

REG-04: INFORMATION SECURITY INCIDENT & CERT-IN REPORTING LOG

JOHN THOMAS FINTECH PRIVATE LIMITED

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

Version: 1.0 | Effective Date: 14-Oct-2026

ISO/IEC 27001:2022 Controls: 5.24, 5.25, 5.26, 5.27, 5.28

1. Incident Register Table

Incident ID	Date & Time Detected	Incident Description & Category	Priority Level	Affected Asset(s)	Containment Time	Resolution Time	CERT-In Notified?	Root Cause Summary	Corrective Action Ref	Status
INC-2026-001	02-Oct-2026 14:15 IST	Simulated Phishing Test Campaign: 1 user clicked credential harvesting link in training simulation.	P3 (Simulated)	Corporate Email	< 30 min	2 hours	N/A (Internal drill)	Lack of sender domain scrutiny during rapid email processing.	CAR-2026-01	CLOSED
INC-2026-002	08-Oct-2026 03:22 IST	AWS GuardDuty detected anomalous spike in failed SSH attempts against staging bastion host from foreign IP range.	P3 (Low)	Staging Bastion	< 15 min	1 hour	No (Blocked by WAF/Firewall)	Automated bot scanning public IP. Bastion SSH port exposed to 0.0.0.0/0.	CAR-2026-02	CLOSED

2. CERT-In Incident Escalation Contact Record

- Reporting Email:** incident@cert-in.org.in
- Help Desk Phone:** +91-1800-11-4949 / +91-11-24368544
- Reporting Portal:** <https://www.cert-in.org.in>
- Mandatory Reporting Window:** Within **6 hours** of noticeable cyber security incident.