INFORMATION TECHNOLOGY USAGE POLICY

The Reserve Bank of India ("**RBI**") has issued various guidelines to all regulated entities with an aim to enhance safety, security, and efficiency in processes leading to benefits for such regulated entities and their customers. The Information Technology Usage Policy ("**Policy**") of Jayshree Dealers Private Limited ("**the Company**") has been prepared and reviewed in accordance with the extant regulations of the RBI in this regard.

The Company has decided to outsource its Information Technology ("**IT**") platforms and its upkeep / maintenance to agencies adept at handling such matters, in accordance with the Outsourcing Policy of the Company. To ensure effective implementation of this Policy, the Company shall assess the technical competence of the technical outsourced agencies / technical service providers and their ability to adhere to the contents of this Policy. The Board shall (either through itself, or a sub-committee constituted in this regard, or through the appointment of a Designated Director in this regard) exercise oversight and supervision of all technical activities and their adherence to this Policy. The Company shall also undertake periodic assessment of the IT training requirements to ensure the availability of sufficient, competent and capable human resources in the Company as well as in its service providers.

I. SECURITY ASPECTS

A. Password Policy

All users **of the Company website / applications (including employees)** are responsible for keeping their passwords secure and confidential. The password credentials of the users must comply with the password parameters ("Complexity Requirements") and standards laid down in this **Policy**. Passwords must not be shared with or made available to anyone in any manner that is not consistent with this **Policy**. The Complexity Requirements for setting passwords are as follows:

1) A strong password must be at least 8 (eight) characters long.
2) It should not contain any of the user's personal information—specifically his/her real name, username, or even company name.
3) It must be unique from the passwords used previously by the users.
4) It should not contain any word spelled completely.
5) It should contain characters from the four primary categories i.e. uppercase alphabets, lowercase alphabets, numbers, and characters.

6) To ensure that a compromised password is not misused on a long-term basis, users are encouraged to change the password every 30 (thirty) days.

7) Passwords must not be stored or written down in readable form on computers / other devices / paper without access control systems or in other locations where unauthorized persons might discover them.

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

9) Under no circumstances, shall the users use another user's account or password without proper authorization.

B. Access Controls

1) All access is governed by policies of the Company including but not limited to requirements laid down in this policy.

2) 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 the Company, irrespective of the medium on which the information resides.

II. INFORMATION SECURITY and CYBER SECURITY

A. Information Security

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

1) *Identification and classification of information assets*: The Company maintains detailed inventory of information assets with distinct and clear identification of the asset.

2) *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.

3) *Role Based Access Control:* Access to information is based on well-defined user roles (system administrator, user manager, application owner). The Company has a clear delegation of authority to upgrade/change user profiles and permissions and key business parameters.

4) *Personnel Security:* A few authorized application owners/users may have intimate knowledge of financial institution processes and they pose a potential

5) threat to systems and data. The Company has a process of appropriate checks and

6) 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, including that of outsourced agencies assisting the Company in technology related matters.

7) *Physical Security:* The confidentiality, integrity, and availability of information can be impaired through physical access and damage or destruction to physical components. The Company has created a secure environment for physical security of information assetssuch 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.

8) *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 also ensure reliability of information. The Company, through various SOPs, ensures that it complies with this requirement to carry out all its business operations.

9) *Trails:* The 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.

10) *Digital Signatures:* A Digital Signature certificate authenticates the entity's identity electronically. The Company protects the authenticity and integrity of important electronic documents.

11) *Regulatory Returns:* The Company has an adequate system and formats to file regulatory returns to the RBI on a periodic basis. The filing of regulatory returns is managed and verified by persons duly authorized by the Company.

B. Cyber Security

1) The 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.

2) Then Company realizes that managing cyber risk requires the commitment of the entire organization to create a cyber-safe environment. This requires a high level of awareness among staff at all levels. The Company ensures that its employees, outsourced agencies and the Board have a fair degree of awareness of the fine nuances of the threats.

III. CONFIDENTIALITY

1) The Company ensures preservation and protection of the security (as set out in detail above).

2) The Company also ensures confidentiality of customer information in the custody or possession of the Company and its service providers.

3) Access to customer information by employees of the service provider is done only on a 'need to know' basis i.e., limited to those areas where the information is required by the service provider to perform the outsourced function.

4) The Company further ensures that the service provider isolates and clearly identifies the customer information, documents, records, and assets of the Company to protect the confidentiality of the information. The Company has strong safeguards in place so that there is no comingling of information / documents, records, and assets at the service provider level.

5) The Company shall also ensure that it immediately notifies the RBI in the eventuality of any breach of security and leakage of confidential customer-related information.

IV. BACK-UP OF DATA WITH PERIODIC TESTING

1) In order to prevent loss of digitally stored information, a periodic backup procedure is carried out.

2) Restoration testing on a time-to-time basis is done as both hard disks and magnetic tapes are prone to errors. 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.

The Board shall review this Policy from time to time, in accordance with further developments in Information Technology norms and modifications in the extant RBI guidelines in this regard.