

POL-02: ASSET MANAGEMENT POLICY

JOHN THOMAS FINTECH PRIVATE LIMITED

CIN: U62099KL2026PTC106017 | Doc ID: JT-ISMS-POL-002

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

ISO/IEC 27001:2022 Controls: 5.9 (Inventory of assets), 5.10 (Acceptable use of assets), 5.14 (Information transfer), 7.10 (Storage media), 7.14 (Secure disposal)

1. Purpose & Objectives

This policy establishes mandatory guidelines for the identification, inventorying, classification, ownership, usage, and secure disposal of all information assets owned, leased, or managed by JOHN THOMAS FINTECH PRIVATE LIMITED.

2. Scope

Applies to all physical hardware (laptops, monitors, networking gear), cloud virtual assets (AWS EC2 instances, S3 buckets, RDS databases), software licenses, intellectual property (source code repos, design documents), and corporate data.

3. Asset Inventory & Ownership (Control 5.9)

- Asset Register:** Every asset must be cataloged in the master Information Asset Register (REG-03) .
- Designated Asset Owners:** Every asset must have an assigned organizational owner responsible for:
 - Ensuring proper classification and access privileges.
 - Authorizing access modifications.
 - Verifying timely patch application and lifecycle reviews.
- Asset Tagging:** Physical hardware is tagged with a unique barcode/serial number upon procurement.

4. Handling & Movement of Assets

- Endpoint Protection:** All developer and employee laptops must be enrolled in Mobile Device Management (MDM) with mandatory full-disk encryption (FileVault / BitLocker).

2. **Removable Media:** Connecting personal USB flash drives or external HDDs is prohibited. USB ports are locked by default via MDM unless authorized for specific cryptographic token use.
3. **Off-Premises Use:** Company assets utilized outside the Kochi office must comply with remote working guidelines (P0L-07).

5. Decommissioning & Secure Disposal (Control 7.14)

1. Physical storage media destined for decommissioning must be sanitized according to NIST SP 800-88 Rev. 1 (Cryptographic Wipe or Physical Destruction).
2. Cloud virtual resources (EBS volumes, S3 buckets) must be securely deleted with multi-factor authentication deletion protection removed only by authorized DevOps leads.
3. Disposal certificates must be retained in the asset register for audit verification.

6. Approvals & Governance

Approved by Board of Directors. Review annually.