DAIN COLOUR CHEM LIMITED

RISK MANAGEMENT POLICY

Under Regulation 17(9)(b) of the Securities and Exchange Board of India (Listing Obligations and Disclosure Requirements) Regulations, 2015

CIN: U15130GJ2023PLC138560

Registered Office: Plot No.5, Neelkanth Industrial Estate, B/H Gayatri Dairy, Vill-Dhanot, Gandhinagar- 382729, Gujarat, India

RISK MANAGEMENT POLICY

1. Introduction

The Companies Act, 2013 emphasizes the requirement of risk management policy for the Company. Section 134(3)(n) of the Companies Act, 2013 requires that the report by the Board laid at the general meeting shall include a statement on the development and implementation of a risk management policy for the company including identification therein of elements of risk, if any, which in the opinion of the Board may threaten the existence of the Company shall be included in the Board's report.

The audit committee is required to evaluate the internal financial controls and risk management systems of the Company and the Independent Directors shall satisfy themselves that the systems of risk management are robust and defensible. Section 177(4)(vii) of the Companies Act, 2013 provides that audit committee shall evaluate the internal financial controls and risk management systems of the company.

Regulation 17(9)(a) of SEBI (Listing Obligation and Disclosure Requirements) Regulations, 2015 (**"Listing Regulations"**), inter alia, mandates laying down the procedures for risk assessment and minimization. Further Regulation 17(9)(b) of the Listing Regulations, provides the Board shall be responsible for framing, implementing and monitoring the risk management plan for the company.

Regulations 21(4) further provides that the Board shall define the role and responsibility of the Risk Management Committee and may delegate monitoring and reviewing of the risk management plan to the committee and such other functions as it may deem fit. Such function shall specifically cover cyber security. It further states that role and responsibilities of the Risk Management Committee shall mandatorily include the performance of functions specified in Part D of Schedule II. **(Annexure 1)**

The board of directors (**"the Board"**) of Dain Colour Chem Limited (**"the Company"**) has adopted the following policy and the Board may amend this policy from time to time. In case of any subsequent amendments to the Listing Regulations which makes any of the provisions in the Policy inconsistent, the provisions of the Listing Regulations shall prevail.

2. Objective Of Policy

The objective of this policy includes the following:

- Develop a risk culture that encourages all employees to identify risks, associated opportunities/gains and respond to them with effective actions
- Develop both proactive and reactive mechanism for risk management
- Identify and manage existing/new risks in a planned and coordinated manner by risk register and risk control matrix
- Develop an incident response management framework to manage the risks that may materialize.

3. Definitions

i. **"Company"** means Dain Colour Chem Limited.

ii. **"Risk"** means a probability or threat of damage, injury, liability, loss, or any other negative occurrence that may be caused by internal or external vulnerabilities; that may or may not be avoidable by pre-emptive action.

iii. **"Risk Management"** is the process of systematically identifying, quantifying, and managing all risks and opportunities that can affect achievement of a corporation's strategic and financial goals.

iv. "**Senior Management**" means officers/personnel of the Company who are members of its core management team comprising all members of management one level below the chief executive director or managing director or whole-time director or manager, including the functional heads and shall specifically include company secretary and chief financial officer.

v. **"Risk Management Committee**" means the Committee formed by the Board as under Regulation 21 of the Listing Regulations.

Words and expressions used and not defined in this Policy shall have the meaning ascribed to them in

the Listing Regulations, the Securities and Exchange Board of India Act, 1992, as amended, the Securities Contracts (Regulation) Act, 1956, as amended, the Depositories Act, 1996, as amended, or the Companies Act and rules and regulations made thereunder.

4. **Risk Management Policy & Framework**

Risk is the potential for failure or loss of value or the missed opportunity for value creation / strategic competitive advantage resulting from either a certain action or a certain inaction.

Controlling risk is essential in any business by having processes to ensure safeguarding of assets and compliance with appropriate regulatory frameworks. However, risks may also have to be taken consciously to explore untapped business opportunities in line with the corporate strategy to optimize maximum potential stakeholder's value and to improve their confidence.

Classification of Risks:

A. Financial / Operational / Preventable / Compliance risks:

These are internal risks, arising from within the organization that are controllable and need to be eliminated or avoided. The examples are:

- Governance, organizational structure, roles and accountabilities;
- Policies, objectives and the strategies that are in place to achieve them;
- Contractual compliances;
- Operational efficiency;
- Credit and liquidity risk;
- Human resource management;
- Hurdles in optimum use of resources;
- Culture and values;
- Suppliers/raw material risk;
- Customers risk;
- Technological risk;
- Physical risk – that is risk of damage/breakdown to the assets of the company.

B. External risks

External risks come up due to economic events that arise from outside of an institution's control. It arises from the external events that cannot be controlled by any an institution, cannot be forecasted with reliability, are normally beyond its control, and it is therefore difficult to reduce the associated risks. The examples are :

- Statutory/ regulatory changes/ changes in government policies;
- Market conditions/ trends;
- Economic environment;
- Political Environment;
- Fluctuations in trading activities;
- Foreign exchange rate risk;
- Factors beyond the company's control (including act of God, epidemic, pandemic, war, etc) which significantly reduces demand for its business and/or affects its operations.

C. Disruptive risks:

These are the anticipated or unanticipated events which may result in disruption of the operations of the Company or existence of its current business model and innovations to business models that disrupt the existing paradigm – e.g. changes in food safety regulations, restrictions on use of synthetic food colours, shift in consumer preference towards natural and organic ingredients, volatility in raw material prices, supply chain disruptions, technological advancements in food colouring alternatives, entry of new competitors, product contamination or quality-related issues, changes in environmental laws, and fluctuations in demand from food and beverage industries.

D. Strategic Risks:

Risks taken on consciously linked to strategic choices to earn a higher return.

The aggregate level and types of risk the Company is willing to assume within its risk capacity to achieve its strategic objectives and business plan shall be as per its risk appetite. The risk management process involves the following phases:

- Risk identification
- Risk evaluation and assessment
- Risk mitigation

4.1 Risk Identification

This involves continuous identification of events that may have a negative impact on the company's ability to achieve goals. The company has adopted a robust risk identification process keeping in view the key activities/ focused areas of company's business for the purpose of risk assessment. Identification of risks, risk events and their relationship are based on the basis of discussion with the senior management and analysis of related data/ reports, previous internal audit reports, past occurrences of such events etc. The identification of risk by the company is broadly based on the following internal and external risk factors:

The risks can be broadly identified/ categorized into one or more following categories; however, the risk management committee may revise such categories:

Sr. No.	Risk Category	Risk Identification
1	Regulatory & Compliance Risk	Risk of non-compliance with FSSAI regulations, pollution control norms, environmental laws, labour laws, factory regulations and other statutory requirements.
2	Product Quality & Safety Risk	Risk relating to contamination, adulteration, improper formulation, product defects, quality failures, product recalls or adverse impact on consumer health.
3	Raw Material Risk	Risk arising from shortage, non-availability, price fluctuation or poor quality of raw materials, chemicals and packaging materials.
4	Supply Chain & Logistics Risk	Risk of transportation delays, supply disruptions, vendor dependency, import/export restrictions and interruption in distribution channels.
5	Operational Risk	Risk due to machinery breakdown, fire, chemical leakage, industrial accidents, utility failures or disruption in manufacturing processes.
6	Environmental Risk	Risk arising from hazardous waste disposal, pollution, chemical handling, emissions and non-compliance with environmental standards.
7	Market & Competition Risk	Risk due to intense competition, pricing pressure, entry of new competitors, changing customer preferences and shift towards natural food colours.
8	Financial Risk	Risk relating to liquidity issues, increase in operational costs, bad debts, foreign exchange fluctuation, inflation and interest rate changes.

Sr. No.	Risk Category	Risk Identification
9	Technology & Cyber Security Risk	Risk of cyber-attacks, data breaches, IT system failures, unauthorized access and disruption of digital operations.
10	Human Resource Risk	Risk arising from shortage of skilled manpower, employee attrition, labour disputes, misconduct or workplace safety issues.
11	Reputation Risk	Risk arising from customer complaints, adverse media coverage, regulatory action, product failure or negative publicity affecting the Company's goodwill.
12	Strategic Risk	Risk arising from failure of business strategies, inability to adapt to industry changes, technological advancements or changing market conditions.
13	Business Continuity Risk	Risk due to natural disasters, pandemics, political instability, strikes or unforeseen events causing disruption in business operations.
14	Customer & Credit Risk	Risk relating to dependence on major customers, delayed payments, customer defaults or loss of key accounts.
15	Health & Safety Risk	Risk relating to employee exposure to chemicals, workplace accidents, unsafe working conditions and non-compliance with occupational safety standards.

4.2 Risk Analysis

Risk analysis involves:

- consideration of the causes and sources of risk;
- the trigger events that would lead to the occurrence of the risks;
- the positive and negative consequences of the risk;
- the likelihood that those consequences can occur.

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.

4.3 Risk Assessment

Management considers qualitative and quantitative methods to evaluate the likelihood and impact of identified risk elements. Likelihood of occurrence of a risk element within a finite time is scored based on polled opinion or from analysis of event logs drawn from the past. Impact is measured based on a risk element's potential impact on revenue, profit, balance sheet, reputation, business and system availability etc. should the risk element materialize. The composite score of impact and likelihood are tabulated in an orderly fashion. The Company has assigned quantifiable values to each risk element based on the "impact" and "likelihood" of the occurrence of the risk on a scale of 1 to 4 as follows.

Impact	Risk Level	Likelihood
Minor	1	Low
Moderate	2	Medium

High	3	High
Critical	4	Critical

4.4 Risk Mitigation

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. ***Risk Avoidance (eliminate, withdraw from or not become involved)***
   Risk avoidance implies not to start or continue with the activity that gives rise to the risk.

2. ***Risk 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. ***Risk Sharing (transfer - outsource or insure)***
   Sharing, with another party, the burden of loss or the benefit of gain, from a risk.

4. ***Risk 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.

4.5 Risk Reporting

Periodically, key risks are reported to the Board or Risk Management Committee with causes and mitigation actions undertaken/ proposed to be undertaken.

The internal auditor carries out reviews of the various systems of the Company using a risk-based audit methodology. The internal auditor is charged with the responsibility for completing the agreed program of independent reviews of the major risk areas and is responsible to the audit committee which reviews the report of the internal auditors on a quarterly basis.

The statutory auditors carry out reviews of the Company's internal control systems to obtain reasonable assurance to state whether an adequate internal financial controls system was maintained and whether such internal financial controls system operated effectively in the company in all material respects with respect to financial reporting.

The Management shall periodically review the risk status and effectiveness of mitigation measures and place the same before the Board of Directors.

The Board shall include a statement indicating development and implementation of a risk management policy for the Company including identification of elements of risk, if any, which in the opinion of the Board may threaten the existence of the Company.

5. **Risk Management Tools**

The Company shall adopt appropriate risk management tools, systems and practices to identify, assess, monitor and mitigate risks associated with its business operations.

The key risk management tools used by the Company may include the following:

- Risk Assessment Matrix:
  Evaluation of risks based on likelihood, severity and impact on the Company's operations, financial position and reputation.

- Internal Control Systems:
  Establishment of internal controls, standard operating procedures (SOPs) and authorization mechanisms to minimize operational and financial risks.

- Compliance Monitoring System:
  Periodic monitoring of compliance with applicable laws, regulations, licenses and statutory requirements including FSSAI, environmental and factory regulations.

- Quality Control and Testing Procedures:
  Regular testing and inspection of raw materials, packaging materials and finished products to ensure product quality and safety standards.

- Internal and External Audits:
  Conducting periodic audits to identify process gaps, compliance failures and operational weaknesses and to recommend corrective actions.

- Vendor and Supplier Evaluation:
  Assessment and monitoring of suppliers and vendors based on quality standards, reliability, delivery performance and regulatory compliance.

- Business Continuity and Disaster Recovery Planning:
  Systems and procedures to ensure continuity of operations during emergencies, natural disasters, fire, pandemics or other unforeseen events.

- Insurance Coverage:
  Adequate insurance policies for protection against risks relating to fire, machinery breakdown, product liability, employee safety, stock and other operational risks.

- Cyber Security Measures:
  Use of secure IT infrastructure, access controls, data backup systems, antivirus software and cyber security protocols to protect business information and systems.

- Health, Safety and Environmental (HSE) Measures:
  Safety audits, employee training, emergency response procedures and environmental monitoring systems to reduce workplace and environmental risks.

- Periodic Management Review:
  Regular review of key risks and mitigation measures by senior management and the Board of Directors.

6. **Review Of This Policy**

This Policy shall be reviewed by the Board of Directors periodically, at least once in two years, including by considering the changing industry dynamics and evolving complexity.

7. **Business Continuity Plan**

Business continuity plan refers to maintaining business functions or quickly resuming them in the event of a major disruption, in other words, a disaster management plan. The Company shall formulate a business continuity plan as may be required for protecting the interest of the Company in the event of happening/

occurrence of any unforeseen events that may affect the business of the Company.

Such business continuity plan may vary from time to time depending on Company's need and the risk management strategy being adopted by the company at such time. The business continuity plan may, among other things, focus on protecting the assets and personnel of the Company in the event of a disaster event which affects day to day operations of the company's business. The business continuity plan may be reviewed and amended by the Risk Management Committee from time to time, as the committee may deem fit.

Effective Date: 13th April, 2026