POLICY ON INFORMATION TECHNOLOGY

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

Version	Date of Approval/ Reviewal
V.2	
Recommended By	CEO – NBFC Operations
Approved By	Board - Meeting Dated : 08-11-2023

Owner : IT Manager
Department – Information Technology Department

(1) BACKGROUND

The Reserve Bank of lndia ('RBI') vide its Circular RBI/DNBS/2016 -17/53 and Master Direction DNBS.PPD.No.04/66.15.001/2016-17 dated 08th June, 2017 for Non-Banking Financial Companies - IT/IS/BCP Policy, 2017 dated 08th June, 2017 requires NBFCs to adopt policy with the approval of Board. These Guidelines aim to enhance safety, security, efficiency in processes leading to benefits for NBFCs and their customers. NBFCs, pursuant to these Guidelines, are required to conduct a formal gap analysis between their present status and stipulations as set out in the Guidelines and put in place a time-bound action plan to address the gap.

IT governance is an integral part of corporate governance of **INDUSTRIAL INVESTMENT TRUST LIMITED (IITL)**, and effective IT governance is the responsibility of the board of directors of IITL ("Board") and its executive management.

IITL's board ensures implementation of this IT Framework which, inter alia, includes (i) Security aspects; (ii) User Role; (iii) Information Security and Cyber Security; (iv) Business Continuity Planning Policy; (v) Back-up Data. For the purpose of effective implementation of this IT Framework, the Board shall ensure technical competence at senior/middle level management of IITL. The Board is also responsible for periodic assessment of the IT training requirements to ensure the availability of sufficient, competent and capable human resources in IITL.

(2) APPLICABILITY

As per the circular and master direction NBFC with asset size below Rs. 500 Crore shall adopt IT Policy as per **SECTION B** given in Master direction.

(3) PURPOSE

The objective and purpose of this policy is:

- Developing IT System for maintaining the database.
- To frame IT standards and measures for company in order to comply with above said RBI Master Direction.
- To ensure that each person to be appointed or already appointed understands, the IT policy and their obligation to meet its requirement.
-

(4) REQUIREMENTS OF THIS POLICY

A) Recommended to the Board for approval, basic security aspects such as physical/logical access controls and well defined password policy.

B) Identify and secure a well-defined user role.

C) A maker checker concept to reduce the risk of error and misuse and to ensure reliability of data/information.

D) Information Security and Cyber Security;

E) Requirements as regards Mobile Financial Services, Social Media and Digital Signature Certificates;

F) System generated reports for Top Management summarizing financial position including operating and non-operating revenues and expenses, segments/verticals, cost of funds, etc.;

G) Adequacy to file regulatory returns to RBI;

H) Arrangement for backup of data with periodic testing;

I) Systems should be progressively scaled up as the size and complexity of NBFC's operations increases.

(5) COMPLIANCE

1. All employees are expected to comply with the IT Policy rules and guidelines while purchasing, using and maintaining any equipment or software purchased or provided by the organization.
2. Any employee who notices misuse or improper use of equipment or software within the organization must inform his/her Reporting Manager(s) immediately.
3. Inappropriate use of equipment and software by an employee will be subject to disciplinary action as deemed fit by the Management Committee of the organization.

(6) Employee Training

1. Basic IT training and guidance is provided to all new employees about using and maintaining their Personal Computer (PC), peripheral devices and equipment in the organization, accessing the organization network and using application software.

2. Employees can request and/or the Management Committee can decide to conduct an IT training on a regular or requirement basis.

(7) SECURITY AND USAGE ASPECTS

General Guidelines

1. ***Internet is a paid resource and therefore shall be used only for office work.***
2. ***The organization reserves the right to monitor, examine, block or delete any/all incoming or outgoing internet connections on the organization's network.***
3. ***The organization has systems in place to monitor and record all Internet usage on the organization's network including each website visit, and each email sent or received. The Management Committee can choose to analyze Internet usage and publicize the data at any time to assure Internet usage is as per the IT Policy.***
4. ***The organization has installed an Internet Firewall to assure safety and security of the organizational network. Any employee who attempts to disable, defeat or circumvent the Firewall will be subject to strict disciplinary action***

A. Password Policy

All users are responsible for keeping their passwords secure and confidential. The password credentials of the users must comply with the password parameters ("Complexity Requirements") and standards laid down in this IT Framework. Passwords must not be shared with or made available to anyone in any manner that is not consistent with this IT Framework.

The Complexity Requirements for setting passwords are as follows:

- A strong password must be at least 8 (Eight) characters long.
- It should not contain any of the user's personal information—specifically his/her real name, user name, or even company name.
- It must be very unique from the passwords used previously by the users.
- It should not contain any word spelled completely.
- It should contain characters from the four primary categories i.e. uppercase letters, lowercase letters, numbers, and characters.
- To ensure that a compromised password is not misused on a long-term basis, users are encouraged to change the password every 30 (Thirty) days.
- Passwords must not be stored in readable form in computers without access control systems or in other locations where unauthorized persons might discover them. Passwords must not be written down and left in a place where unauthorized persons might discover them.
- Immediately upon assignment of the initial password and in case of password "reset" situations, the password must be immediately changed by the user to ensure confidentiality of all information.
- Under no circumstances, the users shall use another user's account or password without proper authorization.

- Under no circumstances, should the user share his/her password(s) with other user(s), unless the said user has obtained from the concerned branch manager head the necessary approval on mail in this regard. In cases where the password(s) is shared in accordance with the above, the user shall be responsible for changing the said password(s) immediately upon the completion of the task for which the password was shared.

B. ACCESS CONTROLS

- Access to the IITL's electronic information and information systems, and the facilities where they are housed, is a privilege that may be monitored and revoked without notification. Additionally, all access is governed by law and IITL's policies including but not limited to requirements laid down in this policy.

- Persons or entities with access to the IITL's electronic information and information systems are accountable for all activities associated with their user credentials. They are responsible to protect the confidentiality, integrity, and availability of information collected, processed, transmitted, stored, or transmitted by IITL, irrespective of the medium on which the information resides.

- Access must be granted on the basis of least privilege - only to resources required by the current role and responsibilities of the person.

- Requirements:

  a. All users must use a unique ID to access IITL's systems and applications.

  b. Alternative authentication mechanisms that do not rely on a unique ID and password must be formally approved.

  c. Remote access to IITL's systems and applications must use a two-factor authentication where possible.

  d. System and application sessions must automatically lock after 10 (Ten) minutes of inactivity.

(8) INFORMATION SECURITY AND CYBER SECURITY

(I) INFORMATION SECURITY

IITL has an information security framework with the following principles:

- *Identification and classification of information assets:* IITL maintains detailed inventory of information asset with distinct and clear identification of the asset.

- *Functions:* The information security function is adequately resourced in terms of the number of staff, level of skill and tools or techniques like risk assessment, security architecture, vulnerability assessment, forensic assessment, etc. Further,

there is a clear segregation of responsibilities relating to system administration, database administration and transaction processing.

- *Role based access control* – Access to information is based on well-defined user roles (system administrator, user manager, application owner. IITL has a clear delegation of authority to upgrade/change user profiles and permissions and also key business parameters.

- *Personnel Security* - A few authorized application owners/users may have intimate knowledge of financial institution processes and they pose potential threat to systems and data. IITL has a process of appropriate checks and balances to avoid any such threat to its systems and data. Personnel with privileged access like system administrator, cyber security personnel, etc are subject to rigorous background check and screening.

- *Physical Security* - The confidentiality, integrity, and availability of information can be impaired through physical access and damage or destruction to physical components. IITL has created a secured environment for physical security of information assets such as secure location of critical data, restricted access to sensitive areas like data centres etc. and has further obtained adequate insurance to safeguard such data.

- *Maker-checker* – Maker checker is one of the important principles of authorization in the information systems of financial entities. It means that for each transaction, there are at least two individuals necessary for its completion as this will reduce the risk of error and will ensure reliability of information. IITL ensures that it complies with this requirement to carry out all its business operations.

- *Trails* - IITL ensures that audit trails exist for IT assets satisfying its business requirements including regulatory and legal requirements, facilitating audit, serving as forensic evidence when required and assisting in dispute resolution. If an employee, for instance, attempts to access an unauthorized section, this improper activity is recorded in the audit trail.

- *Social Media Risks* – IITL uses social media to market their products and is well equipped in handling social media risks and threats in order to avoid any account takeover or malware distribution. IITL further ensures proper controls such as encryption and secure connections to mitigate such risks.

- *Digital Signatures* - A Digital signature certificate authenticates entity's identity electronically. IITL protects the authenticity and integrity of important electronic documents and also for high value fund transfer.

- *Regulatory Returns* – IITL has adequate system and formats to file regulatory returns to the RBI on a periodic basis. Filing of regulatory returns is managed and verified by the authorized representatives of IITL.

(II) CYBER SECURITY

- IITL takes effective measures to prevent cyber-attacks and to promptly detect any cyber intrusions to respond / recover / contain the fall out. Among other things, IITL takes necessary preventive and corrective measures in addressing various types of cyber threats which includes denial of service, distributed denial of services (DDoS), ransom-ware / crypto ware, destructive malware, business email frauds including spam, email phishing, spear phishing, whaling, vishing frauds, drive-by downloads, browser gateway fraud, ghost administrator exploits, identity frauds, memory update frauds and password related frauds.

- IITL realizes that managing cyber risk requires the commitment of the entire organization to create a cyber-safe environment. This requires a high level of awareness among staff at all levels. IITL ensures that the top management and the Board have a fair degree of awareness of the fine nuances of the threats. Further, it also proactively promotes, among their customers, vendors, service providers and other relevant stakeholders an understanding of their cyber resilience objectives, and ensures appropriate action to support their synchronised implementation and testing.

(III) CONFIDENTIALITY

- IITL, along with preservation and protection of the security (as set out in detail above), also ensures confidentiality of customer information in the custody or possession of the service provider.

- Access to customer information by employees of the service provider to IITL is on 'need to know' basis i.e., limited to those areas where the information is required in order to perform the outsourced function.

- IITL further ensures that the service provider isolates and clearly identifies IITL's customer information, documents, records and assets to protect the confidentiality of the information. IITL has strong safeguards in place so that there is no comingling of information / documents, records and assets.

- IITL ensures that it immediately notifies RBI in the event of any breach of security and leakage of confidential customer related information.

(9) BACKUP OF DATA WITH PERIODIC TESTING

(i) In order to prevent loss of information by destruction of the magnetic means in which it is stored, a periodic backup procedure is carried out. The responsibility of backing up the information located in shared access servers is the network administrators'.

(ii) Restoration testing on a time to time basis is done as both hard disks and magnetic tapes are prone to errors. As a general rule, daily full backup happens for all critical business application and a complete weekly full backup is carried out including file servers/old data kept on servers.

(10) Software Usage Guidelines

The Software Usage Policy is defined to provide guidelines for appropriate installation, usage and maintenance of software products installed in organization-owned computer.

1. **Third-party software (free as well as purchased) required for day-to-day work will be preinstalled onto all company systems before handing them over to employees. A designated person in the IT Dept/Admin Dept can be contacted to add to/delete from the list of pre-installed software on organizational computers.**
2. **No other third-party software – free or licensed can be installed onto a computer system owned or provided to an employee by the organization, without prior approval of the IT Dept/Admin Dept**
3. **To request installation of software onto a personal computing device, an employee needs to send a written request via the IT Ticket System or IT Support Email.**
4. **Any software developed & copyrighted by the organization belongs to the organization. Any unauthorized use, storage, duplication or distribution of such software is illegal and subject to strict disciplinary action.**

COMPLIANCE :

5. **No employee is allowed to install pirated software on official computing systems.**
6. **Software purchased by the organization or installed on organizational computer systems must be used within the terms of its license agreement.**
7. **Any duplication, illegal reproduction or unauthorized creation, use and distribution of licensed software within or outside the organization is strictly prohibited. Any such act will be subject to strict disciplinary action.**
8. **The Admin Dept. procedures & guidelines need to be followed to purchase new software (commercial or shareware) for official purposes. All approved software will be purchased through the Admin Dept/Accounts Dept unless informed/permitted otherwise.**
9. **Any employee who notices misuse or improper use of software within the organization must inform his/her Reporting Manager(s).**

Software Audit

1. **The Legal and compliance dept. will conduct periodic audit of software installed in all company owned systems to make sure all compliances are being met.**
2. **Prior notice may or may not be provided by the Legal and compliance dept. before conducting the Software Audit.**
3. **During this audit, the IT Dept/Admin dept. will also make sure the anti-virus is updated, the system is scanned and cleaned and the computer is free of garbage data, viruses, worms or other harmful programmatic codes before submitting the same to legal and compliance dept for the check.**
4. **4) The full cooperation of all employees is required during such audits**

(11) AMENDMENT TO THE POLICY

The policy may be amended from time to time by the Board of Directors

(12) APPLICABILITY

The policy shall be effective from the date notified by the Board of Directors.