UDAIPUR COTTON MILLS COMPANY LIMITED

INFORMATION TECHNOLOGY POLICY

1. Introduction

1.1. Master Directions – Information Technology Framework for Non-Banking Financial Company (NBFC) Sector ('Master Directions') were issued by the Reserve Bank of India (RBI) on June 8, 2017. The broad intention of Master Directions was to enhance safety, security, efficiency in information technology processes leading to benefits for NBFCs and their customers.

1.2. The Master Directions require the NBFCs to formulate and adopt an Information Technology (IT) Policy which commensurate with the size, scale and nature of the business carried out by NBFC and which will act as a framework for usage of IT resources within the organization.

1.3. However, keeping in mind, the directions issued by the RBI in this regard, the following internal policy ('IT Policy' or 'Policy') has been formulated and adopted by the board of directors of the Company.

1.4. For the purpose of this Policy, the term "IT" would include but not be limited to the Company's IT network, hardware including portable media, system and application software, communication components including telephone and WAN systems, documentation, physical environment & other information assets.

2. Scope

2.1. This policy applies to all our employees (including secondees who have been seconded to the Company from other organizations), contractors, vendors and anyone who has permanent or temporary access to our systems and hardware.

2.2. The Company's staff shall sign confidentiality (non-disclosure) undertaking as a part of their employment contract, and any temporary staff (including agency staff) and secondees sign the standard confidentiality undertaking before they are permitted to use the Company's systems.

2.3. This policy cover the usage of all 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 desktops, laptops/netbooks, terminals, workstations, wireless computing device, mobile phones, electronic storage devices such as DVDs, CDs, memory sticks, telecom

equipments, networks, databases, printers, servers, pen drives, hard drives, and all networks and hardware to which thus equipment is connected.

- All software including purchased or licensed business software applications – written applications, employee or vendor/supplier, computer operating systems/applications, firmware and any other software residing on Meenakshi Mercantiles Limited.

- All intellectual property and other data stored on Company's Information Technology equipment.

3. Objectives and Purpose

3.1. The objectives of this Policy are, to ensure:

3.1.1. that the identification and acquisition of the IT systems are carried out keeping in mind size, scale & nature of the business;

3.1.2. that the IT systems are made available and accessible as and required by the staff of the Company for effectively performing it duties;

3.1.3. technical competence at each level of employees and to carry out periodic assessment of the technical competence of the employees;

3.1.4. the Company uses up to date technology.

3.2. This Policy sets out the IT security principles including the maintenance, storage & disposal of data, explains the implementation procedure ensuring a centralized and consistent approach to IT security.

3.3. The Policy ensures supporting the business objectives of the Company by balancing the security, integrity & availability of IT systems against the need for staff to access systems and services that are necessary for their job, within the limits imposed by this Policy.

3.4. The Policy will protect the misuse of company's data and minimize the impact of service disruption by setting standards and procedures to manage and enforce appropriate IT security.

3.5. The Policy supports the legal obligations of the Company to maintain the security and confidentially of its information, notably under the Data Protection Act 1998, the Copyright Patents and Designs Act 1988 and the Computer Misuse Act 1990, and supports adherence to information governance standards set by the Master Directions.

4. Roles and Responsibilities

The roles and responsibilities of the various stakeholders pertaining to the IT Policy are as follows:

4.1. Board of Directors –
Approving the IT Policy

4.2. Information Security Committee (ISC) –

- Members of the Committee: Chairperson & Managing Director, 1 Independent Director, Chief Information Security Officer, Expert from IT Department
- Chief Information Security Officer: Executive Director
- Convener: Assistant Company Secretary
- Periodicity of Convening: Once in a year
- Responsibility/Role of the Committee:
  - Analyze the effect of the IT organizational design on the strategy and direction of IT and the Company's business.
  - Ensure that all existing and new Users are instructed about their security responsibilities.
  - Implementing procedures to minimize the Company's exposure to fraud, theft or disruption of its systems.
  - Ensuring day to day management and security of the systems, equipment and services, with specific technical responsibilities being allocated amongst the team and to the outsourced service providers.
  - Spreading awareness amongst the Users about this Policy and ensuring that Users understand and abide by them while carrying out work on Company's behalf.
  - Ensuring compliance with relevant legislation, policies, and good practice for all internal systems.
  - Ensure implementation of IT Policy to the operational level involving IT strategy, Value Delivery, Risk Management, and IT Resource Management.

4.3. Chief Information Security Officer (CISO) –

- Provide support to the Board and ISC in establishing, implementing, monitoring, reviewing, maintaining and improving the overall Information Security of the Organization.
- Coordinating the ISC meetings.
- Coordinating information security initiatives in the organisation.
- Facilitating and Conducting risk assessments of Information Assets used and recommend mitigation controls.
- Promote security awareness amongst staffs, customers and service providers.

4.4. The Users shall ensure the following:

4.4.1. Keep all devices password protected.
4.4.2. Timely upgrade a complete antivirus software.
4.4.3. Do not leave their devices exposed or unattended.
4.4.4. Install security updates of browsers and systems on a monthly basis or as soon as updates are available.

4.4.5. Log into company accounts and systems through secure and private networks only.

4.4.6. Report perceived attacks, suspicious emails or phishing attempts as soon as possible to the senior management.

5. Cyber Security

5.1. The Company shall have in place adequate systems to detect any incidents of cyber security crisis at the earliest possible instance.

5.2. The senior management must organize awareness programs or training among the stakeholders to spread awareness about cyber security threats, magnitude of risks associated with them, their likely impact and the remedial course of action in case of impact.

5.3. As soon as a cyber crisis is detected in the organization, the Company shall immediately switch off all the networks connected to the device or server that is compromised.

5.4. The magnitude of the attack and their likely impact must be identified and such assets/ information must be blocked from any usage.

5.5. All servers must be secured by hardening and ensure that antivirus solution is installed, updated and available on all the System(s).

5.6. The amount of data lost or damage must be calculated and fresh networks and systems must be installed. The degree of theft or compromise must be analyzed and recorded.

5.7. Options to recover the data and the damage done along with any required legal action must be explored from regulatory viewpoints.

5.8. All the systems must be updated to prevent occurrences of such incidents in future.

6. IT Security

6.1. Technical security measures have been put in place in order to protect the Company's IT systems from viruses and other malicious software, and all IT systems shall be monitored for potential security breaches.

6.2. All connections to external computer networks and systems including privately owned IT equipment of all kinds must be approved by the senior management.

6.3. All Company laptops/personal computers must be encrypted with access to the Company's IT networks using a strong authentication method.

6.4. Digital signatures shall be used, wherever possible, to protect the authenticity

and integrity of important electronic documents and for high value fund transfer.

6.5. The Company does not intend and shall not be using mobile financial services or social media.

6.6. The Company shall automate controls by introducing a computer program with logical access, segregation of duties and maker/checker controls to minimize the chance of fraudulent payments. However, maker cannot check/authorize the transactions made by him/her. This will reduce the risk of error and will ensure reliability of information.

7. Software Protection

7.1. Only licensed copies of the commercial software or in house developed software are to be used by the Company. A register of all commercial software, including all software licenses, shall be maintained to ensure that the Company complies with the license conditions and relevant laws. Users must not install any externally developed software on Company's IT equipment without prior approval of the senior management.

7.2. The Users shall be made aware that use of unauthorized copies of commercial software is a criminal offence and shall be subject to disciplinary action

7.3. Application of a robust anti-virus software and firewall policy shall be ensured. The Users shall report any detected or suspected viruses, Trojan, spyware or malware on the User's computer to the senior management.

8. IT enabled Management Information System

8.1. It is important to setup a Management Information System (MIS) which is robust and comprehensive in respect of various business functions and as per the needs of the business.

8.2. In this regard, a MIS system shall be put in place to assist the Top Management as well as the business heads in decision making and also to maintain an oversight over operations of various business functions.

9. User access control to the IT network drives

9.1. No individual will be given access to the IT network unless properly trained and made aware of his or her security responsibilities. The access to IT network drives will be modified or removed as appropriate when a person changes job or leaves the Company.

9.2. No remote access to Company's IT systems will be given to third parties at any

time unless specific authorization is received.

9.3. Users are not permitted to store entertainment files (including but not limited to music, pictures, video, electronic games) upon the Company's IT systems.

10. Business Continuity Planning

The Company shall identify business activities and critical processes in each department, time involved, and details of back-up processes.

A business impact analysis for fund based as well as non-fund-based activities of the Company shall be carried out and risk exposures should be identified.

Based on identifications, a Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP) has been put in place. The DRP includes the following:

- smooth transition to recovery operations following a major incident or event (or disaster);
- escalation of recovery operations in the event of a prolonged disruption; and
- ways to return to normal operations as quickly as possible.

Senior management will assess the greatest risks, the techniques to mitigate, control, or limit the risks, the actions are required to address the greatest exposures including activation of a DRP, and an estimate of costs.

Senior management will thereafter assess the cost-risk trade-off before making decisions and seeking approval from the Board of Directors.

Senior officials of the company shall ensure adherence to business continuity and disaster recovery plans, provide training to the staff for proper implementation of plans and conduct regular testing and upgrading of these plans, whenever required.

11. IT Risk Assessment

MML Should undertake a comprehensive risk assessment of their IT systems on a yearly basis or as decided, keeping in mind the organizational and compliance requirements.

The assessment shall analyze the threats and vulnerabilities to the information technology assets of the organization and its existing security control and processes.

12. Information System (IS) Audit

The objective of the IS Audit is to provide an insight on the effectiveness of controls that are in place to ensure confidentiality, integrity and availability of the organization's IT infrastructure. IS Audit shall identify risks and methods to mitigate risk arising out of IT infrastructure such as server architecture, local area networks, physical and information security, telecommunications, etc.

IS Audit forms and integral part of Internal Audit system of the organization. The organization shall have adequately skilled personnel in Audit Committee who can understand the results of the IS Audit.

IS Audit should cover effectiveness of policy and oversight of IT systems, evaluating adequacy of processes and internal controls, recommend corrective action to address deficiencies and follow-up. IS Audit also evaluates the effectiveness of business continuity planning, disaster recovery set up and ensure that BCP is effectively implemented in the organization.

IS Audit being conducted by an internal team of the organization, having a right mix of skills and understanding of legal and regulatory requirements so as to assess the efficacy of the framework.

IS Audit is conducted once in a year. It is undertaken prior to the statutory audit so that IS Audit reports are available to the Statutory Auditors well in time for examination and for incorporating comments, if any, in the audit reports.

13. Password protection

Password leaks are dangerous since they can compromise our entire infrastructure. It shall be ensured that the passwords are secured so they cannot be easily hacked and remain secret. The Users shall ensure the following:

- Choose passwords with at least eight characters (including capital and lower-case letters, numbers and symbols) and avoid information that can be easily guessed (e.g., birthdays.)
- Remember passwords instead of writing them down. If there is a need to write the password, the User shall be obliged to keep the paper or digital document confidential and destroy it when the work is done.
- Exchange credentials only when necessary.
- Change the passwords every two months.

14. System generated reports

The Company shall integrate its systems in a manner such that the same can generate summarized reports of financial position including operating and non-operating revenues and expenses, cost benefit analysis of segments/verticals, cost of funds, etc. for the purpose of facilitating top management in analysis of financial position. Further, the Company shall put in place adequate systems and procedures required for filing of various regulatory returns to RBI through COSMOS.

15. Disaster recovery and back up

Critical computer equipment must be fitted with battery back-ups (UPS) to

UDAIPUR COTTON MILLS CO. LTD.

ensure that it does not fail during switchovers or emergency shutdowns. The Company shall put in place adequate arrangements for backup of information and data. Periodic testing of backup systems of the Company shall be conducted at periodic intervals.

16. Policy Review

The implementation of the Policy shall be subject to periodic review at least once every year or such intervals as may be decided by the Board of Directors.

For Udaipur Cotton Mills Company Limited

Jayesh Vora

Director

26 APR 2023