



# CYBER SECURITY POLICY

**Industrial Investment Trust Limited**

CIN: L65990MH1933PLC001998

Regd. Off: 101A, The Capital, G-Block,

Plot no.C-70 Bandra Kurla Complex,

Bandra (East) Mumbai Mumbai City

MH 400051

Website: [www.iitlgroup.com](http://www.iitlgroup.com)

| Version        | Date of Approval/ Reviewal         |
|----------------|------------------------------------|
| V.2            | 05-08-2026                         |
|                |                                    |
|                |                                    |
| Recommended By | CEO – NBFC                         |
| Approved By    | Board - Meeting Dated : 05-08-2026 |

## 1. Purpose & Policy Statement

IITL recognises cybersecurity as an enterprise risk. This Policy establishes the framework through which IITL shall prevent, detect, contain, respond to, recover from and learn from cyber threats and incidents. The framework is proportionate to IITL's size, business model, limited customer base and technology footprint.

This Policy operates alongside IITL's Information Security Policy, IT Policy, Cyber Crisis Management Plan/procedures, DPDP / Personal Data Protection Policy, BCP/DR arrangements and applicable outsourcing/vendor procedures.

## 2. Regulatory Basis & Applicability

This Policy is based principally on the Reserve Bank of India (Non-Banking Financial Companies – Cybersecurity, Technology: Risk, Resilience and Assurance Framework) Directions, 2026, particularly the requirements applicable to NBFCs in the Base Layer with asset size below Rs.500 crore, together with applicable CERT-In directions, the Information Technology Act and Rules, the Digital Personal Data Protection Act, 2023 and applicable Rules, and other applicable law/regulatory instructions.

The RBI Directions require a Board-approved cybersecurity policy and a Cyber Crisis Management Plan (CCMP), including vulnerability management, preparedness indicators, cyber-crisis lifecycle controls and cyber-incident reporting.

## 3. Objectives

- Protect IITL information assets, customer information, financial information and critical systems.
- Reduce likelihood and impact of cyber attacks and technology-enabled fraud.
- Establish clear ownership and accountability for cyber risk.
- Maintain preparation, detection, containment, response, recovery and lessons learned.
- Maintain tested resilience, backups, recovery arrangements and crisis communications.
- Ensure timely escalation and regulatory reporting.
- Measure cybersecurity preparedness through defined indicators and independent assurance.

## 4. Cybersecurity Governance

|                                        |                                                                                                                                                          |
|----------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Board</b>                           | <b>Approve/review Cyber Security Policy and CCMP; oversee material cyber risk, preparedness, incidents and remediation.</b>                              |
| Senior Management                      | Implement cybersecurity programme; ensure resources, drills, awareness, remediation and escalation.                                                      |
| CISO / designated cyber-security owner | Drive cybersecurity strategy, enforce controls, coordinate incident response, vulnerability management, testing, monitoring and regulatory coordination. |
| IT In-Charge / Head of IT              | Maintain secure technology operations, architecture, patching, backup, access and recovery capabilities; support cyber response.                         |
| Business/System Owners                 | Own business risk, approve access, classify criticality and support risk treatment.                                                                      |
| Employees                              | Follow security controls, maintain cyber hygiene and immediately report suspected incidents.                                                             |
| Vendors/Service Providers              | Comply with contractual security requirements, maintain resilience and promptly report incidents affecting IITL.                                         |

## 5. Cyber Risk Assessment

- Conduct comprehensive IT/cyber risk assessment at least annually and whenever there is a material change in systems, business model, outsourcing or threat environment.
- Identify critical assets, threats, vulnerabilities, existing controls, residual risks and required mitigation.
- Present results to Senior Management and the Board/appropriate Board-level forum and use them to inform testing, budgeting and remediation.

- Document, time-limit and appropriately approve risk acceptance.

The RBI Directions require annual comprehensive IT risk assessment and analysis of threats, vulnerabilities and existing controls, with the outcome brought to senior stakeholders and the Board.

## 6. Cyber Threat Landscape

- Ransomware / crypto-malware
- Destructive malware
- Phishing, spear-phishing and whaling
- Vishing and social engineering
- Business email compromise / payment fraud
- Credential/password attacks and identity fraud
- Unauthorised remote access
- DoS / DDoS
- Drive-by downloads and malicious websites
- Insider threats
- Data leakage/exfiltration
- Known and zero-day vulnerabilities
- Supply-chain and third-party compromise
- Cloud/account takeover and impersonation risks

## 7. Cybersecurity Baseline Controls

| Access             | Least privilege, need-to-know, role-based access and periodic review.                       |
|--------------------|---------------------------------------------------------------------------------------------|
| Authentication     | Strong authentication; MFA for privileged/critical access wherever technically supported.   |
| Endpoints          | Supported systems, endpoint protection and timely security updates.                         |
| Network            | Firewall, secure remote access, authorised devices and controlled connectivity.             |
| Data               | Classification, secure storage/transmission and protection of customer information.         |
| Logging            | Security-relevant logs and audit trails for critical systems.                               |
| Vulnerability      | Documented VA/PT and remediation programme.                                                 |
| Backup             | Protected backups with periodic restoration testing.                                        |
| Resilience         | BCP/DR aligned to critical-system RTO/RPO.                                                  |
| Awareness          | Ongoing training, testing and phishing/social-engineering preparedness.                     |
| Cryptography       | Strong, non-deprecated algorithms/protocols appropriate to risk.                            |
| Digital signatures | Use DSC/PKI where required for authentication, integrity, authenticity and non-repudiation. |

## 8. Vulnerability Management

- Maintain vulnerability identification, assessment, prioritisation, remediation, validation and closure.
- Critical information systems and DMZ systems with customer interface: VA at least every six months and PT at least annually, plus lifecycle testing as prescribed.
- Use appropriately trained and independent security professionals.
- Use risk-based frequency for non-critical systems.
- Post-implementation testing shall address production; unavoidable deviations shall be documented and approved.
- Risk-rate findings, remediate within defined timelines and escalate overdue high-risk issues.

## 9. Patch & Secure Configuration Management

- Assess business impact of patches/changes and deploy securely and promptly according to risk.
- Material changes shall be approved, tested, documented and capable of rollback.

- Critical systems shall be securely configured; unnecessary services/ports should be disabled where feasible.
- Failed or unexpected patch/change outcomes shall have a recovery mechanism.
- Known vulnerabilities shall not remain unaddressed without documented risk acceptance or compensating controls.

## **10. Access, Privileged Access & Remote Access**

- Grant access only for valid business need.
- Closely supervise privileged users; log and periodically review relevant activities.
- Implement MFA for privileged users of critical systems and critical activities based on risk and technical feasibility.
- Authorise, secure and limit remote access to legitimate business requirements.
- Identify and secure remote-access devices.
- Prohibit personal/unapproved remote-control software that bypasses approved controls.
- Control and monitor third-party remote access and remove it when no longer required.

## **11. Network, Endpoint & Removable Media Security**

- Only authorised and adequately protected devices may connect to IITL networks.
- Personal laptops, tablets and storage devices shall not connect unless expressly authorised and secured.
- Endpoint security shall protect against malware and suspicious activity.
- Removable media shall be restricted to legitimate business use, scanned where feasible and appropriately protected.
- Network security devices/configurations shall be administered only by authorised personnel.
- Internet-facing services shall be minimised and protected.

## **12. Email, Social Engineering & Business Email Compromise**

- Train users to identify phishing, spear-phishing, whaling and vishing.
- Do not open suspicious links/attachments or executable content without verification.
- Independently verify payment requests, beneficiary changes, credentials or sensitive-data requests.
- Use appropriate email authentication/security controls.
- Report suspected compromise immediately.
- Where IITL uses social media for business/marketing, address account takeover and impersonation risks.

## **13. Cryptographic Controls & Digital Signatures**

- Use strong, internationally accepted cryptographic algorithms, key lengths, cipher suites and protocols that are not deprecated or known insecure.
- Protect sensitive information in transit and, where warranted, at rest.
- Protect cryptographic keys and credentials.
- Use DSC/PKI for relevant electronic transactions and important documents to support confidentiality, integrity, authenticity and non-repudiation.

## **14. Application Security & Straight-Through Processing**

- Protect critical applications against unauthorised modification and insecure interfaces.
- Apply approved change-management procedures.
- Automate critical system-to-system transfers with authentication, checks, controls and audit trails where feasible.
- Avoid manual intervention/modification in critical data transfers except through controlled, authorised and auditable exception procedures.

## 15. Logging, Monitoring & Audit Trails

- Maintain audit trails for critical systems sufficient for security investigation, audit and dispute resolution.
- Protect logs from unauthorised alteration/deletion.
- Monitor security logs at a frequency appropriate to risk.
- Retain relevant security/application/authentication/administrative events for applicable legal, regulatory and operational periods.
- Escalate material anomalies.

The RBI Directions require audit logging for systems affecting critical/sensitive information, sufficiently detailed trails and regular monitoring for unauthorized activity.

## 16. Cyber Incident Classification

|                         |                                                                                                                                  |                                                                                                        |
|-------------------------|----------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------|
| Low                     | <b>Blocked phishing attempt; isolated non-critical malware with no material impact</b>                                           | <b>IT/security owner; record and close with evidence</b>                                               |
| Moderate                | Compromised endpoint/account, limited exposure or local disruption                                                               | IT/security + management; investigate/remediate                                                        |
| High                    | Material data exposure, ransomware affecting critical system, prolonged disruption, major fraud or third-party compromise        | Immediate Senior Management escalation; crisis response; assess reporting                              |
| Critical / Cyber Crisis | Widespread ransomware, critical-system outage, significant customer/regulatory impact, major data compromise or sustained attack | Activate CCMP; crisis leadership; Board notification; regulatory/customer communications as applicable |

Classification shall consider confidentiality, integrity, availability, financial impact, customer impact, regulatory impact, duration, spread and reputational consequences.

## 17. Cyber Incident Response Lifecycle

Preparation – maintain contacts, tools, backups, response procedures, vendor contacts and training.

Detection – identify alerts, user reports, anomalies and indicators of compromise.

Analysis – validate, classify, determine scope, impact, affected assets and likely root cause.

Containment – isolate affected devices/accounts/networks and prevent spread.

Eradication – remove malicious components, close vulnerabilities and reset compromised credentials.

Recovery – restore safely from trusted sources, validate systems/data and resume operations.

Lessons learned – review root cause, control gaps, corrective actions and prevention measures.

The RBI framework requires the CCMP to address Detection, Response, Recovery and Containment and requires severity/impact/root-cause analysis with corrective and preventive action.

## 18. Immediate User Actions on Suspected Incident

- Immediately notify the designated IT/CISO/security contact.
- Do not delete suspicious files, logs or messages.
- Do not intentionally alter evidence or reinstall/format an affected device unless instructed.
- If safe and directed, disconnect the affected device/network connection to prevent spread.
- Preserve relevant emails, screenshots and other evidence.
- Do not communicate externally without authorisation.

## 19. Cyber Crisis Management Plan (CCMP)

- Maintain a controlled operational CCMP under this Policy.
- Incident-response team and role matrix.

- Primary/alternate contact details for management, IT/security, Legal/Compliance, communications, vendors and authorities.
- Severity/classification and escalation matrix.
- Ransomware, phishing/BEC, DDoS, data-leakage and critical-system outage playbooks.
- Evidence preservation and forensic arrangements.
- Regulatory/statutory reporting procedures.
- Customer/stakeholder communication protocol.
- Business continuity and recovery linkages.
- Post-incident review and corrective-action tracking.

## **20. Regulatory Reporting**

Cyber incidents falling within applicable RBI reporting requirements shall be reported to RBI on the DAKSH platform within six hours of detection. IITL shall also proactively notify CERT-In where required. Internal approvals shall not delay a mandatory notification.

The six-hour RBI reporting requirement is expressly stated in the RBI Directions.

The incident record shall capture detection time, reporting time, authority, reference/acknowledgement, impact, actions and closure. Personal-data breaches shall also be assessed under IITL's DPDP / Personal Data Protection Policy.

## **21. Ransomware & Malware Response**

- Isolate affected systems/accounts promptly.
- Protect and preserve backups from compromise.
- Identify initial access vector and affected scope.
- Engage specialist/forensic assistance where required.
- Do not restore compromised systems until the environment/source is assessed.
- Reset/rotate compromised credentials and close exploited vulnerabilities.
- Validate restored systems before production use.
- Complete root-cause analysis and lessons learned.

## **22. Business Continuity, DR & Cyber Resilience**

- Define RTO/RPO for critical systems appropriate to business/regulatory requirements.
- Periodically restore/test backups and protect them from unauthorised access.
- Conduct DR drills at least half-yearly for critical information systems where applicable.
- DR tests shall demonstrate actual switching/operation sufficiently to validate business continuity.
- Restore cybersecurity controls along with critical operations.
- Remediate and retest material drill gaps.

The RBI Directions prescribe half-yearly DR drills for critical information systems and require RTO/RPO, backup restoration, matching DC/DR configurations and resilience testing with vendors/partners.

## **23. Third-Party & Supply-Chain Cyber Risk**

- Assess cyber risk before onboarding material IT/security vendors.
- Contracts shall address security, confidentiality, incident notification, audit/access, continuity and exit as appropriate.
- Control, monitor and periodically review third-party remote access.
- Consider concentration, single-point-of-failure and supply-chain risks.
- Escalate vendor cyber incidents affecting IITL.

- IITL remains accountable for its regulatory obligations notwithstanding outsourcing.

The RBI framework requires proportionate vendor-risk controls addressing concentration, conflicts, single points of failure, customer-data protection, availability and supply-chain risks.

## 24. Cybersecurity Awareness & Training

- Provide ongoing cybersecurity awareness training to all users.
- Cover phishing, social engineering, passwords, safe browsing, data handling, removable media, remote access and incident reporting.
- Provide Board/Senior Management familiarisation appropriate to oversight role.
- Assess training effectiveness through testing/simulations or other suitable measures.
- Maintain current training records.

The RBI framework requires ongoing training, periodic updating, effectiveness measurement and a current repository of training status.

## 25. Cybersecurity Preparedness Indicators & Metrics

| Incident readiness | Response, escalation and closure time                     |
|--------------------|-----------------------------------------------------------|
| RBI reporting      | Incidents reported within applicable six-hour requirement |
| Vulnerability      | Critical/high findings open and ageing                    |
| VA/PT              | Completion against schedule; remediation status           |
| Access             | Privileged-access review and MFA coverage                 |
| Backup             | Backup success and restoration-test success               |
| Resilience         | RTO/RPO achieved in drills                                |
| Awareness          | Training completion and phishing-test performance         |
| Vendor             | Material vendor reviews/incidents                         |
| Audit              | Open high-risk findings and ageing                        |

The RBI Directions require cybersecurity preparedness indicators and metrics for system performance, recovery and business resumption.

## 26. Information Systems Audit & Independent Assurance

- Cybersecurity controls shall form part of the IS Audit/internal assurance framework.
- IS Audit shall assess policy effectiveness, IT/security controls, BCP/DR and applicable legal/regulatory compliance.
- Use suitably skilled personnel; external specialists may be used where internal expertise is insufficient.
- Audit findings shall be independently evaluated and reported to the appropriate Board-level forum.
- Material deficiencies shall have accountable owners and closure timelines.

The RBI Directions require IS Audit to cover IT infrastructure, information security, BCP/DR and legal/regulatory compliance, with suitably skilled independent auditors and at least annual periodicity in the applicable framework.

## 27. Data Protection & DPDP Interface

- Protect customer/employee personal data against unauthorised access, disclosure, alteration, loss and destruction.
- Assess personal-data incidents under the DPDP / Personal Data Protection Policy.
- Coordinate safeguards, retention, deletion, vendor processing and breach escalation across cybersecurity and privacy frameworks.
- Nothing in this Policy limits a legal/statutory breach-notification requirement.

## **28. Physical & Personnel Security**

- Privileged personnel shall be subject to appropriate background screening to the extent permitted by law and proportionate to role risk.
- Critical IT areas/equipment shall have restricted access.
- Leavers' access and credentials shall be disabled promptly.
- Security responsibilities shall be included in relevant employment/vendor terms.

## **29. Exceptions & Risk Acceptance**

Any exception shall identify the control requirement, business reason, affected system/data, risk, compensating control, approving authority, validity period and review date. Exceptions to mandatory regulatory requirements shall not be treated as ordinary policy exceptions; any legally permissible remediation approach shall be documented and escalated appropriately.

## **30. Non-Compliance & Disciplinary Action**

Violation of this Policy may result in disciplinary action in accordance with IITL's employment/service rules, contractual terms and law. Depending on severity, IITL may restrict access, suspend privileges, investigate, recover losses where legally permissible, terminate contractual access and/or refer matters to law-enforcement or regulatory authorities.

## **31. Board & Management Reporting**

- Material cyber incidents and impact/recovery status.
- Regulatory incidents and reporting status.
- Critical/high vulnerabilities and overdue remediation.
- VA/PT status and material findings.
- Backup/DR test outcomes and RTO/RPO performance.
- Security-awareness status.
- Material third-party cyber risks/incidents.
- Outstanding audit findings and corrective action.

## **32. Records & Evidence**

- Cyber risk assessments
- Asset/critical-system inventory
- VA/PT reports and remediation evidence
- Access/MFA reviews
- Incident and regulatory-reporting register
- Logs and relevant forensic evidence
- Backup/restore and DR drill evidence
- Training/awareness records
- Vendor cyber due diligence and incident records
- Policy exceptions and risk acceptances
- Board/management cyber-risk reports

## **33. Review & Amendment**

This Policy shall be reviewed at least annually and after a material cyber incident, significant technology/business change, material outsourcing change or regulatory amendment. The Board shall approve material changes.

## Appendix A – Cyber Incident Register – Minimum Fields

| Field             | Minimum Record                                  |
|-------------------|-------------------------------------------------|
| Incident ID       | Unique reference                                |
| Detection         | Date/time and source                            |
| Classification    | Low / Moderate / High / Critical                |
| Affected assets   | Systems, applications, accounts, data           |
| Impact            | Operational, financial, customer, regulatory    |
| Actions           | Containment, eradication, recovery              |
| Reporting         | RBI/CERT-In/other authority, time and reference |
| Root cause        | Technical/process/third-party cause             |
| Corrective action | Owner, due date and closure evidence            |
| Lessons learned   | Control improvements                            |

## Appendix B – Cyber Crisis Contact Matrix

| Role                            | Primary Contact | Alternate Contact |
|---------------------------------|-----------------|-------------------|
| CEO / Senior Management         |                 |                   |
| CISO / Security Owner           |                 |                   |
| IT In-Charge                    |                 |                   |
| Legal / Compliance              |                 |                   |
| Internal Audit                  |                 |                   |
| Critical IT Vendor              |                 |                   |
| Cyber Forensics / IR Specialist |                 |                   |
| RBI reporting contact           |                 |                   |
| CERT-In coordination            |                 |                   |

## Appendix C – Quick Cyber Response Checklist

- Recognize and report immediately.
- Do not destroy evidence.
- Contain affected systems/accounts safely.
- Activate incident-response/CCMP escalation according to severity.
- Assess customer, financial, operational and regulatory impact.
- Preserve logs/evidence and engage specialists if needed.
- Assess RBI/CERT-In/DPDP and other reporting obligations.
- Recover from trusted systems/backups.
- Validate security before resuming normal operations.
- Complete root-cause analysis, remediation and lessons learned.