Balrampur
Chini Mills Limited

RISK MANAGEMENT:
FRAMEWORK & POLICY

CONTENTS

1. RISK MANAGEMENT POLICY

1.1 Objective

This policy is to enable the Company to develop a comprehensive focus on various risk management activities of the company and provide the details of the Risk Management Principles and Risk Management Framework. The policy forms part of Balrampur Chini Mills Limited's ("BCML") Internal control & Governance arrangements and shall operate in conjunction with other business and operating / administrative practices. The Policy shall be applicable to all businesses and employees of the Company. The Policy is drafted in accordance with Section 134 of the Companies Act, 2013 and relevant regulations of the SEBI (Listing Obligations and Disclosure Requirements) Regulations, 2015, as amended. The Regulations states as follows:

To formulate a detailed risk management policy which shall include:

(a) A framework for identification of internal and external risks specifically faced by the listed entity, in particular including financial, operational, sectoral, sustainability (particularly, ESG related risks), information, cyber security risks or any other risk as may be determined by the Committee.
(b) Measures for risk mitigation including systems and processes for internal control of identified risks.
(c) Business Continuity Plan.

The specific objectives of the Risk Management Policy are:

- To achieve the strategic objective while ensuring appropriate management of risks;
- To establish a common risk management framework across the company;
- To establish ownership throughout the Organization and integrate risk management in the culture and strategic decision making across all levels of organization;
- To help the decision makers of the organization explicitly take account of uncertainty, the nature of that uncertainty, and work towards a comprehensive solution to address the same;
- To ensure that all the current and potential risk exposures of the organization are identified, qualitatively and quantitatively evaluated, analyzed and appropriately managed;
- To enable compliance with the relevant legal and regulatory requirements and adoption of leading practices.

1.2 Philosophy

The risk management philosophy of the Company is built based on its Vision and strategic goals. Since, risk is an integral part of every business activity, the Company aims to embed risk management in its regular course of business. This ensures that risk management is not seen as a traditional silo-based activity but is practiced by individual functions/business as a part of their day to day operations.

The Company has adopted an integrated approach for risk management wherein it ensures all material risks are identified, assessed, and mitigated for the long-term sustainability of the organization. In addition, the mitigation plans for all the key risks are aligned with the Company's strategic business plans and performance management system which are reviewed by the senior leadership on a periodic basis.

The Company also has well defined polices, standard operating procedures and controls in place to minimize and mitigate the financial and operational risks. The Company's internal auditor carries out reviews and the internal control advisory activities aligned to the key risks and their mitigation plans. This provides an independent assurance to the Audit Committee (AC) of the Company on the adequacy and

effectiveness of the risk management for operational and financial risks. Compliance with the Company's Code of Conduct and Whistle Blower Policy also ensures ethical culture and responsible decision making within the organization.

2. THE RISK MANAGEMENT FRAMEWORK

An effective risk management framework requires consistent processes for assessment, mitigation, monitoring and communication of risk issues across the organization. The risk management framework adopted by BCML is mapped as per the ISO Standard 31000: Risk Management - Principles and guidelines and is in-line with recommendations of The Committee of Sponsoring Organizations of the Treadway Commission ("COSO"). Hence, an enterprise wide and comprehensive view will be taken of risk management to address risks inherent to strategy, operations, finance and compliance and their resulting organizational impact.

An effective Risk Management Framework comprises of:

- Risk management process; and
- Risk management organization structure

i) **Risk management Process** can be defined as the identification, assessment, and prioritization of risks followed by coordinated and economical application of resources to minimize, monitor, and control the probability and/or impact of unfortunate events or to maximize the realization of opportunities.

ii) **Risk Management Organization Structure:** The risk management process has to be supported by a risk management structure which primarily comprises of:
- Team structure of the Risk Management Function
- Roles and Responsibilities
- Risk management activity calendar

This Framework enhances the capability of the company to recognise and face various risks that the company encounters at various levels of strategy and business. This Framework integrates other policies addressing various areas of risk that the company has in place. The Framework explicitly addresses issues in comprehensive management of risk including recognition, classification, measurement, and reporting. The comprehensive understanding of risk profile will allow the company to integrate risk concerns in their strategic and operating decision making process as well as help is computation of capital required to face the risk.

2.1 RISK MANAGEMENT PROCESS

The risk management process adopted by BCML has been tailored to the business processes of the organization. Broadly categorizing, the process consists of the following stages/steps:
Establishing the Context
Risk Assessment (identification, analysis & evaluation)
Risk Treatment (mitigation plan)
Communication and consultation
Monitoring, reviewing and reporting

[Refer figure below for detailed flow of the risk management process]

2.1.1 Establishing the Context

Articulate the objectives and define the external and internal parameters to be taken into account when managing risk and sets the scope and risk criteria for the remaining process.

Establishing the External Context

Understanding the external context is important in order to ensure that the objectives and concerns of external stakeholders are considered when developing risk criteria. It is based on the organization-wide context, but with specific details of legal and regulatory requirements, stakeholder perceptions and other aspects of risks specific to the scope of the risk management process.

The external context can include, but is not limited to:

The social and cultural, political, legal, regulatory, financial, technological, economic, natural and competitive environment, whether international, national, regional or local;

Key drivers and trends having impact on the objectives of the organization; and Relationships with, perceptions and values of external stakeholders

Establishing the Internal Context

The risk management process should be aligned with the organization's culture, processes, structure and strategy. Internal context is anything within the organization that can influence the way risks will be assessed and managed.

It is necessary to understand the internal context. This can include, but is not limited to:

- Governance, organizational structure, roles and accountabilities;
- Policies, objectives, and the strategies that are in place to achieve them;
- Capabilities, understood in terms of resources and knowledge (e.g. capital, time, people,

processes, systems and technologies);

- The relationships with and perceptions and values of internal stakeholders; the organization's culture;
- Information systems, information flows and decision making processes (both formal and informal);
- Standards, guidelines and models adopted by the organization

2.1.2 Risk Assessment

Risk assessment is the overall process of risk identification, risk analysis /estimation and risk evaluation.

2.1.2.1 Risk Identification

Risk identification will be an exercise to identify exposure of the company to uncertainty. This will involve understanding of the market in which it operate, legal, social, political, and cultural environment around it, strategic and operational objectives, including factors critical to its success, and threats and opportunities related to achievement of these objectives.

Risk identification will ensure that all significant activities within the company have been identified and all risks flowing from these activities defined. Volatility related to these activities will be identified and categorised.

Business activities and decisions will be classified to ensure grouping of homogenous focus groups. The classification groups will include:

Strategic: These concern long-term strategic objectives of the company and will be affected by issues like capital availability, sovereign and political risks, legal and regulatory changes, reputation and changes in the physical environment, etc.

Operational: These concern day-today issues confronting the company as it strives to deliver its strategic objectives.

Financial: These concern effective management and control of finances of the company and effects of external factors like availability of credit, foreign exchange rates, interest rate movement, and other market exposures.

Knowledge Management: These concern effective management and control of knowledge resources, services delivery, information protection, and communication thereof. External factors having an impact on this classification would include unauthorised use or abuse of intellectual property, failure of logistics, emergence of competitive technology, loss of key person, etc.

Compliance: These concern issues including regulatory, data protection, environmental, trade, consumer protection, employment practices, etc.

Risk Register

Risk identification will be a continuous in-house activity with well communicated, consistent, and co-ordinated processes and tools leading to in-house ‘ownership’ of the risk management process is essential. All risks identified will be reported in a structured format and maintained in a risk register.

(Please refer the appendix)

2.1.2.2 Risk Analysis/ Estimation

i. The company recognises that risk estimation can be quantitative, semi-quantitative, or qualitative and will be essentially driven in terms of probability of occurrence and possible consequence.

ii. The company will adopt to various measures for covering the dual aspects of risk estimation and will granulate, at the minimum, at a gradation of five, as described herein below:

a) Impact/ Consequences will be estimated Negligible, Minor, Moderate, Major and Severe.
b) Likelihood/ Probability will also be estimated as Rare, Not Likely, Likely, Highly Likely and Expected.

iii. Factors that affect consequences and likelihood should be identified. Risk is analyzed by determining consequences and their likelihood, and other attributes of the risk. An event can have multiple consequences and can affect multiple objectives. Existing controls and their effectiveness and efficiency should also be taken into account **(*Please refer to the Appendix for Impact and Likelihood definition*)**

2.1.2.3 Risk Evaluation

The purpose of risk evaluation is to assist in making decisions, based on the outcomes of risk estimation, about which risks need treatment and the priority for treatment implementation. Risk evaluation involves comparing the level of risk found during the analysis process with risk criteria established when the context was considered. Based on this comparison, the need for treatment can be considered.

Decisions should take account of the wider context of the risk and include consideration of the tolerance of the risks borne by parties, other than the organization, that benefit from the risk. Decisions should be made in accordance with legal, regulatory and other requirements.

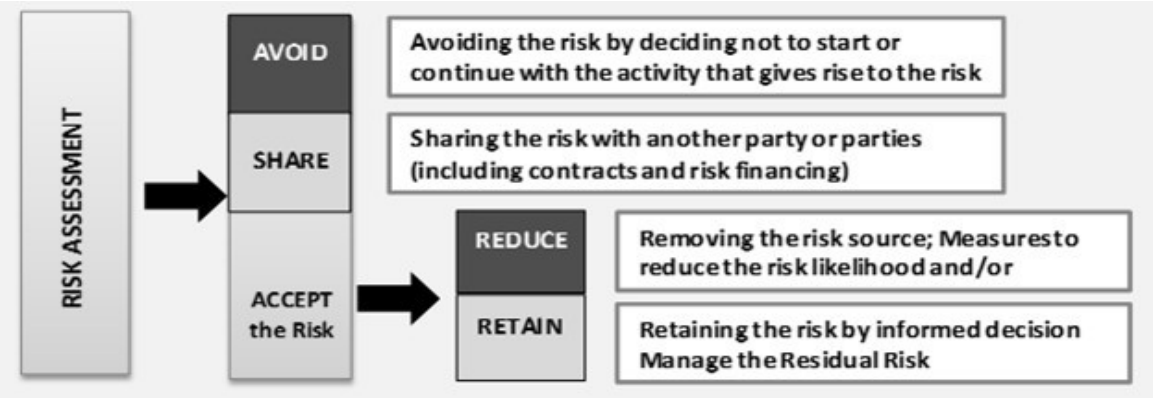
2.1.2.4 Risk Treatment

Risk treatment involves selecting one or more options for modifying risks, and implementing those options. Once implemented, treatments provide or modify the controls.

Risk treatment involves a cyclical process of:

- Assessing a risk treatment;
- Deciding whether residual risk levels are *tolerable;*
- If not tolerable, generating a new risk treatment; and
- Assessing the effectiveness of that treatment.

Based on the Risk level, the company should formulate its Risk Management Strategy. The strategy will broadly entail choosing among the various options for risk mitigation for each identified risk. Risk treatment options are not necessarily mutually exclusive or appropriate in all circumstances. Following framework shall be used for risk treatment:



1. **Avoidance (eliminate, withdraw from or not become involved)**

As the name suggests, risk avoidance implies not to start or continue with the activity that gives rise to the risk.

2. **Reduction (optimize - mitigate)**

Risk reduction or "optimization" involves reducing the severity of the loss or the likelihood of the loss from occurring. Acknowledging that risks can be positive or negative, optimizing risks means finding a balance between negative risk and the benefit of the operation or activity; and between risk reduction and effort applied.

3. **Sharing (transfer - outsource or insure)**

Sharing, with another party, the burden of loss or the benefit of gain, from a risk

4. **Retention (accept and budget)**

Involves accepting the loss, or benefit of gain, from a risk when it occurs. Risk retention is a viable strategy for risks where the cost of insuring against the risk would be greater over time than the total losses sustained. All risks that are not avoided or transferred are retained by default. This includes risks that are so large or catastrophic that they either cannot be insured against or the premiums would be infeasible. This may also be acceptable if the chance of a very large loss is small or if the cost to insure for greater coverage amounts is so great it would hinder the goals of the organization too much.

2.1.3 Communication and consultation

Communication and consultation with external and internal stakeholders should take place during all stages of the risk management process. Therefore, plans for communication and consultation should be developed at an early stage. These should address issues relating to the risk itself, its causes, its consequences (if known), and the measures being taken to treat it. Effective external and internal communication and consultation should take place to ensure that those accountable for implementing the risk management process and stakeholders understand the basis on which decisions are made, and the reasons why particular actions are required.

2.1.4 Monitoring & Review

In order to ensure that risk management is effective and continues to support organizational performance, processes shall be established to:

- Measure risk management performance against the key risk indicators, which are periodically reviewed for appropriateness

- Periodically measure progress against, and deviation from, the risk management plan
- Periodically review whether the risk management framework, policy and plan are still appropriate, given the organizations' external and internal context
- Report on risk, progress with the risk management plan and how well the risk management policy is being followed
- Periodically review the effectiveness of the risk management framework.
- Structured scientific and analytical tools may be used for this purpose

2.1.4.1 Risk Reporting

Reporting is an integral part of any process and critical from a monitoring perspective. Results of risk assessment need to be reported to all relevant stake holders for review, inputs and monitoring.

Approach for Implementation at BCML:

The **Risk Unit Owners** shall prepare unit level risk evaluation reports on a half-yearly basis and submit the same to Corporate Level Steering Committee.

The Risk Unit Owners shall review the Risk Registers and identify any emerging/new risk and the existing control to mitigate that risk. They must ensure robustness of design and operating effectiveness of existing mitigating controls. If required, re–rate (existing risks)/rate (emerging risks) and prepare, implement action plan for risk treatment in situations where the existing controls are inadequate.

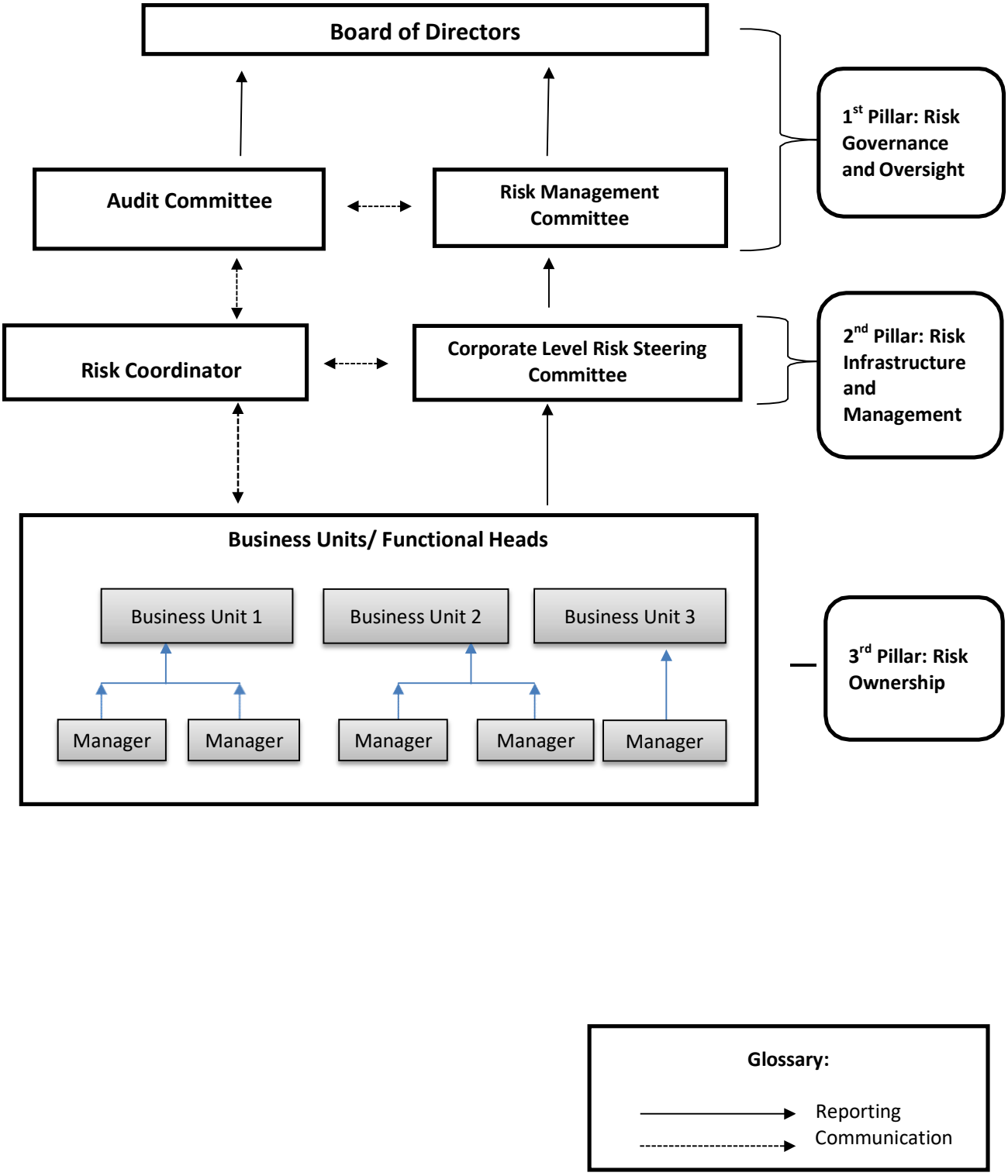
The Risk Co-ordinator would be required to prepare on a half-yearly basis a report for the Corporate Level Risk Steering Committee detailing the following:

- List of applicable risks for the business, highlighting the new risks identified, if any and the action taken w.r.t the existing and new risks;
- Prioritized list of risks highlighting the Key strategic and operational risks facing BCML
- Root causes and mitigation plans for the Key Risk
- Status of effectiveness of implementation of mitigation plans for the Key Risks identified till date.

The Corporate Level Risk Steering Committee would be required to submit report to the Risk Management Committee on a half-yearly basis consisting of the following:

- An overview of the risk management process in place.
- Key observations on the status of risk management activities in the period, including any new risks identified and action taken w.r.t these risks.
- Status of effectiveness of implementation of the mitigation plan for key risk.

2.2 RISK MANAGEMENT ORGANIZATION STRUCTURE (GOVERNANCE STRUCTURE)



2.2.1 Roles and Responsibilities

a) Board of Directors

The Board shall oversee the establishment and implementation of an adequate system of risk management across the Company by defining the risk management policy and reviewing the risk governance and monitoring mechanism. The Board shall meet at least once in a year to review the top risks faced by the Company and the status of their mitigation plan. It will also review the Risk Management Policy at least once in two years.

b) Risk Management Committee ("RMC")

Risk Management Committee (RMC) shall assist the Board in framing policy, guiding implementation, monitoring, and reviewing the effectiveness of risk management policy and practices. The Committee shall act as a forum to discuss and manage key strategic and business risks.

The Committee chaired by an Independent Director, shall meet Half-yearly to review the risk strategy and ensure that proper risk management principles are embedded into all processes and activities of the Company. Accordingly, the Corporate Level Risk Steering Committee (CLRSC) shall table its report before the Risk Management Committee for its review and consideration. The Risk Management Committee may, after due consideration of the report submitted by CLRSC, communicate such risks to the Audit Committee which it feels the same requires further deliberations by the Audit Committee.

c) Audit Committee ("AC")

Audit Committee shall carry out periodic evaluation of risk management program and provide insight to the risk management committee. The Audit Committee shall exercise direct oversight over the Financial Risks faced by the Company on the basis of the Internal Financial Controls and Internal Audit mechanisms put in place by the Company. If any risk (whether financial or non-financial) is highlighted/ escalated by the Risk Management Committee then the Audit Committee shall duly consider the same and provide necessary guidance.

Since the Audit Committee reviews the Internal Audit Reports on a quarterly basis, the Audit Committee may highlight such risk to the Risk Management Committee if it feels that the same requires further deliberation by the Risk Management Committee.

Accordingly, there would be co-ordination between the Audit and the Risk Management Committee in discharging the Risk Management obligations.

d) Corporate Level Risk Steering Committee ("CLRSC")

The Corporate Level Risk Steering Committee (CLRSC) shall consist of the senior management team who shall be accountable to design and implement risk management processes within the organization.

The primary responsibility of the CLRSC shall be implementing the Risk Management Policy within the Company and developing a risk intelligent culture that helps improve organization resilience to critical business risks. They would support in identifying high priority risk, defining the right mitigation strategies and review the status of its mitigation plan on periodic basis.

e) Risk Coordinator

Mr.Manoj Agarwal, Company Secretary & Compliance Officer of the Company shall act as the Risk Coordinator. The risk coordinator shall ensure risk management processes as defined in this policy are executed and coordinate the effort of various functionsin this regard. The risk coordinator would also be responsible for conducting internal risk review meetings, maintaining risk registers and risk management policy, and suggesting best practices for strengthening the risk management process.

2.2.2 Risk Ownership:

The final ownership of risk identification, monitoring and mitigation shall rest with the respective Business Unit Heads/ Functional heads. The Business Unit Heads of various units shall accept the risk of their respective areas and own the risk management plan of their unit.

The Risk owner shall drive and monitor the progress of risk mitigation strategies. The risk owner may further delegate the mitigation strategies and action plans down the hierarchy to ensure ground level implementation of the mitigation action plans. The risk owner shall also be responsible for reporting the status of mitigation plan to the Risk Coordinator. For cross-unit risk, a cross-unit team with clear demarcated roles and responsibilities shall be formed to drive implementation of mitigation action plans and review risk status periodically. Thus, the Company's Risk Management framework is well integrated with the business operations and key executives play vital role in its implementation, upholding its integrity.

2.2.3 Risk Management Activity Calendar

Forum	Timelines*
Board of Directors	**Annually**
Risk Management Committee	**Half Yearly**
Corporate Level Risk Steering Committee	**Half Yearly**
Business Unit Heads/ Functional Heads	**Half-yearly**

*****Additionally, on the happening of any trigger event*

Note:

The Audit Committee reviews the Internal Audit Report on a quarterly basis and therefore it may highlight any risk (whether financial or non-financial) it deems necessary to the Risk Management Committee for its consideration and review.

3. BUSINESS CONTINUITY PLAN

Business Continuity Plans (BCP) are required to be defined for risks corresponding to High Impact and High Velocity to enable rapid response to address the consequence of such risks when they materialize. Business Continuity Planning shall be embedded in the Internal Controls and Crisis Management framework for areas like manufacturing units, sales offices, information technology function, etc. The internal crisis management team shall be responsible for laying out crisis response mechanism, communication protocols, and periodic training and competency building on crisis management.

4. REVISION OF POLICY

Risks are ever changing in this volatile business environment and hence there is a need to periodically revisit the approach towards Risk management. Therefore, this policy shall be reviewed at least once in two years. Any revision to the policy shall be incorporated with the approval of Risk Management Committee and Board of Directors.

5. LIMITATIONS AND AMENDMENT(S)

In the event of any conflict between the provisions of this Policy and that of the Companies Act, 2013 and relevant regulations of the SEBI (Listing Obligations and Disclosure Requirements) Regulations, 2015 ("Applicable Law"), the provisions of Applicable Law(s) shall prevail over this Policy.

By order of the Board
Sd/-
Company Secretary
Balrampur Chini Mills Limited

Place: Kolkata
Date of Approval: 2nd February, 2022
Date of Revision: 9th November, 2022
: 17th May, 2024