



# **Baid Leasing and Finance Co. Ltd.**

**Regd. Office:** “Baid House”, 2nd Floor, 1-Tara Nagar, Ajmer Road, Jaipur-06 Ph:9214018855  
**E-mail:** [baidfinance@baidgroup.in](mailto:baidfinance@baidgroup.in) **Website:** [www.balfc.com](http://www.balfc.com) **CIN:** L65910RJ1991PLC006391

## **BAID LEASING AND FINANCE CO. LTD**

### **INFORMATION TECHNOLOGY POLICY**

**Reserve Bank of India vide its circular RBI/DNBS/2016-17/53 (Master Direction DNBS. PPD.No.04/66.15.001/2016-17) dated 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 B of the Guidelines i.e. NBFCs with asset size of below 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 and its executive management.**

#### **Purpose:**

The purpose of the policy is to ensure that all computer systems and information facilities are used for the purposes intended by the organization.

#### **Scope:**

This policy applies to all employees, independent contractors, and third parties using systems (workstations, servers, LANs, WAN, and applications) owned or supported by the organization, within designated office premises or outside. They are referred to as "Users' or the purpose of this document.

#### **User Role:**

The information systems and facilities should be used in an efficient, effective, ethical, and lawful manner. Information systems shall include workstations, laptops, tablets, smart phones, all other appliances and gadgets provided by the organization for official use, LAN, WAN, servers, and applications (internally developed, third-party or hosted) as well as access to critical business data& other organization information.

Users are the individuals who have been authorized to access a system in order to perform job duties on a need to know basis. While users should be aware that all the data they create on the systems remains the property of **Baid Leasing and Finance Co. Ltd.** The organization shall take reasonable measures with respect to data privacy; users are responsible and accountable for the secure handling of the systems and data in their custody. Users are required to comply with all security policies and processes implemented by the company from time to time.



# Baid Leasing and Finance Co. Ltd.

Regd. Office: "Baid House", 2nd Floor, 1-Tara Nagar, Ajmer Road, Jaipur-06 Ph:9214018855  
E-mail: [baidfinance@baidgroup.in](mailto:baidfinance@baidgroup.in) Website: [www.balfc.com](http://www.balfc.com) CIN: L65910RJ1991PLC006391

## SECURITY ASPECTS

### Password Policy:

Use of company systems for the business purpose.

### Passwords:

- a. All passwords used to access computer systems should be safeguarded.
- b. The domain login passwords should be minimum 8 characters.
- c. Passwords must contain a mix of upper and lower case characters and have at least 2 numeric characters.
- d. The numeric characters must not be at the beginning or the end of the password. Special characters must be included in the password where the computing system permits. The special characters are (!@#\$% & \*+=?/~'";:,<>11).
- e. The password is required to be changed every 45 days.
- f. There should not be any default password (e.g.password@123,June@2013,etc.) or any dictionary word.
- g. Passwords should not be repeated for a minimum of 5 consecutive changes.
- h. Passwords must not be easy to guess.
- i. Passwords should not be printed, stored online, or given to/shared with others.
- j. Users are responsible for all transactions made / activities done using their accounts.

### Access Controls:

- Access to the Company'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 Company policies including but not limited to requirements laid down in this policy.
- Persons or entities with access to the Company'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 Company, 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 Company'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 Company 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.



# Baid Leasing and Finance Co. Ltd.

Regd. Office: "Baid House", 2nd Floor, 1-Tara Nagar, Ajmer Road, Jaipur-06 Ph:9214018855  
E-mail: [baidfinance@baidgroup.in](mailto:baidfinance@baidgroup.in) Website: [www.balfc.com](http://www.balfc.com) CIN: L65910RJ1991PLC006391

## Internet Usage Policy:

Internet access and other electronic communication systems [such as e-mail and voice mail] are essentials for day-today business operations. In order to maintain the integrity of the organization technology infrastructure and information, user awareness and precautions on security aspects is mandated:

- a. Only approved software, tools are to be used for official purposes. Users are prohibited from using non-Corporate e-mail accounts for official business communication.
- b. All official documents, including electronic communications are the property of the organization, and are subject to review, if required.
- c. Access to the internet is provided upon a valid request and subject to approval from suitable authority and should be used for official purposes.
- d. The organization has the right to log and review all on-line activity in order to identify any inappropriate use or abuse of the facilities provided.
- e. Internet access restrictions have been kept to the minimum. The protection & confidentiality of business data rests with the user. Any breach of the above clauses, which can be attributed to specific user activity will be the sole responsibility of the user and appropriate action may be taken by the organization.
- f. The organization prohibits the misuse of facilities to engage in anything that violates Company policy or wastes computer resources. This includes, but is not limited to; downloading or playing games, gambling, sending or viewing material that is harassing, obscene, offensive, sexually explicit, inappropriate, or spending excessive amounts of time connected to the Internet.
- g. Downloading any documents, software, audio, video, and pictures those are not business- related.
- h. Engaging in activity with the intent to: harass other users, degrade the performance of systems, deprive an authorized user access to a computer, circumvent computer security measures, or gain access to a Company system for which proper authorization has not been granted.
- i. Use of corporate equipment for storing or printing of inappropriate material is prohibited.
- j. Without prior written authorization from the IT Head, IT users shall not perform any of the following activities:
  - Copy software for use on any computer other than provided by the company.
  - Provide copies of software or any other documentation to any independent contractors/ Clients of Company or any third person.
  - Install unauthorized software on any of Company's IT equipment, workstations or servers.
  - Download any software from the Internet or other online service to any of IT equipment, workstations or servers; Modify, revise, transform, recast, or adapt any software.
  - Remove or disable any of the software or services which have been installed or configured by the organization.

Users shall connect to the internet using only the means provided by the organization.



# Baid Leasing and Finance Co. Ltd.

Regd. Office: "Baid House", 2nd Floor, 1-Tara Nagar, Ajmer Road, Jaipur-06 Ph:9214018855

E-mail: [baidfinance@baidgroup.in](mailto:baidfinance@baidgroup.in) Website: [www.balfc.com](http://www.balfc.com) CIN: L65910RJ1991PLC006391

## **E-mail:**

- a. All users are provided corporate mail account for official use. Gross misuse or violations [forwarding of chain mails, extremely large attachments to multiple recipients etc.] may invite Disciplinary actions. The company reserves the right to scrutinize all mail communication.
- b. Users should not open mail or attachments received from unknown people or suspected sources. This is to prevent inadvertent spread of viruses.

## **Social Networking Sites (Facebook, LinkedIn, Twitter, Flickr, personal blogs etc.)**

The organization supports open dialogue and the exchange of ideas. Users are expected for responsible engagement in collaboration, dialogue or participation in external / internal blog, wiki, online social network (such as Twitter or Facebook) or any other form of online publishing.

- a. Participation in forums or discussions is the user's own decision and at their own risk.
- b. Users are expected to act responsibly on forums and social media, users will be responsible for losses to the organization on account of user's participation on social media.
- c. Users are responsible for the privacy and confidentiality of personal information.
- d. Users are expected to refrain from sharing company related confidential information in the public domain.
- e. Online activities shall not interfere with user's official activities or commitment to organization customers.
- f. Respect copyright, fair use and financial disclosure laws.

## **Computing device Usage:**

- a. Desktops and laptops should be locked when left unattended.
- b. Printers should not be used to print personal documents.
- c. Users should collect information printed immediately so that company information and documents are not disclosed to unintended receivers.
- d. Company documents should be discarded properly through shredding process.
- e. Desktops and laptops should be disconnected from power supply sources at the end of every working day.
- f. Laptops and other devices should not be left in the office or at any outside location in an insecure manner. Loss or theft of the device is solely the user's responsibility.
- g. Access to USB storage devices or Pen Drive is prohibited. However access will be permitted on an exceptional basis to users with prior approval of a suitable authority
- h. Administrative privileges on the network or local systems will be granted on a need basis to select members of the technology team.
- i. Laptop Users, vendors or partners will be granted access to information and applications or systems upon approval from the appropriate authority.

## **Personal Device Usage:**

- a. Employees are permitted to access applications published on internet such as Outlook email, Office Communicator (Lync) from personal devices such as Mobile Phones or Smart phones, Tablets & Laptops.
- b. Access to corporate applications is permitted through a secure VPN port(virtual private network portal)subject to necessary review & approvals.



# Baid Leasing and Finance Co. Ltd.

Regd. Office: "Baid House", 2nd Floor, 1-Tara Nagar, Ajmer Road, Jaipur-06 Ph:9214018855  
E-mail: [baidfinance@baidgroup.in](mailto:baidfinance@baidgroup.in) Website: [www.balfc.com](http://www.balfc.com) CIN: L65910RJ1991PLC006391

- c. Personal devices such as Laptops, Smart Phones & Tablets can be connected to a separate wireless zone for accessing internet, however such devices will only be able to access applications published on internet such as Email& Communicator.

## **Incident reporting:**

- a. Users should report to the helpdesk any alert of virus infected file prompted by the anti-virus software. In case of doubt, it is recommended to call helpdesk and clarify.
- b. Users should report any weaknesses identified in computer security, any incidents of possible misuse, or violation of security policies to the concern IT person. This can be done via email or a call for clarification and assistance.

## **Violations:**

Any non-compliance with these requirements of this policy will amount to violation that may result in disciplinary action which may be:

- a. Warning notice.
- b. Short-term or permanent loss of access.
- c. Disciplinary actions including termination.
- d. Initiation of legal action including criminal prosecution under applicable Indian laws.

## **INFORMATION SECURITY AND CYBER SECURITY**

### ***(i) Information Security:***

*Company has an information security framework with the following principles:*

- **Identification and classification of information assets:** Company 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.). Company 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. Company 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



# Baid Leasing and Finance Co. Ltd.

Regd. Office: "Baid House", 2nd Floor, 1-Tara Nagar, Ajmer Road, Jaipur-06 Ph:9214018855  
E-mail: [baidfinance@baidgroup.in](mailto:baidfinance@baidgroup.in) Website: [www.balfc.com](http://www.balfc.com) CIN: L65910RJ1991PLC006391

components. Company 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 centers 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. Company ensures that it complies with this requirement to carry out all its business operations.
- **Trails** - Company 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.
- **Mobile Financial Services** – Company has a mechanism for safeguarding information assets that are used by mobile applications to provide services to customers. The technology used by Company for mobile services ensures confidentiality, integrity and authenticity and provides for end-to-end encryption.
- **Social Media Risks** – Company 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. Company 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. Company protects the authenticity and integrity of important electronic documents and also for high value fund transfer.
- **Regulatory Returns** – Company has adequate system and formats to file regulatory returns to the Reserve bank of India ("RBI") and other authorities on a periodic basis. Filing of regulatory returns is managed and verified by the authorised representatives of Company.

## (ii) **Cyber Security**

- Company takes effective measures to prevent cyber-attacks and to promptly detect any cyber- intrusions to respond / recover / contain the fall out. Among other things, the Company 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.
- Company realises 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. Company ensures that the top management and



# **Baid Leasing and Finance Co. Ltd.**

**Regd. Office:** “Baid House”, 2nd Floor, 1-Tara Nagar, Ajmer Road, Jaipur-06 Ph:9214018855  
E-mail: [baidfinance@baidgroup.in](mailto:baidfinance@baidgroup.in) Website: [www.balfc.com](http://www.balfc.com) CIN: L65910RJ1991PLC006391

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**

- Company, along with preservation and protection of the security, 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 Company is on 'need to know' basis i.e., limited to those areas where the information is required in order to perform the outsourced function.
- Company further ensures that the service provider isolates and clearly identifies Company's customer information, documents, records and assets to protect the confidentiality of the information. Company has strong safeguards in place so that there is no comingling of information / documents, records and assets.

Company ensures that it immediately notifies Reserve Bank of India (“RBI”) in the event of any breach of security and leakage of confidential customer related information.

### **BACK-UP OF DATA 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 of backing up the information located in shared access servers is the network administrators’.
- 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.

### **POLICY REVIEW**

The Board of the Company may review this policy from time to time, and as required.