IBL FINANCE LIMITED

REGISTERED OFFICE: Shop – 151, Silver Stone Arcade, Nr. Kanthariya Hanuman Temple, OP-34/A+B+C+D,FP-50, Singanpore Causeway Road, Surat – 395004, Gujarat.

Information Technology Policy

1. Purpose

In terms of the provisions of Section-B of the Master Direction - Information Technology Framework for the NBFC Sector dated June 8, 2017, (“Master Directions”) issued by the Reserve Bank of India (RBI), every Non-Banking Financial Company (NBFC) having asset size less than Rs. 500 crores shall have Board approved Information Technology Policy/Information System Policy. This Information Technology Policy (“**IT Policy**”) is a formal document to provide guidance to the management of IBL Finance Limited (“**IBL**” / “**Company**”) for developing basic IT systems mainly for maintaining the database and follow the basic standards mentioned in the said Directions.

The Master Directions require the NBFCs to formulate and adopt an Information Technology Policy commensurate with the size, scale and nature of the business carried out by NBFC, which will act as a framework for usage of IT resources within the organisation. Accordingly, this IT Policy is adopted by the Board of the Company.

IBL provides unsecured personal loans digitally through its mobile app and therefore has access to the customer’s personal and financial information. To ensure confidentiality, integrity and availability of information, appropriate safeguards need to be in place to protect it from a wide range of threats. It is therefore essential that an appropriate set of controls and procedures are implemented to achieve information security.

2. Reference

In this IT Policy, a reference to the following word(s) shall have following meanings assigned to it:

2.1 Information Technology Resources:

Information Technology Resources for purposes of this IT Policy include, but are not limited to, IBL owned or those used under licence or contract or those devices not owned by IBL but intentionally connected to IBL - owned Information Technology Resources such as computer hardware, printers, fax machines, voice-mail, software, e-mail and internet and intranet access.

2.2 User:

Anyone who has access to Information Technology Resources, including but not limited to, all employees, temporary employees, contractors, vendors and suppliers.

2.3 Password:

A password is a string of characters used for authenticating a user on an Information Technology Resources of IBL.

3. Policy

The use of IBL’s Information Technology Resources in connection with IBL’s business and limited personal use is a privilege but not a right, extended to various Users. The privilege carries with it the responsibility of using IBL’s Information Technology resources efficiently and responsibly.

By accessing IBL’s Information Technology Resources, the User agrees to comply with this IT Policy. Users also agree to comply with the applicable laws and all governing contracts and licenses and to refrain from engaging in any activity that would subject IBL to any liability. IBL reserves the right to amend these policies and practices at any time without prior notice.

Any action that may expose IBL to risk of unauthorized access to data, disclosure of information, legal liability, or other potential system failure is prohibited and may result in disciplinary action, including termination of employment and/or criminal prosecution.

4. Scope

This IT Policy applies to everyone who, in India, has access to IBL’s Information Technology Resources and it shall be the responsibility of senior management at the registered office to ensure that this IT Policy is clearly communicated, understood and followed by all Users.

The IT Policy covers the usage of all of the Information Technology Resources and communication resources, whether they are owned or leased by the Company or are under the Company's possession, custody, or control, including but not limited to:

- All computer-related equipment, including desktop personal computers (PCs), portable PCs, terminals, workstations, PDAs, wireless computing devices, telecom equipment, networks, databases, printers, servers and shared computers, and all networks and hardware to which the equipment is connected.
- All electronic communications equipment, including telephones, pagers, radio communicators, voice-mail, e-mail, fax machines, PDAs, wired or wireless communications devices and services, internet and intranet and other on-line services.
- All software including purchased or licensed business software applications, IBL-written applications, employee or vendor/supplier-written applications, computer operating systems, firmware, and any other software residing on IBL-owned equipment.

This IT Policy also applies to all Users, whether on Company premises or otherwise, connected from remote connections via any networked connection, or using Company’s equipment.

5. Appointment of Head of IT

The Company shall designate one of its employees as Head of Information Technology (IT) department who shall ensure compliance of the IT Policy. The Head (IT) shall perform such function as specified in this IT Policy.

6. Responsibility Allocation

6.1 Board

The Board shall put in place a policy for effective management of IT assets of the Company and shall ensure its proper implementation by:

- approving IT strategy and policy documents and ensuring that the management has put an effective strategic planning process in place;
- ascertaining that management has implemented processes and practices that ensure that the IT delivers value to the business;
- ensuring IT investments represent a balance of risks and benefits and that the budgets are acceptable;
- monitoring the method that management uses to determine the IT resources needed to achieve strategic goals and provide high-level direction for sourcing and use of IT resources;
- ensuring proper balance of IT investments for sustaining Company's growth and becoming aware about exposure towards IT risks and controls.
- establishing a management level Committee consisting of appropriate business owners, the development team and other stakeholders to provide oversight and monitoring of progress of any IT project undertaken by the Company as part of its Change Management Policy.
- Ensure effective implementation of the Change Management Policy of the Company

The Board may delegate any one or all the above functions to a Board committee or management-level committee as it may deem fit subject to periodical reporting by the committee as decided by the Board.

6.2 Head (IT)/Senior Management

Head (IT) along with Senior Management of the Company shall be responsible for implementing the IT Policy. The Head (IT) shall further undertake functions as prescribed in this IT Policy.

7. Access Control

7.1 All Company computers that are either permanently or temporarily connected to the internal computer networks must have a password-based access control system. Regardless of the network connections, all computers handling confidential information must also employ appropriate password-based access control systems.

7.2 All in-bound connections to IBL computers from external networks must be protected with an approved password or ID access control system. Modems may only be used at IBL after receiving the written approval of the Head (IT) and must be turned off when not in use.

7.3 All access control systems must utilize user-IDs, passwords and privilege restrictions unique to each user.

7.4 Users shall not make copies of system configuration files (e.g. Passwords, etc) for their own, unauthorized personal use or to provide to other users for unauthorized uses.

7.5 Users are forbidden from circumventing security measures.

7.6 Users are strictly prohibited from establishing dial-up connections, using modems or other such apparatus, from within any IBL's premises.

7.7 Users who have been given mobile/portable laptop or any other device and duly authorized for such remote access, which connects to IBL's mail system on a real-time basis, can do so through the Internet.

7.8 Unless the prior approval of the senior management or Head (IT) has been obtained, Users shall not establish internet or other external network connections that could allow non-authorized users to gain access to IBL systems and information. These connections include the establishment of multi-computer file systems, internet web pages & FTP servers.

7.9 Users must not test, or attempt to compromise computer or communication system security measures unless specifically approved in advance and in writing by the senior management or CIO. Incidents involving unapproved system cracking (hacking), password cracking (guessing), file decryption, software copying, computer configuration changing or similar unauthorized attempts to compromise security measures will be considered serious violations of this IT Policy. Likewise, short-cuts bypassing system security measures is absolutely prohibited.

8. Passwords

8.1 Individual password security is the responsibility of each user.

8.2 Passwords are an essential component of IBL's computer and network security systems. To ensure that these systems perform effectively, the users must choose passwords that are difficult to guess. This means that passwords must not be related to your job or personal life. This also means passwords should not be a single word found in the dictionary or some other part of speech.

8.3 To make guessing more difficult, passwords should also be at least eight characters long.

8.4 To ensure that a compromised password is not misused on a long-term basis, Users are encouraged to change passwords every 30 days. Password history would be maintained for previous three passwords. This applies to the Systems Login (windows password) and Cloud Mail passwords.

8.5 Passwords must not be stored in readable form in batch files, automatic log-in scripts, software macros, terminal function keys, 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.

8.6 Immediately upon assignment of the initial password and in all cases of password "reset" situations, the password must be immediately changed by the user to ensure confidentiality of all information.

8.7 Under no circumstances, Users shall use another User’s account or password without proper authorization.

8.8 Under no circumstances, the User must share his/her password(s) with other User(s), unless the said user has obtained from the concerned senior management/Head (IT) the necessary approval in this regard. In cases where the password(s) is/are 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(s) was shared.

8.9 In cases where no prior approval had been obtained for sharing of password(s) with other user(s), such user shall be completely responsible for all consequences that shall follow in respect of breach of this IT Policy and IBL shall initiate appropriate disciplinary proceedings against the said User.

9. User Roles

9.1 **Administrator**: Head (IT) will be the Administrator for the Information Technology Resources. If a User requires special permissions, they should contact the Administrator, who shall have the following power and functions:

- Full access to host systems, routers, switches, firewalls and other security devices as required to fulfill their respective duties.
- Right to inspect any data stored on computer system in the course of investigating security incidents, or safeguarding against security threats.
- Ensure safe keeping of IT assets of the Company.

9.2 **Guest**: The Guest will have the read only permissions.

9.3 **Technician**: The Technician will have the well-defined set of permissions.

9.4 **Auditor**: The Auditor will have the permissions to view the details of software inventory, check for license compliance etc.

9.5 **IT Asset Manager**: IT Asset Manager will have complete access to the Asset Management Module.

10. 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. IBL ensures that it complies with this requirement to carry out all its business operations.

Further, Company shall appoint security officer to ensure security of IT systems while Head (IT) shall be responsible for implementation of the systems. The security officer shall perform formal checks through Internal Audit program.

11. Information Security and Cyber Security

It must be ensured that business information, inclusive of the computing systems is protected from inappropriate access, disclosure or modification. Information, as an asset, should be protected just as any other company asset and therefore to safeguard its value, IBL *via* this IT Policy has mandated for its employees to go through the IT Policy, understand, accept and practice the rules and regulations that have been defined. It is the Company's policy to:

- Ensure that information is accessible only to those authorized to have access;
- Safeguard the accuracy and completeness of information and processing methods;
- Ensure that authorized users have access to information and associated assets when required;
- Ensure that information it manages shall be secured to protect against the consequences of breaches of confidentiality, failures of integrity or interruptions to the availability of that information;
- Promote this IT Policy and raise awareness of information security;
- Provide appropriate information security training for the staff;
- Provide a distinct identification number for each information asset and maintain a list of all IT assets of the Company;
- In case the Company stores personal data of its customers, it shall use public key infrastructure to ensure confidentiality of data, access control, data integrity, authentication and nonrepudiation;
- Computer networks and systems outside of the Company is considered as insecure;
- To establish suitable data backup and retention policy

12. Incident Management Process and Cyber Crisis Management Plan

Incident shall refer to occurrence of any "Key Risk Indicator" as prescribed in the Para 12.1 of IT Policy. The employees shall be required to follow the specified process in this respect.

- The employees shall ensure that on occurrence of any Key Risk Indicator or unusual security incidents as specified in point 2 of Annex I of the Master Direction, such incident shall be brought to notice of the Head (IT) at the earliest,

- The Head (IT) may further report such incidents to the Board on yearly basis. No reporting shall be required where no such incidents have occurred.
- The affected system may be shut down immediately and all connections from such system shall be severed.
- It shall be strived that data in the system is deleted on the earliest to ensure there is no further compromise of sensitive data
- The back-up may be restored in the system only after consulting the Head (IT).

12.1 Key Risk Indicator

The Key Risk Indicators shall be:

- Frequent pop-up windows, especially the ones that encourage you to visit unusual sites, or download antivirus or other software
- Changes to your home page
- Mass emails being sent from your email account
- Frequent crashes or unusually slow computer performance
- Unknown programs that startup when you start your computer
- Programs automatically connecting to the Internet
- Unusual activities like password changes
- Any unauthorised activities in the system

Any suspicious activities/message appearing on the IT system.

13. Digital Signature Certificates, Mobile Financial Services and Social Media

13.1 Digital Signature Certificates

Digital signatures are considered accepted means of validating the identity of a signatory in IBL's electronic documents and correspondence, and thus a substitute for traditional "wet" signatures. This only applies to digitally signed documents and correspondence sent to the Company or received by the Company by IBL's employees and directors.

13.2 Mobile Financial Services

The Company gives unsecured personal loans digitally through its mobile application. The Company shall develop a mechanism for safeguarding information that is collected from the mobile application with a view to ensure confidentiality, integrity, authenticity and providing end-to end encryption. The Company shall also put in place a Board-approved Policy in this regard.

13.3 Social Media

The Company uses Facebook, Instagram, Google, Youtube, Linkedin, Pinterest, Twitter, Whatsapp and other social media platform available from time to time (hereinafter referred to as ‘Social Media’) to market its products. As Social Media is vulnerable to account takeovers and malware distribution, the Company shall have proper controls, such as encryption and secure connections to mitigate such risks.

14. System Generated Reports

The computer systems should be capable for generating reports for top management summarizing financial position including operating and non-operating revenues and expenses, cost benefit analysis of segments/verticals, cost of funds, etc.

Further, systems shall be designed to ensure that proper audit trails and sufficient data are available to enable effective functioning of audit function of the Company.

15. Adequacy to file regulatory returns to RBI (COSMOS)

The computer systems should be fully adequate to file all the applicable regulatory returns to RBI (COSMOS) and the same shall be reviewed from time to time.

16. Business Continuity Planning (BCP) Policy

Interruptions to business functions can result from major natural disasters such as earthquakes, floods, and fires, or from man-made disasters such as terrorist attacks, riots or war. The most frequent disruptions are less sensational - equipment failures, theft or sabotage.

Business Continuity Planning (BCP Plan), also known as Contingency Planning, defines the process of identification of the business verticals and locations that a business plans to keep functioning in the occurrence of such disruptive events, as well the failover processes & the length of time for such support. This encompasses hardware, software, facilities, personnel, communication links and applications.

BCP plan is intended to enable a quick and smooth restoration of operations after a disruptive event. It includes business impact analysis, where each critical business function has been reviewed to determine the maximum allowable downtime before causing significant degradation to the business operations of IBL.

The BCP plan also defines actions to be taken before, during, and after a disaster.

Purpose

The plan has been developed to allow for continuity of business operations at a minimum level within location of IBL at Surat, Gujarat in the event of an emergency.

BCP Objective

- Protect personnel, assets and information resources from further injury and/ or damage
- Minimize economic losses resulting from disruptions to business functions
- Provide a plan of action to facilitate an orderly recovery of critical business functions
- Identify key individuals who will manage the process of recovering and restoring the business after a disruption
- Identify the teams that will complete the specific activities necessary to continue critical business functions
- Specify the critical business activities that must continue after a disruption
- Recover critical business functions and support entities
- Minimize damage and loss
- Resume critical functions at an alternate location
- Return to normal operations when possible

BCP Committee Members:

01. Anamika Singh
02. Harshita Pipaliya

Recovery Management Co-ordinator (RMC)

Sunil Tarsariya

Procedure – Business Continuity Plan

This is a disaster recovery plan for IBL Data. The information present in this plan guides IBL operation & data management and technical staff in the recovery of computing and network facilities in the event that a disaster destroys all or part of the facilities. The primary focus of this BCP is to provide a plan to respond to a disaster that destroys or severely cripples IBL operation & data computer systems. The intent is to restore operations as quickly as possible with the latest and most up-to-date data available.

Disaster recovery plans are developed to span the recovery of data, systems, links and also include worst case scenarios such as:

1. Loss of access to facility
2. Loss of access to information resources
3. Loss of key personnel who are responsible for performing critical functions

Personnel

Immediately following the disaster, a planned sequence of events begins. Key personnel are notified and recovery teams are grouped to implement the plan. Personnel currently employed are listed in the plan.

Salvage Operations at Disaster Site

Early efforts are targeted at protecting and preserving the computer equipment. In particular, any storage media are identified and either protected from the elements or removed to a clean, dry environment away from the disaster site.

Designate Recovery Site / Alternate site / Backup site

The Company shall establish an alternative location (other than the city in which the business operation is located) as a backup site.

Purchase New Equipment

The recovery process relies heavily upon vendors to quickly provide replacements for the resources that cannot be salvaged. The IBL operation will rely upon emergency procurement procedures for equipment, supplies, software, and any other needs.

Begin Reassembly at Recovery Site

Salvaged and new components are reassembled at the recovery site. If vendors cannot provide a certain piece of equipment on a timely basis, then recovery personnel can make last-minute substitutions. After the equipment reassembly phase is complete, the work turns to concentrate on the data recovery procedures.

Executive Management Team (EMT)

This group consists of members of BCP Committee, the Recovery Management Coordinator. The Executive Management Group makes the decision to mobilize the IBL recovery organization. This decision is based upon their best judgment in determining the extent and impact of the outage.

Recovery Management Co-ordinator (RMC)

The Recovery Management Coordinator (RMC) is the individual who manages the recovery operation. She/He manages the following:

- administrative and logistical requirements of the recovery effort, and performance those duties and activities not directly related to the recovery of business functions.
- communication with all IBL employees during recovery operations.
- computer processing, internal/ external network connectivity and computer support requirements of the recovery effort.

Restore Data from Backups:

Data can be restored from other locations in case of any disaster. And if disaster effect the city as whole, say Surat, then back up data can be restored from the backup site.

Prevention

As important as having a disaster recovery plan is, taking measures to prevent a disaster or to mitigate its effects beforehand is even more important. This portion of the plan reviews the various threats that can lead to a disaster, where our vulnerabilities are, and steps we should take to minimize our risk. The threats covered here are both natural and human-created:

i. Fire

The threat of fire in office premises is real and poses a high risk. The building is filled with electrical devices and connections that could overheat or short out and cause a fire.

Hand-held fire extinguishers are placed in visible locations throughout the building. All Staff are trained in the use of fire extinguishers.

ii. Flood

Due care and appropriate preventive measure are carried out, thus risk due to flood is very much limited.

iii. Cyclones and High Winds

Very sever cyclone can only have marginal impact on the operations. Due care and preventive measure appropriate are carried out.

iv. Earthquake

The threat of an earthquake in Surat is medium to low but should not be ignored. An earthquake has the potential for being the most disruptive for this disaster recovery plan. Restoration of computing and networking facilities following a bad earthquake could be very difficult and require an extended period of time due to the need to do large scale building repairs.

The preventative measures for an earthquake can be similar to those of a Cyclone. Even if the building survives, earthquakes can interrupt power and other utilities for an extended period of time.

v. Computer Crime

Computer crime is becoming more of a threat as systems become more complex and access is more highly distributed. With the new networking technologies, more potential for improper access is present than ever before. Computer crime usually does not affect hardware in a destructive manner. It may be more insidious, and may often come from within. All systems have security products installed to protect against unauthorized entry. All systems are protected by passwords. All users are required to change their passwords on a regular basis. All systems should log invalid attempts to access data, and the system administrator reviews these logs on a regular basis.

All systems are backed up on a periodic basis. Physical security of the data storage area for backups is implemented. Standards have been established on the number of backup cycles to retain and the length of their retention.

vi. Terrorist Actions and Sabotage

Terroristic action and sabotage are potential risk under the circumstances on all the offices in big cities. To prevent such occurrence IBL has system in place whereby each office will permit entry on verification of identity and due care is taken to provide adequate security.

Testing and Evaluation

The response to each threat situations is tested periodically to assess the preparedness of the organization to execute the recovery plans. Some of the threats that occur frequently, are tested in due course of business, hence are not tested specifically. Others however, require testing and for them a disaster scenario is assumed and the team representatives "walk through" the recovery actions checking for errors or omissions. Persons involved in the test include the Recovery Management Coordinator.

An ongoing testing programme is established. However, special testing is considered whenever there is a major revision to IBL operation or when significant changes in hardware or communications environments occur. The Recovery Management Coordinator is responsible for analyzing change, updating impacts on the plan and for making recommendations for plan testing.

The Recovery Management Coordinator shall review the test results, discuss weaknesses, resolve problems and suggest appropriate changes to the plan.

17. Data Backup with Periodic Testing

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 for backing up the information located in shared access servers is the network administrators. It must be borne in mind that not only are hard disks inclined to fail, but also magnetic tapes are quite prone to errors that destroy their contents, so we need to do the restoration testing time to time basis.

- **General Rule**: As daily full backup is happening for all applications.
- **Data Backup in File Servers**: The system management backs up all the information in the file servers through an automated procedure.
- **Data Backup in Database Servers**: The system management backs up all the information in the databases through an automated procedure.
- **Data Backup in Desktop PC and Notebook**: This task is the responsibility of the user to whom the computer has been assigned.

18. Exemptions / Amendments / Delegations

The Board of Directors of the Company shall always have a right to amend / modify / waive any clause / requirement specified under this IT Policy.

****