GALADA FINANCE LIMITED

Information Technology Policy

Version 1.5

Version	Prepared by	Reviewed by	Approved by	Reviewed Date
1.0	K. R. Manimeghala	Naveen Galada	Board	09.11.2018
1.1	K. R. Manimeghala	Naveen Galada	Board	27.05.2019
1.2	K. R. Manimeghala	Naveen Galada	Board	25.07.2020
1.3	K. R. Manimeghala	Naveen Galada	Board	29.06.2021
1.4	K.R. Manimeghala	Naveen Galada	Board	28.05.2022
1.5	K.R. Manimeghala	Naveen Galada	Board	27.05.2023

Table of Contents

1. INTENT: 3
2. PURPOSE 3
3. REFERENCE 3
   - INFORMATION TECHNOLOGY RESOURCES 3
   - USER 3
   - POLICY 3
4. POLICY: 4
5. SCOPE 4
6. GENERAL STANDARDS FOR ACCEPTABLE USE OF GALADA FINANCE LIMITED INFORMATION TECHNOLOGY RESOURCES REQUIRE 5
7. GENERAL INFORMATION TECHNOLOGY USAGE POLICY 5
   - PASSWORDS 5
   - ACCESS CONTROL 6
   - MANAGING SYSTEM PRIVILEGES 6
   - CHANGES TO SYSTEMS 7
   - SECURITY (ACCESS CONTROL) 7
8. SOFTWARE LICENSING POLICY 8
9. INTERNET AND INTRANET USAGE POLICY 8
10. EMAIL USAGE POLICY 9
11. HELPDESK PROCESS 10
12. DATA BACKUP 10
13. BUSINESS CONTINUITY PLANNING (BCP) 11

1. Intent:

Increased protection of information and Information Technology Resources to assure the usability and availability of those resources to all users of Galada Finance Limited (The Company/GFL) is the primary intent of this Policy. The Policy also addresses privacy and usage guidelines for those who access the Company's Information Technology Resources.

2. Purpose:

The Company 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 the Company's IT resources authorized users, the need for an increased effort to protect the information and the technology resources that support it, is felt by the Company and hence this Policy.

Since a limited amount of personal use of these facilities is permitted by the Company to 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 behaviour while using the Company's Information Technology facilities.

3. Reference:

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

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 the Company-owned Information Technology Resources such as computer hardware, printers, fax machines, voice-mail, software, e-mail and Internet and intranet access.

User:

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

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

4. Policy:

The use of the Company's information technology resources in connection with the Company'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 the Users of the company's Information Technology resources efficiently and responsibly.

By accessing the Company's 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 the Company to any liability. The Company reserves the right to amend these policies and practices at any time without prior notice.

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 **every one who, in India, has access to the Company's Information Technology Resources and it shall be** the responsibility of the registered office to ensure that this policy is clearly communicated, understood and followed by all users.

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, the Company-written applications, employee or vendor/ supplier-written applications, computer operating systems, firm ware, and any other software residing on the Company-owned equipment.

- All intellectual property and other datas to read on the Company's 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 the Company Information Technology resources require:

- Responsible behaviour with respect to the electronic information environment at all times.

- Compliance with all applicable laws, regulations and the Company's policies

- Respect for the rights and property of others including intellectual property rights

- Behaviour consistent with the privacy and integrity of electronic networks, electronic data and information and electronic infrastructure and systems.

7. General Information Technology Usage Policy

Passwords

- Individual password security is the responsibility of each user.

- Passwords are an essential component of the Company'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.

- To make guessing more difficult, passwords should also be atleast 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(windowspassword)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 Board 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.

Access Control

- All the 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.

- 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 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 the Company system anonymously. To prevent unauthorized access all vendor-supplied default passwords must be changed before the Company's use.

- Access to the server room is restricted and only recognized IT staff or someone with due authorization 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.

Managing System Privileges

- Requests for new user-Ids and changes in privileges must be made to the IT Department in Mail. Users must clearly state why the changes in privileges are necessary.

- In response to feedback from the Human Resources Department, the IT department 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.

Changes to Systems

- No user must physically connect or disconnect any equipment, including the Company owned computers and printers, to or from any of the Company 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 Authority.

- Only persons who have been authorized by the Company can make emergency changes to any of the Company computer system or network.

Security (Access Control)

- 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 the Company's premises.

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

- Unless the prior approval of the Authority has been obtained, users shall not establish Internet or other external network connections that could allow non-authorized users to gain access to the Company systems and information. These connections include the establishment of multi-computer file systems, Internet web pages & FTP servers.

8. Cyber Security Policy

The Reserve Bank of India has issued new cyber security guidelines to entities directing them to devise cyber security policies distinct from their institutions' existing IT or IS security policies.

- This move comes in the wake of the growing frequency and impact of cyber attacks on the financial sector, underlining the urgent need for a robust cyber security/resiliency framework.

- Within this new notification, RBI calls upon entities to immediately put in place a cyber security policy duly approved by their board, containing an appropriate approach to combat cyber threats.

9. Cyber Crisis Management Plan

- As per RBI recommendation entities must evolve a cyber crisis management plan, considering that cyber risk is different from other risks, as the traditional BCP/DR arrangements may be inadequate.

- As per RBI recommendations entities are urged to follow guidelines and leverage its threat intelligence services to assess preparedness.

- Entities are to follow four aspects - detection, response, recovery and containment - as part of the cyber crisis management plan and promptly detect cyber-intrusions to respond/recover and contain the fallout.

- Entities should be aware of how to fight regular threats and take necessary preventive and corrective measures in addressing various types of cyber threats including, but not limited to : distributed denial-of-service attacks, ransomware/ cryptoware, 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, password related frauds, etc.

- The adequacy of and adherence to the cyber resilience framework should be assessed through development of indicators. These should be used for comprehensive testing through independent compliance checks and audits by qualified and competent professionals. Awareness among stakeholders, including employees, may also form part of it.

10. Users must not test, or attempt to compromise computer or communication system security measures unless specifically approved in advance and in writing by the Authority. 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 by passing system security measures is absolutely prohibited.

11. 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 and must not use/ install/ download any software for their individual use or even for business purpose without prior approval of the Authority at registered office. In case any such software is found on any of the Company system which is not allocated to the individual user, it shall be the responsibility of the user to inform the same to the IT department, in cases the same is not installed by the said user otherwise the Company shall initiate appropriate disciplinary proceedings against the said user.

- All necessary software's are pre-installed on all the Company systems for day-to-day office needs. Request for any additional needs to be addressed to the Authority for approval.

- Use of the Company network resources 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.

12. Internet and Intranet Usage Policy

- Internet software may only be installed/ used by or with the approval of the Authority. Software patches or updates may only be downloaded, subject to approval and ensuring strict adherence to the vendor's security and usage guidelines.

- The IT department reserves the right to block access to any Internet resource without any prior notice, in case any one 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 business. The approval for the same needs to be obtained by the Department Head/Branch Manager from the Authority.

- Similarly, to protect the Company's IT systems from imported viruses, down loading or exchanging screen savers, 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.

13. Further more, 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 with in either the Company network or the internet mail Usage Policy

14. Email Usage Policy:

- All authorized users of the Company are provided with an E-mail account, which is either individual to the specific user or generic Email ID 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 the Company's operations. In case any individual is found using e-mail service, which is objectionable by any means, the access can be terminated by IT department without any prior information, however the same may be re-instated with the approval from the Managing Director.

- 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 .

- 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 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 IT Department 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 the Company's operations. Users must not use the system to promote an external cause without prior permission from the Authority.

- Reasonable personal use of the email system is permitted. Personal use of the e-mail service must not interfere with the Company's operations, involve cost implications for the Company or take precedence 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.

15. Helpdesk Process

All locations with in India where the Company operates whether by itself or through its sub-agencies all help and support pertaining to the system/ user/ network/ back-end shall be provided by the registered office. In case any user finds any problem with the IT systems or need any help, they can send in their request to registered office via e-mail to info@galadafinance.in. In the event of emergencies the Authority may be contacted via telephone at+91-044-43099009 or+91-9381439096/+91-9600925757, however all phone calls must be followed by an e-mail letter.

16. Data Backup

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 critical business applications (i.e. Monday to Friday–set of 10tapesfor12weeks)and a complete weekly Full backup are carried out including file servers/old data kept on servers(i.e. on all Saturdays–set of 2 tapes), 11 tape for monthly backup and 1tape for yearly backup total using 24LTO6tapes and Magnetic tape library for whole month. Maintaining the magnetic tapes of the last12week's backups and after that all the tapes are into recycling mode after 84days.We are keeping the separately month end backup tape, as month end full backup on each last working day of every month, all the Software encrypted tapes are kept outside the Company's premises with the Managing Director of the company, in order to prevent data loss.

- **Data Backup in File Servers**: The Systems Management backs up all the information in the file servers through an automated procedure.

- **Data Back up in Database Servers**: The Systems Management backs up all the information in the data bases through an automated procedure.

- **Data Back up in Desktop PC and Note book**: This task is the responsibility of the user to whom the computer has been assigned.

17. BUSINESS CONTINUITY PLANNING (BCP)

- BCP 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 at NBFC is also designed to minimise the operational, financial, legal, reputational and other material consequences arising from a disaster. NBFC has a Board approved BCP Policy. The functioning of BCP shall be monitored by the Board by way of periodic reports.

- NBFC requires its service providers to develop and establish a robust framework for documenting, maintaining and testing business continuity and recovery procedures. NBFC 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, NBFC 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 NBFC and its services to the customers.

- NBFC ensures that service providers are able to isolate NBFC's information, documents and records and other assets. In appropriate situations, NBFC can remove, all its assets, documents, records of transactions and information given to the service provider, from the possession of the service provider in order to continue its business operations, or delete, destroy or render the same unusable.

- The CIO 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 CIO to minimise losses in case of a disaster. NBFC also has the option of alternate service providers and would be able to bring the outsourced activity back in-house in case of an emergency.

- NBFC also has in place necessary backup sites for their critical business systems and Data canters.

- These plans are also tested by NBFC on a regular basis. The results along with the gap analysis are placed by the CIO before the Board.