

PRO-04: CHANGE MANAGEMENT PROCEDURE

JOHN THOMAS FINTECH PRIVATE LIMITED

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

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

ISO/IEC 27001:2022 Controls: 8.32 (Change management), 8.31 (Separation of environments)

1. Objective

To ensure all modifications to production infrastructure, database schemas, fintech applications, and security configurations are implemented with formal authorization, rigorous testing, security evaluation, and backout planning to prevent unintended disruptions.

2. Change Categorization

Category	Description	Approval Level	Testing & Lead Time
Standard Change	Pre-approved, routine updates with low risk (e.g., weekly dependency patch, OS update in staging).	Peer Review / Tech Lead	Automated CI/CD pipeline pass
Normal Change	Significant architectural changes, new fintech feature rollouts, API version increments, schema migrations.	Change Advisory Board (CAB)	Staging regression test, security scan, 48h lead time
Emergency Change	Urgent production bugfix or security patch responding to an active P1 incident or zero-day exploit.	Emergency CAB (CISO + Tech Lead)	Expedited testing, post-implementation review within 24h

3. Change Advisory Board (CAB)

- Members: CISO, Lead Architect, DevOps Lead, QA Lead.
- Meets weekly or ad-hoc for normal changes.

4. Operational Change Workflow

1. **Request for Change (RFC):** Created via Jira ticket documenting scope, business justification, risk analysis, and **Rollback Plan**.
2. **Testing in Staging:** Change must pass end-to-end automated regression and SAST security checks in the staging environment.
3. **Approval:** CAB review and cryptographic sign-off on PR.
4. **Execution:** Automated deployment via CI/CD.
5. **Post-Implementation Verification:** Automated smoke tests verify system integrity. If anomalies occur, the rollback plan is triggered immediately.