

# PRO-02: INFORMATION SECURITY INCIDENT MANAGEMENT PROCEDURE

## JOHN THOMAS FINTECH PRIVATE LIMITED

**CIN:** U62099KL2026PTC106017 | **Doc ID:** JT-ISMS-PRO-002

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

**ISO/IEC 27001:2022 Controls:** 5.24 (Incident planning), 5.25 (Assessment of events), 5.26 (Response to incidents), 5.27 (Learning from incidents), 5.28 (Collection of evidence)

**Statutory Mandate:** CERT-In 6-Hour Cyber Incident Reporting Rule (April 2022)

### 1. Purpose & Incident Response Team (SIRT)

This procedure establishes a structured, end-to-end response framework for detecting, containing, investigating, eradicating, and reporting cybersecurity incidents.

#### Security Incident Response Team (SIRT):

- Incident Commander:** CISO / Security Lead
- Technical Leads:** Cloud DevOps Lead & Lead Software Architect
- Communications & Legal:** Managing Director / Legal Counsel

### 2. Incident Classification & Severity Matrix

| Priority             | Definition                                                                                                 | Examples                                                                                                     | Response SLA           | Reporting SLA                              |
|----------------------|------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------|------------------------|--------------------------------------------|
| <b>P1 - Critical</b> | Catastrophic security breach, customer financial data compromised, total system outage, active ransomware. | Production DB leak, unauthorized root access, ransomware encryption.                                         | Containment < 1 hour   | <b>CERT-In notice within 6 hours</b>       |
| <b>P2 - High</b>     | Major security event with partial impact or elevated risk of data compromise.                              | Active brute force on API gateway, unpatched critical RCE vulnerability, loss of encrypted corporate laptop. | Containment < 4 hours  | Regulatory notice if customer data at risk |
| <b>P3 - Medium</b>   | Minor security issue; no customer financial data compromised.                                              | Isolated malware on non-critical endpoint, suspicious phishing email reported.                               | Containment < 24 hours | Internal log within CAR register           |
| <b>P4 - Low</b>      | Security event with minimal risk.                                                                          | Port scan against external firewall blocked by WAF, single failed login attempt.                             | Monitored              | Internal report                            |

### 3. Incident Lifecycle Workflow

```

[1. Identification] ---> [2. Triage & Classify] ---> [3. Containment] ---> [4. Eradication & Recovery]
CloudWatch/SIEM alert      Assign P1-P4 Severity      Isolate affected VPC      Remove compromised assets
Internal staff report      Mobilize SIRT              Revoke credentials        Patch systems

```

#### Phase 1: Detection & Identification

- Security events are ingested via CloudWatch, GuardDuty, and internal employee reporting channels ( security@johnthomasfintech.com ).

#### Phase 2: Containment

- Short-Term Containment:** Isolate compromised virtual instances (quarantine security group), revoke compromised IAM tokens, block attacking IP ranges at AWS WAF.
- Evidence Preservation:** Take forensic memory snapshots and disk clones prior to terminating instances. Preserve cryptographic checksums of system logs.

#### Phase 3: Eradication & Recovery

- Eliminate threat root causes, rotate all system secrets and database passwords.
- Verify system integrity and restore services from verified immutable backups.

#### Phase 4: Statutory Reporting to CERT-In (Within 6 Hours)

For specified cyber incidents (data breach, ransomware, targeted attacks, compromise of critical systems):

- Submit formal incident notification to **CERT-In** (incident@cert-in.org.in) within **6 hours** of notice.
- Provide initial incident details using CERT-In's incident reporting format.

#### Phase 5: Post-Incident Review (PIR)

Within 5 business days, convene the SIRT to conduct a 5-Whys Root Cause Analysis, update the Incident Log ( REG-04 ), and issue a Corrective Action Request ( REG-05 ).