BUSINESS CONTINUITY PLAN (BCP)

JMJ FINANCE LIMITED

Purpose

JMJ FINANCE LIMITED (or "JMJ") wishes to adopt industry leading best practices in establishing a set of operating principles which govern how risks of a significant business disruption are mitigated to protect the Company's customers, employees and stakeholders. The Company has a well defined business continuity program which comprises of policies and procedures with clearly defined roles, responsibilities and ownership for Crisis Management, Emergency Response, Business recovery and IT Disaster Recovery Planning. The Board and senior management of the Company approves and oversees the annual BCP strategy and road map. This Business continuity program is developed to manage the impact of significant disruptions and will endeavour to resume business and operations to an acceptable level within a reasonable time in the event of a disaster. BCP at JMJ is also designed to minimise the operational, financial, legal, reputational and other material consequences arising from a disaster.

Scope

This plan shall apply to all operations wherein the Company is likely to get affected in terms of income, assets, reputation, property etc. The BCP is prepared to cope with any unforeseen natural or man-made disasters on the JMJ's business.

This policy shall be read along with IT policy of the Company for more clarity.

Measures/ Initiatives

The measures taken by the JMJ are as follows-

- In order to mitigate the risk of unexpected termination of the outsourcing agreement or liquidation of the service provider, JMJ 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 JMJ and its services to the customers.

- JMJ ensures that service providers are able to secure JMJ's information, documents and records and other assets.

- In appropriate situations, JMJ 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 IT team is primarily responsible for review of IT related aspects of software and other IT resources and to ensure continued effectiveness including identifying critical business verticals, locations and shared resources to enable the senior management prepare a detailed business impact analysis. The IT team may contact concerned Head of Departments for details of operations and risk involved in each level.

- After the vulnerabilities and inter relationships between various systems, departments and business processes are identified, there should be a recovery strategy available with the senior management to minimise losses in case of a disaster.

- JMJ 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.

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

- CIO shall be appointed to ensure the implementation of this policy with support of IT Department and other concern officials.

- These plans are also tested by JMJ on a regular basis. The results along with the gap analysis are placed by the CIO/Head of IT department, as the case may be, before the Board, whenever required.

- JMJ has necessary backup facility for their critical business systems and Data centres.

- JMJ shall test the BCP either annually or when significant IT or business changes take place to determine if the entity could be recovered to an acceptable level of business within the timeframe stated in the contingency plan. The test should be based on 'worst case scenarios'. The results along with the gap analysis may be placed before the Board. The GAP Analysis along with Board's insight should form the basis for construction of the updated BCP.

- 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.

The Board approves of this IT Framework and has overall charge of the operational functions of JMJ.

The Board is further responsible for timely amending this IT Framework pursuant to its operations and/or any change in the regulations or new regulations issued by the RBI in relation to this IT Framework.

//**Approved//**