Screen_Policy.md](#) — *Control 7.7 (Screen locks, Physical shredding)*
- [03_POLICIES_AND_STANDARDS/POL-12_Backup_and_Data_Retention_Policy.md](#) — *Controls 8.13, 8.14 (3-2-1 Backups, Cross-Region, Statutory Retention)*

04. Standard Operating Procedures (SOPs) & Operations

- [04_PROCEDURES_AND_OPERATIONS/PRO-02_Incident_Management_Procedure.md](#) — *Controls 5.24-5.28 (CERT-In 6-Hour Reporting SLA)*
- [04_PROCEDURES_AND_OPERATIONS/PRO-03_Business_Continuity_and_Disaster_Recovery_Plan.md](#) — *Controls 5.29, 5.30 (RTO < 4h, RPO < 15m)*
- [04_PROCEDURES_AND_OPERATIONS/PRO-04_Change_Management_Procedure.md](#) — *Control 8.32 (CAB, Pull Request Approvals, Rollback Plans)*
- [04_PROCEDURES_AND_OPERATIONS/PRO-05_Control_of_Documented_Information_Procedure.md](#) — *Clause 7.5 (Document Taxonomy & Versioning)*
- [04_PROCEDURES_AND_OPERATIONS/PRO-06_Employee_Onboarding_and_Offboarding_Security.md](#) — *Controls 6.1-6.6 (BGV, NDAs, Immediate Offboard Revocation)*

05. Evaluation, Internal Audit & Continuous Improvement

- [05_EVALUATION_AND_AUDIT/PRO-07_Internal_Audit_Procedure.md](#) — *Clause 9.2 (Internal Audit Mandates & Independence)*
- [05_EVALUATION_AND_AUDIT/PRO-08_Management_Review_Procedure.md](#) — *Clause 9.3 (Board Review Process & Agendas)*
- [05_EVALUATION_AND_AUDIT/PRO-09_Corrective_Action_and_Improvement_Procedure.md](#) — *Clause 10.1 & 10.2 (5-Whys RCA, CAPA Workflow)*
- [05_EVALUATION_AND_AUDIT/CHK-01_ISO_27001_2022_Internal_Audit_Checklist.md](#) — *Complete Clauses 4-10 and Annex A Audit Checklist*

06. Operational Registers, Evidence Logs & Templates

- [06_REGISTERS_AND_TEMPLATES/REG-03_Information_Asset_Register.md](#) — *Control 5.9 (Hardware, Cloud & Data Asset Tracking)*
- [06_REGISTERS_AND_TEMPLATES/REG-04_Security_Incident_Log.md](#) — *Control 5.26 (Security Incidents & CERT-In Escalation Contact)*
- [06_REGISTERS_AND_TEMPLATES/REG-05_Corrective_Action_Register.md](#) — *Clause 10.1 (Corrective Action Requests - CAR Log)*
- [06_REGISTERS_AND_TEMPLATES/TEM-01_Management_Review_Meeting_Minutes.md](#) — *Clause 9.3 (Formal Board MRM Minutes)*

Statutory & Legal Framework Alignments

1. **Digital Personal Data Protection Act (DPDP Act), 2023:** Data classification, consent logging, cryptographic safeguards, and protection of Data Principals.
2. **CERT-In Cyber Security Directions (April 2022):** Mandatory 6-hour cybersecurity incident reporting, 180-day audit log retention, and NTP clock synchronization (`time.cert-in.org.in`).
3. **Information Technology Act, 2000 & IT (Amendment) Act, 2008:** Reasonable security practices under Section 43A and Section 72A.
4. **Reserve Bank of India (RBI) Cyber Security Guidelines:** Multi-factor authentication, API gateway controls, encryption of financial payloads, and third-party supplier governance.
5. **Companies Act, 2013:** Statutory record retention (8 years) and corporate governance accountability.

Certification Readiness Status

- **Management System Clauses (Clauses 4 to 10):** 100% Documented & Audited
- **Statement of Applicability (SoA):** All 93 controls evaluated and mapped
- **Internal Audit:** Completed with zero Major Nonconformities
- **Management Review Meeting (MRM):** Completed and signed off by Board of Directors
- **Recommendation: READY FOR STAGE 1 & STAGE 2 EXTERNAL CERTIFICATION AUDIT**

