



INFORMATION TECHNOLOGY POLICY
BERAR FINANCE LIMITED

RECORD OF REVIEW:

Document Number	01
Revision Number	03
Document Classification	Internal
Originally formulated	August 25, 2018
Created by	Secretarial Department
Reviewed by	Board of Directors of the Company
Approved by	Board of Directors of the Company

<u>Version No</u>	<u>Created/Modified Date</u>	<u>Created/modified by</u>	<u>Approved by</u>
1	August 25, 2018	Secretarial Department	Board of Directors
2	March 22, 2021	Secretarial Department	Board of Directors
3	April 28, 2022	Secretarial Department	Board of Directors

Table of Contents

Point No	Contain	Page No.
1	Intent	4
2	Purpose	4
3	Reference	4
3.1	Information Technology Resources	4
3.2	User	4
3.3	Policy	4
3.4	IT Strategy Committee & Governance Framework	5
3.5	Roles and Responsibilities of IT Strategy Committee	5
4	Policy	5
5	Scope	6
6	General standards for acceptable use of Berar Information Technology resources requirement	6
7	General Information Technology Usage Policy	7
7.1	Password	7
7.2	Access Control	7
7.3	Managing System Privileges	8
7.4	Change to System	8
7.5	Security (Access Control)	8
8	Software Licensing Policy	9
9	Internet and Intranet Usage Policy	9
10	Email Usage Policy	10
11	IT Operations	11
12	Acquisition and Development of Information Systems and Change Management	11
13	IT Outsourcing	11
14	Information System Audit	11
15	Helpdesk Process	11
16	Data Backup	12
17	Business Continuity Planning & Disaster Recovery	12
18	IT Enabled Management Information System	12

1. Intent:

Increased protection of information and Information Technology Resources to assure the usability and availability of those resources to all users of Berar Finance Limited is the primary intent of this Policy. The Policy also addresses privacy and usage guidelines for those who access Berar Finance Limited Information Technology Resources.

2. Purpose:

Berar Finance Limited recognizes the vital role information technology plays in effecting Company business as well as the importance of protecting information in all forms. As more information is being used and shared in digital format by Berar Finance Limited authorized users, the need for an increased effort to protect the information and the technology resources that support it, is felt by Berar Finance Limited and hence this policy.

Since a limited amount of personal use of these facilities is permitted by Berar Finance Limited to its users, including computers, printers, e-mail and Internet access, therefore, it is essential that these facilities are used responsibly by users, as any abuse has the potential to disrupt Company business and interfere with the work and/or rights of other users. It is therefore expected of all users to exercise responsible and ethical behavior while using Berar Finance Limited Information Technology facilities.

3. Reference:

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

3.1 Information Technology Resources:

Information Technology Resources for purposes of this Policy include, but are not limited to, the Company owned or those used under license or contract or those devices not owned by the Company but intentionally connected to Berar Finance Limited owned Information Technology Resources such as Computer hardware, printers, fax machines, voice-mail, software, e-mail and Internet and intranet access.

3.2 User:

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

3.3 Policy:

This Policy includes within its purview the following referred Policies:

- The General Information Technology Usage Policy
- The Software Licensing Policy
- The Internet and Intranet Usage Policy
- The E-mail Usage Policy
- The Helpdesk Process
- The Business Continuity Planning and Disaster Recovery
- Cyber Security Policy & Cyber Crisis Management Plan (CCMP)

3.4 IT Strategy Committee & Governance Framework:

Reserve Bank of India vide its circular RBI/DNBS/2016-17/53 (Master Direction DNBS.PPD.No.04/66.15.001/2016-17) of June 8, 2017 has given guidelines for Information Technology Framework for the NBFC sector ("Guidelines").

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.

This IT Framework falls within the scope of "Section A" of the Guidelines i.e. NBFCs with asset size of above INR 500 crores (Indian Rupees Five Hundred Crores only).

IT governance is an integral part of corporate governance of NBFC, and effective IT governance is the responsibility of the board of Directors of NBFC ("Board"), IT Strategy Committee, Risk Management Committee and its executive management.

Berar Finance Limited shall have IT strategy Committee consisting Whole Time Director, Independent Director, Chief Information Officer ("CIO") and Chief Technology Officer ("CTO"). The IT strategy Committee 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 & Disaster recovery Policy; (v) Back-up Data. For the purpose of effective implementation of the suggested IT Framework, the CIO is ensuring technical competence at senior/middle level management of BFL. The CIO is also managing the periodic assessment of the IT training requirements to ensure the availability of sufficient, competent, and capable human resources in the company.

3.5 Roles and Responsibilities of IT Strategy Committee:

- The Committee will be responsible for approving IT strategy and policy documents and ensuring that the management has put an effective strategic planning process in place.
- The Committee should focus and analyze that management has implemented the best practices and policies ensuring IT governance has delivered value to the business.
- The Committee will be responsible for Allotment of admissible budget for the IT infrastructure upgradation and new requirements for the business.
- The Committee will be responsible for Monitoring the IT framework and entire governance process to achieve strategic goals and suggest amendments, if required.
- The Committee should ensure the investments done for IT infrastructure sustaining Company's growth and becoming aware about exposure towards IT risks and controls.

4. Policy:

The use of the Berar Finance Limited information technology resources in connection with Berar Finance Limited business use and limited personal use a privilege but not a right, extended to various users. The privilege carries with it the responsibility of using the Users of Berar Finance limited Information technology resources efficiently and responsibly.

By accessing Berar Finance Limited Information Technology Resources, the user agrees to comply with this 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 Berar Finance Limited to any liability.

The Company reserves the right to amend these policies and practices at any time without prior notice. Berar Finance Limited has segregated the duties and implemented an IT enabled system for the IT Team, Security Officers for both physical security as well as cyber security and maintained detailed inventory of Information Asset with distinct and clear identification of the asset in soft copy and physical registers.

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

5. Scope:

This policy applies to everyone who is in India, has access to Berar Finance Limited Information Technology Resources and it shall be the responsibility of all Branch Managers in the Branches and Management at Head office to ensure that this policy is clearly communicated understood and followed by the users.

This Policy also applies to all contracted staff and vendors /suppliers providing services to Berar Finance Limited that bring them into contract with Berar Finance Limited Information Technology resources. The HR / Admin Department and the respective Branch Managers who contracts for these services shall be Responsible to provide the contractor /vendor /supplier with a copy of this Policy before any access is given to them These policies cover the usage of all of the Company's Information Technology 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, telecomm equipment, networks, databases, printers, servers and shared computers, and all networks and hardware to which this 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, Berar Finance Limited -written applications, employee or vendor/supplier-written applications, computer operating applications, employee or vendor/supplier-written applications, computer operating systems firmware, and any other software residing on Berar Finance Limited - owned equipment.
- All intellectual property and other data stored on Berar Finance Limited Information Technology equipment.
- These policies also apply to all users, whether on Company property or otherwise, connected from remote connections via any networked connection, or using Company equipment.

6. General standards for acceptable use of Berar Information Technology resources requirement:

- Responsible behavior with respect to the electronic information environment at all times
- Compliance with all applicable laws, regulations and Berar Finance Limited policies
- Respect for the rights and property of others including intellectual property rights
- Behavior consistent with the privacy and integrity of electronic networks, electronic data and information and electronic infrastructure and systems.

7. General Information Technology Usage Policy:

7.1 Passwords:

- Individual password security is the responsibility of each user.
- Passwords are an essential component of Berar Finance Limited computer and network security systems. To ensure that these system perform effectively, the user must choose password that 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.
- To make guessing more difficult, passwords should also be at least seven characters long. 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 Logon (windows pass word) and cloud mail passwords.
- 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.
- 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.
- Under no circumstances, Users shall use another user's account or password without proper authorization.
- Under no circumstances, the user must share his/her password(s) with other user(s), unless the said user has obtained from the concerned Branch Manager/Head Office authorized official 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.
- 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 Policy and the Company shall initiate appropriate disciplinary proceedings against the said user.

7.2 Access Control:

- All the Company computers that are either permanently or temporarily connected to the internal Computer networks must have a password-based control system. Regardless of the network connections, all computers handling confidential information must also employ appropriate password –based access control.
- All in-bound connections to the Company computers from external networks must be protected with an approved password or ID access control system Modems may only be used at the Company after receiving the written approval of the Management and must be turned off when not in use.
- All access control systems must utilize user-IDs, passwords and privilege restrictions unique to each user. Users are prohibited from logging into any Company's computer system

anonymously to prevent unauthorized access all vendor-supplied default passwords must be changed before the Company use.

- Access to the server room is restricted with RFID lock and only recognized staff or someone with due authorization from the Management is permitted to enter the room.
- 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.

7.3 Managing System Privileges:

- Requests for new user-IDs and changes in privileges must be made to the designated authority in Mail. Users must clearly state why the changes in privileges are necessary.
- In response to feedback from the Human Resources Department, the Management will revoke any privileges no longer needed by users. After receiving information from HR / Admin department all system access privileges will be terminated within 24 hours when a user leaves the Company.
- The Company management reserves the right to revoke the system privileges of any user at any time. Conduct that interferes with the normal and proper operation of the Company information Systems, which adversely affects the ability of others to use these information systems, or which is harmful or offensive to others will not be permitted.

7.4 Changes to Systems:

- No user must physically connect or disconnect any equipment, including the Company owned computers and printers, to or from any Company's network.
- With the exception of emergency situations, all changes to the Company information technology systems and networks must be documented, and approved in advance by the concerned Management.
- Only persons who have been authorized by the Management can make emergency changes to any Company's computer system or network.

7.5 Security (Access Control):

- There is maker-checker concept to reduce the risk of error and misuse and to ensure reliability of data/information
- Users are forbidden from circumventing security measures.
- Users are strictly prohibited from establishing dial-up connections, using modems or other such apparatus, from within any Berar Finance Limited premises.
- Users who have been given mobile/portable laptop / palmtop or any other device and duly authorized for such remote access, which connects to Berar Finance Limited mail system on a real-time basis can do so through Internet.
- Unless the prior approval has been obtained, users shall not establish Internet or other network connections that could allow non-authorized users to gain access to the Company's Computer systems and information. These connections include establishment of multi-computer file systems, Internet web pages & FTP servers.
- Users must not test, or attempt to compromise computer or communication system security measures unless specifically approved in advance and in writing by the Management. 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 the

Company policy. Likewise, short-cuts bypassing system security measures is absolutely prohibited.

8. Software Licensing Policy:

- For all software including purchased or licensed business software applications, the Company-written applications, employee or vendor/supplier-written applications, computer operating systems, firmware, and any other software residing on the Company owned equipment, all users must comply with the software licensing policy. They must not use/install/download any software for their individual use or even for business Purpose without prior approval of the Management at Corporate office. In case any such software found on any Company system which is not attached to the individual user, it shall be the responsibility of the user to inform the same to the IT department, in case the same is not installed by the said user otherwise the Company shall initiate appropriate disciplinary proceedings against the said user.
- The necessary software's are pre-installed on all the Company systems for day-to-day office needs. They generate system based reports for Top Management summarizing financial position including operating and non-operating revenue and expenses , cost benefit analysis of segments/vehicles, cost of funds. Request for any additional needs to be addressed to the Management for approval.
- Use of the Company network resource to illegally distribute or duplicate unauthorized copyrighted or licensed material is prohibited. Users shall not make unauthorized copies of copyrighted software, except as permitted by law or by the owner of the copyright.

9. Internet and Intranet Usage Policy:

- Internet software may only be installed / used by or with the approval of the Management. Software patches or updates may only be downloaded, subject to approval and ensuring strict adherence to the vendor's security and usage guidelines.
- Access to the internet and its resources is provided for the purposes of conducting business on behalf of the Company, filing of various returns to statutory authorities governing the Company such as MCA, RBI (XBRL Returns) etc Reasonable personal use of the Internet is permitted, according to constraints and conditions set by the Sophos Advanced Firewall.
- The management reserves the right to block access to any Internet resource without any prior notice, in case anyone required access to restricted site, the same may be dealt as special case provided the same is identified as use strictly for official purpose and conducting the Company's business. The approval for the same needs to be obtained by Department Head / Branch Manager from the Management.
- Similarly, to protect Berar Finance Limited IT systems from imported viruses, downloading or exchanging screensaver ,games ,entertainment software or other inappropriate files(for example video or audio materials for personal use),playing games against opponents or gambling over the internet is not permitted.
- Furthermore users may not conduct any form of "hacking" or use malicious code to penetrate or attempt to penetrate other computers or to deliberately release viruses or other harmful programs within either the Company network or the internet or bypass security features.

10. Email usage policy:

- All authorized users of the Company are provided with an official E- mail account created under the registered berarfinance.com domain and the same is protected with a password which is provided to the individual user. The use of E-mail should be restricted only for the business purpose; however personal mail can also be exchanged to a limited quantum provided that such exchange does not amount to breach of this IT policy or otherwise materially affects Berar Finance Limited operations. In case any individual is found using e-mail service, which is objectionable by any means, the access can be terminated by the management without any prior information, however the same may be re- instated with the approval from the Managing Director and the Management at the Head office.
- Email users should be aware that exchange of information with external sites may not be secured with high risks of spam, Trojans, malicious codes etc. Hence exchange of information should be limited to reliable sites. Users are prohibited to use their names /e-mail ids/mail domain in public domain without prior authorization from the management.
- Information must not be transmitted internally or externally which is beyond the bounds of generally accepted standards, values and ethics. This includes, for example, material which could be considered offensive or discriminatory; pornographic or obscene, defamatory or any other material which is otherwise abusive or contains illegal content prohibited by law or regulation of the country or which brings the organization into disrepute. Information is understood to include text, images and is understood to include printing information and sending information via email.
- All material contained on the email system belongs to the Company and users should consider messages produced/received by them on the Company account to be secure. The confidentiality of email data should be maintained by the individual user.
- Security regarding access to the email system is of paramount importance. User identities and personal passwords must not be shared with others. Users should be cautious of providing their email addresses to external parties, especially mailing lists.
- Users transferring or receiving files or attachments from external sources should note that the Company system automatically checks downloaded material for viruses. However, in the event that a virus is suspected, the file or attachment must not be opened and the matter must be reported to the Management immediately for inspection and action.
- The Company email users are required to use this communication tool in a responsible fashion and to observe the related guidelines. The Company provides the email system for the purposes of conducting official business and it may not be used for personal gain or business activities unrelated to Berar Finance Limited operations. Users must not use the system to promote an external cause without prior permission from the management.
- Reasonable personal use of the email system is permitted. Personal use of the e- mail service must not interfere with Berar Finance Limited operations, involve cost implications for the Company or take procedure over the user's job accountabilities.
- Where it is considered that there has been a breach in the use of the email system, the Service of the user will be terminated without any prior information.

11. IT Operations:

- a) IT Operations team is involved in maintaining IT resources, day-to-day activities and taking regular backup of crucial business data so that the required information is available in a timely, reliable, secure and resilient manner in case of System failure or disaster.
- b) The IT Strategy Committee, Risk Management Committee and Senior Management understands the risk associated with the existing and planned IT operations and the risk tolerance to establish and monitor policies for risk management.

12. Acquisition and Development of Information Systems and Change Management:

IT Strategy Committee shall also consider and review the following aspects:

- a) Acknowledging and planning the change proposals from business.
- b) Cost benefit analysis of the changes proposed.
- c) Analyzing risks associated with the changes proposed and understanding the impact.
- d) Actual change implementation, monitoring and reporting.

13. IT Outsourcing:

Berar Finance Limited ensures its service providers to develop and establish a robust framework for documenting, maintaining and testing business continuity and recovery procedures. Company also ensures that the service provider periodically tests the Business Continuity and Recovery Plan and occasionally conducts joint testing and recovery exercises with its service provider. In order to mitigate the risk of unexpected termination of the outsourcing agreement or liquidation of the service provider, company retains an appropriate level of control over their outsourcing and the right to intervene with appropriate measures to continue its business operations in such cases without incurring prohibitive expenses and without any break in the operations of our company and its services to the customers. Berar Finance Limited ensures that service providers are able to isolate crucial information, documents and records and other assets.

14. Information System Audit:

The Audit Committee ensures that an Information System Audit of the Internal System and processes is conducted at least once every year to assess operational risk faced by Berar Finance Limited.

Our designated Auditor performs examination of the Information technology (IT) infrastructure, resources and business applications. The audit reports and evaluation of evidence obtained determines if the information systems are properly safeguarding the IT assets, maintaining data integrity, and operating effectively to achieve our goals.

Berar Finance Limited ensures our information technology audits are used to evaluate our organization's ability to protect its information assets and to properly dispense information to authorized parties.

15. Helpdesk Process:

Berar Finance Limited has enabled an Enquiry & Complaint management process to handle, manage, respond and reporting the customer enquiries and grievances.

For our esteemed customers, on our official website we have provided options either to submit a query or report any concern along with the resolution SLAs and contact information for our Customer Care Head and Grievance Redressal Officer.

If the complaint of any Customer is not redressed within 30 days from the lodging of complaint with the Company or if the customer is not satisfied with the response of/ resolution provided by the Company, the customer may appeal to the Office of Ombudsman, RBI.

For enabling the Helpdesk Process, we have IT enabled software having dashboards and features like sending auto-confirmation email to the customer along with the ticket number. Our Customer Relationship Management (CRM) team acknowledges the enquiry/concern from the concerned customers, coordinates within the internal departments to provide the desired resolution.

For more information, please visit <https://www.berarfinance.com/contact.html>.

16. Data Backup:

In order to prevent loss of information by destruction of the magnetic means on which it is stored, a periodic backup procedure is carried out. Company takes daily backup in Data Server, designated system Hard Disk & Two Removable Hard Disks to have sufficient retrievable options.

Restoration testing on a time to time basis is done as both hard disks and other means are prone to errors. As a general rule, daily full backup happens for all critical business application data.

17. Business Continuity Planning (“BCP”) / Disaster Recovery (“DR”) :

BCP/DR forms a significant part of any organisation's overall Business Continuity Management plan, which includes policies, standards and procedures to ensure continuity, resumption and recovery of critical business processes.

BCP/DR at Berar Finance Limited shall be designed to minimize the operational, legal, financial, reputational, IT resources and other material consequences arising from a disaster. The functioning of BCP shall be monitored by the Board by way of periodic reports.

The BCP Committee Shall be is responsible for formulation, review and monitoring of BCP to ensure continued effectiveness including identifying critical business verticals, locations and shared resources to prepare a detailed business impact analysis. After the vulnerabilities and inter relationships between various systems, departments and business processes are identified, there should be a recovery strategy available with the BCP Committee to minimize losses in case of a disaster.

18. IT Enabled Management Information System:

Berar Finance Limited understands the important of the Data governance, which is an integral part of corporate governance of any company. We have business systems and applications in place to generate MIS reports that gathers data from multiple online systems, analyzes the information, and reports cleansed and formatted data to aid in management decision-making.

The ultimate goal of using the IT enabled management information system is to increase the value and profits of the business. This is done by providing managers, Board of Directors with timely and appropriate information allowing them to make effective decisions within a shorter period of time.
