



## INFORMATION 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 and Policy Statement

This Policy establishes the information-security framework of IITL. It consolidates the useful control principles contained in the Company's existing Information Security Policy with the governance, technology and security controls contained in IITL's fresh IT Policy and IT Security & Information Security Policy. The framework is proportionate to IITL's status as a non-deposit taking NBFC-BL.

The objective is to protect confidentiality, integrity, availability and authenticity of information and to prevent unauthorised access, alteration, disclosure, destruction, loss or misuse.

## 2. Regulatory Framework

The Policy shall be read with applicable RBI directions, including the RBI framework on Cybersecurity, Technology: Risk, Resilience and Assurance applicable to NBFCs, applicable CERT-In directions, the Information Technology Act and Rules, the Digital Personal Data Protection Act, 2023 and the Digital Personal Data Protection Rules, 2025, as amended or replaced from time to time.

The notified DPDP Rules contain phased commencement provisions; IITL shall comply with each provision from its applicable commencement date and maintain implementation readiness.

Where law or regulatory direction is more stringent than this Policy, the law/regulatory direction shall prevail.

## 3. Scope

- All information created, received, processed, stored, transmitted or disposed of by IITL.
- All servers, desktops, laptops, applications, databases, networks, cloud services, email, removable media and backups.
- All employees, directors, consultants and third parties accessing IITL systems or information.
- Electronic and physical information where compromise may affect IITL, customers, employees, counterparties or regulatory compliance.

## 4. Information Security Principles

| Principle        | Requirement                                                                |
|------------------|----------------------------------------------------------------------------|
| Confidentiality  | Access only by authorised persons for legitimate business purposes.        |
| Integrity        | Protect information from unauthorised or accidental modification/deletion. |
| Availability     | Keep critical information and systems available to authorised users.       |
| Authenticity     | Maintain reasonable ability to verify users, communications and records.   |
| Least privilege  | Provide only minimum required access.                                      |
| Need to know     | Restrict sensitive information to persons requiring it.                    |
| Defence in depth | Use multiple complementary controls.                                       |
| Proportionality  | Controls shall reflect IITL's size, systems, data and risk profile.        |

## 5. Information Classification and Handling

| Class        | Examples                                                                                          | Minimum Controls                                                                  |
|--------------|---------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------|
| Restricted   | KYC, customer financial data, credentials, cryptographic keys, sensitive regulatory/security data | Need-to-know; strong access; secure transmission/storage; no unauthorised copying |
| Confidential | Internal financials, contracts, employee records, management reports                              | Authorised access; controlled sharing                                             |
| Internal     | Routine internal policies/procedures                                                              | Internal use; controlled external disclosure                                      |
| Public       | Approved public disclosures                                                                       | External release only after approval                                              |

- Users shall not downgrade classification for convenience.
- Restricted/Confidential data shall not be sent to personal email, unauthorised cloud storage or messaging platforms.
- Sensitive printed material shall be protected from unauthorised viewing and securely disposed of.

## 6. Governance and Responsibilities

| Role                                | Responsibilities                                                                                                                                                |
|-------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Board                               | Approve Policy; oversee material information-security risks/incidents and significant remediation.                                                              |
| Senior Management                   | Implement controls and allocate resources.                                                                                                                      |
| IT / Information Security In-Charge | Access administration, security configuration, patching, backups, monitoring, vulnerability coordination, incident coordination and vendor technical oversight. |
| System / Business Owner             | Approve access; classify information; confirm business need.                                                                                                    |
| Users                               | Protect credentials/data; follow controls; report incidents immediately.                                                                                        |
| Vendors                             | Comply with contractual security requirements and promptly report incidents.                                                                                    |
| Assurance                           | Conduct risk-based review/testing and track findings.                                                                                                           |

## 7. Asset and Information Inventory

- Maintain an inventory of critical hardware, software, applications, databases, network devices, cloud services and major information repositories.
- Record owner, purpose, criticality, location/hosting and key vendor dependencies.
- Review periodically and on material system changes.
- Unauthorised/obsolete assets shall be removed, disabled or subject to documented compensating controls.

## 8. User Access Management

- Access shall be authorised by the relevant system/business owner.
- Use least privilege and need-to-know.
- Use unique IDs wherever technically possible; shared accounts are prohibited except where technically unavoidable and controlled.
- Review user and privileged access periodically.

- Promptly modify/disable access on role change, exit or cessation of need.
- Maintain access records as confidential information.

## 9. Passwords, Authentication and Privileged Access

- Passwords shall be strong, confidential and not shared.
- Default credentials shall be changed.
- MFA shall be used for privileged, remote and critical access wherever technically supported.
- Provide controlled password-reset and locked-account procedures.
- Administrative privileges shall be restricted to authorised personnel.
- Privileged activities shall be logged where feasible and privileged access reviewed periodically.

## 10. Segregation of Duties / Maker-Checker

- Material financial, customer-master, payment, accounting and security-sensitive activities shall use maker-checker controls where system functionality permits.
- IT administration shall be separated from business approval wherever practicable.
- No person should ordinarily initiate and independently approve the same material transaction.

## 11. Physical Security

- Protect IT equipment against theft, unauthorised use, fire, water, power disruption and foreseeable hazards.
- Restrict access to server/network areas where maintained by IITL.
- Secure portable devices when unattended or transported.
- Position sensitive screens/printers to reduce unauthorised viewing.
- Authorisation is required before removing Company equipment from premises.
- Report lost/stolen equipment immediately.

## 12. Endpoint and Removable-Media Security

- Use authorised, supported operating systems and applications.
- Maintain endpoint anti-malware/security protection and timely security updates.
- Users shall not install unauthorised software.
- Enable automatic screen locking.
- USB/external media shall be used only for legitimate business purposes and scanned where technically feasible.
- Restricted data shall not be copied to removable media without authorisation and appropriate protection.

## 13. Email, Internet and Phishing

- Do not open suspicious attachments/links or execute unknown files.
- Use approved business channels for sensitive information.

- Independently verify unusual payment instructions or bank-detail changes.
- Do not bypass internet/security controls.
- Pirated, unlicensed or unauthorised software is prohibited.
- Report phishing, malware or credential compromise immediately.

#### **14. Network Security**

- Maintain an appropriate network/device inventory and basic network documentation.
- Restrict network access to authorised users/devices.
- Maintain appropriately configured firewall/network security controls.
- Remote access shall be authenticated, authorised and secured.
- Only authorised personnel/vendors may administer network equipment.
- Material configuration changes shall be documented and approved.
- Where justified by business continuity needs, alternate connectivity should be available for critical operations.

#### **15. Application, Database and Operating-System Security**

- Operational, lending, accounting and other critical applications shall use role-based access.
- Direct database access shall be restricted to authorised administrators.
- Material changes shall follow change-management controls.
- Data shall not be copied into testing environments unless necessary and adequately protected.
- Operating systems shall be patched and securely configured; unnecessary services/tools should be disabled.
- Unsupported versions shall be replaced or subject to documented compensating controls.

#### **16. Logging, Monitoring and Audit Trails**

- Critical systems shall maintain security-relevant logs sufficient to investigate material events where technically feasible.
- Protect logs against unauthorised alteration/deletion.
- Review security alerts and suspicious access according to risk.
- Maintain audit trails capable of supporting investigation of material transactions and incidents.
- Escalate material anomalies.

#### **17. Vulnerability, Patch and Security Testing**

- Identify and prioritise vulnerabilities.
- Prioritise critical and internet-facing vulnerabilities.
- Conduct periodic security testing proportionate to IITL's technology footprint and applicable regulatory requirements.
- Assign owners and target dates to material findings.
- Document compensating controls and residual-risk acceptance where immediate remediation is not possible.

## **18. Backup and Recovery**

- Back up critical business and regulatory data at defined intervals.
- Protect backups from unauthorised access, alteration and deletion.
- Where feasible, maintain segregation between backup and primary environments to reduce ransomware impact.
- Perform periodic restoration tests and retain evidence.
- Monitor backup failures and correct them promptly.
- Apply applicable legal/regulatory retention requirements.

## **19. Business Continuity and Disaster Recovery**

- Maintain practical BCP/DR arrangements proportionate to IITL's size and critical operations.
- Identify critical processes, systems, dependencies and recovery priorities.
- Maintain practical alternate arrangements for prolonged system/network failure.
- Test BCP/DR at least annually and after material changes.
- Track material test findings to closure.

## **20. Information-Security Incident Management**

1. Record the alert/incident.
2. Validate and classify severity.
3. Identify affected systems, information and users.
4. Contain the incident.
5. Preserve relevant evidence and logs.
6. Investigate scope and root cause.
7. Eradicate the threat and remediate weaknesses.
8. Restore systems/data safely.
9. Validate recovery and monitor for recurrence.
10. Document lessons learned and corrective actions.

## **21. Cyber and Regulatory Escalation**

Cyber incidents shall additionally be handled under IITL's Cyber Security & Cyber Crisis Management Policy. RBI, CERT-In and other regulatory/statutory reporting shall be completed within the applicable prescribed timelines. Internal approval processes shall not delay a mandatory regulatory notification.

Personal-data incidents shall also be assessed under IITL's DPDP / Personal Data Protection Policy and applicable DPDP requirements. The notified Rules prescribe security safeguards and breach-management obligations, subject to their applicable commencement dates.

## **22. Data Protection and Privacy**

- Process personal data only for legitimate authorised purposes.
- Restrict access based on business need.
- Maintain appropriate retention and secure deletion controls.

- Use appropriate safeguards when personal data is shared with processors/vendors.
- Escalate suspected personal-data leakage under both this Policy and the DPDP/Cyber policies, as applicable.

## 23. Vendor, Outsourcing and Cloud Security

- Risk-assess material IT vendors before onboarding.
- Contracts should cover confidentiality, security, incident notification, continuity, data handling, return/deletion and audit/assurance as appropriate.
- Limit vendor access to necessary systems/data and remove access when no longer required.
- Cloud services shall consider access control, availability, data security, hosting/location, backup, exit and portability.
- Outsourcing does not transfer IITL's regulatory accountability.

## 24. Structured Digital Database / Confidential Regulatory Information

The existing policy specifically addresses a structured digital database of designated personnel and states that the information is confidential, encrypted and backed up. The new framework retains these control objectives without tying the requirement to a particular application or a single individual.

- Such databases shall be classified Restricted.
- Access shall be role-based and limited to authorised personnel.
- Material access/change activity should be logged where feasible.
- Data shall be appropriately protected in storage and transmission.
- Backups shall have equivalent confidentiality and access controls.

## 25. Security Awareness and Training

- Provide periodic awareness covering phishing, social engineering, passwords, data handling, removable media, remote access and incident reporting.
- Provide role-specific guidance to personnel handling customer/KYC/financial data.
- Maintain training/completion records.

## 26. Remote Work and Mobile Access

- Use approved secure remote-access mechanisms.
- Do not use insecure/public systems for Restricted information unless specifically secured and authorised.
- Maintain endpoint protection and screen lock.
- Report lost/stolen devices immediately.
- Withdraw remote access when no longer required.

## 27. Physical Records and Secure Disposal

- Store sensitive records in controlled locations.

- Do not leave Confidential/Restricted documents unattended in common areas.
- Use secure shredding or equivalent disposal.
- Securely erase data before IT equipment is reused or disposed of.

## 28. Exceptions, Compliance and Assurance

Exceptions shall be documented with business reason, affected asset/data, risk assessment, compensating controls, approving authority and expiry/review date. Material exceptions shall be escalated. IITL may conduct internal or independent reviews of access, backup, vulnerabilities, incidents, vendors and other controls. Material observations shall have remediation plans.

## 29. Management Information and Board Reporting

| Area             | Illustrative Reporting                                  |
|------------------|---------------------------------------------------------|
| Incidents        | Material incidents, impact, recovery, corrective action |
| Vulnerabilities  | Critical/high findings and ageing                       |
| Access           | Privileged-access exceptions and review status          |
| Backup/BCP       | Backup failures, restoration and BCP tests              |
| Security testing | Material findings and remediation                       |
| Vendors          | Material incidents or unresolved vendor risks           |
| Awareness        | Training completion and material security trends        |

## 30. Records to be Maintained

IT/information asset inventory; user and privileged-access records; access reviews; incident register; vulnerability/patch register; backup and restoration records; BCP/DR tests; security testing/assurance reports; vendor security records; training records; policy exceptions and risk acceptances. The system documentation and user documentation to be updated as and when there are changes or at least once a week.

## 32. Relationship with Other IITL Policies

This Policy shall be read together with IITL's IT Policy, Cyber Security & Cyber Crisis Management Policy, BCP/DR arrangements, Outsourcing Policy and Change Management Policy, applicable KYC/AML and records-retention policies.

## 33. Review and Approval

The Policy shall be reviewed at least annually and earlier where there is a material change in law, RBI requirements, technology, business model, outsourcing arrangements or cyber threat profile.

## Appendix A – Annual Information Security Checklist

| Control         | Annual Confirmation              |
|-----------------|----------------------------------|
| Policy          | Board review/approval completed  |
| Asset inventory | Updated                          |
| Access          | User/privileged review completed |

|                  |                                           |
|------------------|-------------------------------------------|
| Endpoint/network | Security and patching reviewed            |
| Vulnerabilities  | Material findings tracked                 |
| Backup           | Restore testing completed                 |
| BCP/DR           | Annual test completed                     |
| Incidents        | Register reviewed                         |
| Vendors          | Critical vendors reviewed                 |
| Training         | Awareness completed                       |
| Privacy          | Personal-data security/retention reviewed |
| Assurance        | Risk-based review completed               |

## Appendix B – Immediate User Reporting Triggers

- Phishing/suspicious email or link.
- Lost/stolen laptop, mobile or removable media.
- Suspected credential compromise.
- Unauthorised access or unusual login.
- Unusual payment/bank-detail change request.
- Malware/ransomware warning.
- Accidental disclosure/misdirected email containing customer/employee information.
- Unauthorised software installation.
- Suspicious alteration/deletion of records.
- Any suspected personal-data breach.

***\*\*\*Separate Password Policy, Internet Use Policy, User Access Management Policy stands withdrawn with the implementation of this new policy.***