MEENSKSHI MERCANTILES LIMITED

CYBER CRISIS MANAGEMENT PLAN

1. PREAMBLE

The Board of Directors (the "Board") have adopted this Cyber Crisis Management Plan in order to prescribe the procedure to handle any cyber-attack on the company and its information technology resources. The Board is empowered to review and amend this Code from time to time.

2. PURPOSE AND OBJECTIVE

The purpose of this plan is to ensure that all relevant stakeholders are fully aware of the process to be followed during cyber crisis.

Objective of this plan is to establish Cyber Crisis Management practices throughout the organization and its business units for identifying, responding and managing the cyber crisis which may occur across the enterprise environment.

3. MEANING OF CYBER CRISIS

Cyber crisis is an adverse event where:

- The IT system is attacked or threatened with an attack.
- The IT system is compromised in a situation such as malware attacks, advance persistent threats etc.

4. INCIDENT REPORTING

- The Chief Financial Officer will assess the incident which may lead to cyber crisis based on the above defined classification criteria (mentioned in point no. 3 of Plan) and report it to the Board for further decision making.
- Upon the knowledge of the crisis in any situation, the Board would assess the situation and after due discussion, will decide whether 'Cyber Crisis' needs to be declared and if declared, shall accordingly form a Cyber Crisis Management Team (CCMT) comprising of members as the board may specify.

5. ROLE OF THE CYBER CRISIS MANAGEMENT TEAM

- Upon being appointed, the CCMT will take immediate cognizance of the crisis and shall inform relevant stakeholders involved in the incident.
- The CCMT will collate all information required for assessing the cyber crisis and its immediate impact. Necessary instructions will be given to the affected personnel to minimize negative impact to the organization's operations.

MEENAKSHI MERCANTILES LIMITED

6. OBJECTIVES OF CYBER CRISIS MANAGEMENT TEAM (CCMT):

- Assess the situation and take decision as per the Cyber Crisis management plan.
- Manage external and internal communications.
- Guide the stakeholders throughout the duration of the cyber crisis.
- Prepare a recovery plan and resumption timetable.
- Approve appropriate expenditure(s).

7. DECISION MAKING

- The CCMT shall take a decision on managing the cyber crisis and inform the Board about the decision for recovery procedures.
- CCMT shall take decision on appropriate communication strategy for communicating with the stakeholders including but not limited to shareholders, employees, regulatory authorities, etc., in accordance with the severity of the cyber crisis as the CCMT may deem necessary.
- CCMT shall take a decision to engage with relevant law enforcement agencies and/or regulatory authorities for further investigation or support.
- CCMT shall take a decision on invoking the BCP/DR if necessary.
- CCMT shall take a decision on options available for effective incident response and recovery from a cyber-crisis based on the operational/business/cost implications.

8. POST EVENT ANALYSIS

- Root cause analysis and documenting learnings.
- Managing the preservation of the evidences collected.
- Recording details of all decisions and actions taken.
- Reporting to regulatory authorities, (if required).
- Declaration to media (if any).

9. MONITORING AND REVIEW

The Board shall review the plan from time to time and shall have the power to amend the plan or repeal the same by introducing a new Cyber Crisis Management Plan as it may deem necessary in the best interest of the Company.