Krystal Integrated Services Limited

(Previously known as Krystal Integrated Services Private Limited)

Risk Management Policy

SUMMARY OF POLICY / CODE	
Owner / Created by	Secretarial Team
Adherence by	Board of Directors
Version	1.4
Effective Date	September 15, 2023
Last Review Date	July 31, 2025
Review Frequency	AN - Annually OT – Other i.e upon regulatory change
Related Regulations	Securities and Exchange Board of India (Listing Obligations and Disclosure Requirements) Regulations, 2015
Next Review Date	August 2027/as and when required due to change in regulations and/or applicable laws. Any subsequent amendment / modification in the Securities and Exchange Board of India (Listing Obligations and Disclosure Requirements) Regulations, 2015 and/or applicable laws in this regard shall automatically apply to this Policy.
Reviewed by	Risk Management Committee (RMC)
Approved by	Board of Directors
Approval Date	August 04, 2026
Confidentiality level	Board/RMC Document

Change History				
Version	**Effective Date**	**Created by**	**Approved by**	**Description of change**
1.1	September 15, 2023	Secretarial Team	Board of Directors	Initial Policy
1.2	August 12, 2024	Secretarial Team	Board of Directors	Annual review and no changes were required.
1.3	July 31, 2025	Secretarial Team	Board of Directors	Annual review and no changes were required.

Change History				
Version	**Effective Date**	**Created by**	**Approved by**	**Description of change**
1.4	August 04, 2026	Secretarial Team	Board of Directors	Annual review; to align policy with Company's risk governance framework applicable provisions of SEBI (Listing Obligations and Disclosure Requirements) Regulations, 2015.

KRYSTAL INTEGRATED SERVICES LIMITED

RISK MANAGEMENT POLICY

1. Introduction

Krystal Integrated Services Limited ("**the Company**") recognizes that effective risk management is an integral part of good corporate governance and a key driver for achieving sustainable growth, operational excellence, and long-term value creation. The Company operates in a dynamic business environment that presents various strategic, operational, financial, legal, regulatory, technological, environmental, and reputational risks.

This Risk Management Policy ("**Policy**") establishes a structured and enterprise-wide approach for identifying, assessing, evaluating, mitigating, monitoring, and reporting risks that may affect the Company's ability to achieve its strategic and business objectives.

The Policy seeks to embed risk management into the Company's decision-making processes, business planning, and day-to-day operations while fostering a proactive risk-aware culture across all levels of the organization.

For the purpose of this Policy, references to the Company shall include Krystal Integrated Services Limited and its subsidiaries, unless the context otherwise requires.

2. Regulatory Framework

This Policy has been formulated in accordance with the applicable provisions of:

- the Companies Act, 2013 and the rules framed thereunder;
- the SEBI (Listing Obligations and Disclosure Requirements) Regulations, 2015 ("SEBI Listing Regulations"), as amended from time to time;
- the Securities and Exchange Board of India ("SEBI") circulars and guidelines relating to risk management and corporate governance, as applicable;
- Secretarial Standards issued by the Institute of Company Secretaries of India ("ICSI"), wherever applicable; and
- Such other applicable laws, regulations, and statutory requirements governing risk management.

The Company shall review and update this Policy from time to time to ensure continued compliance with applicable laws, regulations, and evolving business requirements.

3. Objectives

The objectives of this Policy are to:

- establish a comprehensive Enterprise Risk Management ("ERM") framework across the Company;
- identify, assess, evaluate, monitor, and manage risks that may affect the achievement of the Company's strategic and operational objectives;
- promote a proactive and consistent approach towards risk management throughout the organization;

- integrate risk management into strategic planning, business operations, investment decisions, and resource allocation;
- define clear roles, responsibilities, and accountability for risk management across all levels of the organization;
- strengthen internal controls and governance mechanisms for effective risk oversight;
- safeguard the interests of shareholders, customers, employees, business partners, and other stakeholders;
- ensure compliance with applicable legal, regulatory, and contractual obligations;
- enhance business resilience through effective contingency planning and crisis management; and
- Support sustainable business growth while protecting the Company's assets, reputation, and long-term value.

4. Scope and Applicability

This Policy shall apply to:

- Krystal Integrated Services Limited;
- all subsidiaries of the Company, to the extent permitted under applicable laws;
- all business units, functions, departments, locations, projects, and operations of the Company;
- All directors, senior management personnel, employees, and persons entrusted with risk management responsibilities.

The Policy shall cover all categories of risks that could materially affect the Company's strategic objectives, financial performance, operational efficiency, legal and regulatory compliance, business continuity, information security, environmental and social responsibilities, and corporate reputation.

The principles set out in this Policy shall be integrated into the Company's business processes, decision-making framework, strategic initiatives, and operational activities.

5. Definitions

Unless the context otherwise requires, the following terms shall have the meanings assigned below:

Board means the Board of Directors of Krystal Integrated Services Limited.

Committee means the Risk Management Committee constituted by the Board in accordance with applicable laws and regulations.

Enterprise Risk Management (ERM) means a structured and integrated process adopted by the Company to identify, assess, evaluate, mitigate, monitor, and report risks across the organization.

Risk means the possibility of an event or circumstance occurring that could have a positive or negative impact on the achievement of the Company's objectives.

Risk Appetite means the nature and extent of risk that the Company is willing to accept in pursuit of its strategic and business objectives.

Risk Tolerance means the acceptable level of variation from the Company's defined risk appetite.

Risk Owner means the individual or function responsible for identifying, managing, monitoring, and reporting a specific risk.

Senior Management shall have the meaning assigned under the applicable provisions of the SEBI Listing Regulations.

Words and expressions used but not defined in this Policy shall have the meanings assigned to them under the Companies Act, 2013, the SEBI Listing Regulations, or any other applicable law, as amended from time to time.

6. Risk Governance Framework

The Company shall establish an Enterprise Risk Management ("ERM") framework to ensure that risks are effectively identified, assessed, managed, monitored, and reported across the organization. Risk management shall be integrated into the Company's strategic planning, operational processes, financial management, internal control systems, and decision-making framework.

The governance framework shall operate on the principle that risk management is a shared responsibility across all levels of the organization. While the Board provides strategic oversight, the Risk Management Committee, Audit Committee, Senior Management, and Functional Heads shall collectively ensure effective implementation of this Policy.

i. Board of Directors

The Board shall have the overall responsibility for overseeing the Company's risk management framework and shall, inter alia:

- approve and periodically review the Risk Management Policy;
- oversee the implementation of an effective Enterprise Risk Management framework;
- determine the Company's overall risk appetite and risk tolerance, wherever considered appropriate;
- review significant strategic, financial, operational, compliance, cybersecurity, ESG, and reputational risks facing the Company;
- ensure that adequate systems of internal control and risk management are established and remain effective;
- periodically review reports submitted by the Risk Management Committee and the Audit Committee;
- satisfy itself that appropriate resources, processes, and controls are available to manage material risks;
- ensure that risk management forms an integral part of the Company's strategic and business planning processes; and
- Ensure compliance with applicable legal and regulatory requirements relating to risk management.

ii. Risk Management Committee

The Risk Management Committee ("RMC") shall be constituted by the Board in accordance with applicable provisions of the Companies Act, 2013 and the SEBI (Listing Obligations and Disclosure Requirements) Regulations, 2015, wherever applicable.

The Committee shall, among other things:

- assist the Board in overseeing the Company's Enterprise Risk Management framework;
- review the adequacy and effectiveness of the risk management systems and processes;
- identify emerging risks and recommend appropriate mitigation strategies;
- review the Company's risk profile and key risk indicators on a periodic basis;
- monitor implementation of risk mitigation plans across business functions;
- review business continuity and crisis management preparedness;
- review significant cybersecurity, information security, ESG, and sustainability-related risks;
- escalate material risks to the Board together with appropriate recommendations; and
- Perform such other functions as may be delegated by the Board from time to time.

iii. Audit Committee

The Audit Committee shall support the Board in ensuring the adequacy of internal financial controls and risk management systems.

The Committee shall:

- review the effectiveness of internal control systems;
- consider internal audit findings relating to risk management;
- monitor financial reporting risks and compliance risks;
- review observations of statutory auditors and internal auditors having risk implications;
- oversee fraud risk management and whistle-blower-related matters; and
- Coordinate with the Risk Management Committee wherever matters overlap.

iv. Managing Director & Senior Management

The Managing Director and Senior Management shall be responsible for implementing the risk management framework approved by the Board.

Their responsibilities shall include:

- promoting a strong risk management culture across the organization;
- ensuring that risks are identified, assessed, and managed in all business functions;
- allocating adequate resources for risk management activities;
- ensuring implementation of approved mitigation plans;
- monitoring key risks and reporting material developments to the Risk Management Committee and the Board;
- ensuring compliance with applicable laws, regulations, and internal policies;
- reviewing emerging risks arising from business expansion, technology, market conditions, and regulatory changes; and
- Ensuring effective business continuity and crisis response arrangements.

v. Functional Heads / Risk Owners

Each Functional Head shall act as the Risk Owner for risks relating to their respective functions.

Risk Owners shall be responsible for:

- identifying risks within their respective business areas;
- maintaining departmental risk registers;
- assessing the likelihood and potential impact of identified risks;
- implementing approved mitigation measures;
- continuously monitoring changes in the risk environment;
- reporting significant risks and incidents to Senior Management;
- ensuring compliance with internal controls and policies; and
- Periodically reviewing the effectiveness of mitigation measures.

7. Risk Management Framework

The Company shall adopt an Enterprise Risk Management framework based on a continuous and structured process consisting of:

- establishing the business context;
- identifying risks;
- assessing risks;
- evaluating and prioritising risks;
- implementing mitigation measures;
- monitoring residual risks;
- reporting significant risks to the appropriate governance bodies; and
- Periodically reviewing and improving the effectiveness of the framework.

Risk management shall form part of strategic planning, budgeting, project evaluation, operational decision-making, investments, mergers and acquisitions, procurement, and other significant business activities.

The Company shall maintain appropriate documentation, including risk registers, mitigation plans, action trackers, and periodic risk reports.

8. Risk Identification

Risk identification shall be a continuous process undertaken across all business functions.

Risks may be identified through:

- strategic planning exercises;
- management reviews;
- operational performance reviews;
- internal and external audits;
- regulatory inspections;
- customer and stakeholder feedback;
- incident reporting;
- business continuity assessments;

- technology and cybersecurity assessments;
- market intelligence;
- industry developments; and
- Environmental, social, and governance (ESG) assessments.

Risk identification shall consider both internal and external factors that may affect the achievement of business objectives.

Emerging risks, including technological disruptions, geopolitical developments, climate-related risks, changes in legislation, supply chain disruptions, and evolving customer expectations, shall also be periodically evaluated.

9. Risk Assessment

Each identified risk shall be assessed to determine its significance and potential impact on the Company.

The assessment shall normally consider:

- likelihood of occurrence;
- financial impact;
- operational impact;
- legal and regulatory implications;
- health, safety, and environmental consequences;
- impact on customers and stakeholders;
- reputational impact; and
- Effectiveness of existing controls.

The Company may adopt qualitative, quantitative, or hybrid assessment methodologies depending upon the nature and complexity of the risk.

Risk assessments shall be reviewed periodically or whenever there are significant changes in the Company's business environment.

10. Risk Evaluation and Prioritisation

Following assessment, risks shall be evaluated and prioritised to determine the appropriate management response.

Risks may be categorised as High, Medium, or Low based on their likelihood and impact.

The Company may use a Risk Matrix to evaluate inherent risk, existing controls, and residual risk.

The treatment strategy for identified risks may include one or more of the following:

- avoidance of the risk;
- reduction or mitigation through appropriate controls;
- transfer of risk through contractual arrangements or insurance;
- acceptance of the risk within approved risk appetite and tolerance levels; or

- Continuous monitoring where the residual risk is considered acceptable.

Priority shall be given to risks that have the potential to significantly affect the Company's strategic objectives, financial position, operations, legal compliance, reputation, employees, customers, or other stakeholders.

The Risk Management Committee shall periodically review the Company's risk profile to ensure that significant risks are appropriately prioritised and managed.

11. Risk Mitigation

The Company shall implement appropriate risk mitigation measures to reduce the likelihood and/or impact of identified risks to an acceptable level, consistent with the Company's risk appetite and business objectives.

Risk mitigation strategies may include, but are not be limited to:

- strengthening internal controls and standard operating procedures;
- implementing preventive and detective control mechanisms;
- diversification of operations, customers, vendors, and investments, where appropriate;
- obtaining adequate insurance coverage for insurable risks;
- adopting technology-based solutions to improve operational efficiency and monitoring;
- conducting periodic compliance reviews and internal audits;
- providing regular employee training and awareness programmes;
- establishing contingency and recovery plans for critical business processes; and
- Implementing corrective and preventive actions arising from audits, inspections, or incidents.

Each Risk Owner shall be responsible for implementing approved mitigation plans within the agreed timelines and periodically reviewing their effectiveness.

12. Risk Monitoring & Reporting

Risk management shall be a continuous process supported by periodic monitoring and reporting mechanisms.

The Company shall:

- maintain and periodically update enterprise and functional risk registers;
- establish Key Risk Indicators (KRIs), wherever appropriate, to facilitate proactive monitoring;
- periodically review the status of identified risks and mitigation measures;
- report significant or emerging risks to Senior Management and the Risk Management Committee;
- promptly escalate material risks that may have a significant impact on the Company's business, financial performance, operations, compliance, or reputation;
- review risk reports at periodic intervals as determined by the Board or the Risk Management Committee; and
- Continuously evaluate the effectiveness of the risk management framework and recommend improvements where necessary.

Material incidents and significant changes in the Company's risk profile shall be reported to the Board in a timely manner.

13. Key Risk Categories

The Company shall periodically identify and monitor risks across various categories, including but not limited to:

a. Strategic Risks

Risks arising from changes in market conditions, competition, business strategy, acquisitions, expansion plans, technological disruption, or macroeconomic developments.

b. Operational Risks

Risks associated with service delivery, man power availability, procurement, supply chain management, project execution, infrastructure, health and safety, and operational processes.

c. Financial Risks

Risks relating to liquidity, credit, interest rates, foreign exchange exposure, taxation, financial reporting, fraud, and capital management.

d. Legal and Regulatory Risks

Risks arising from non-compliance with applicable laws, contractual obligations, labour laws, environmental regulations, and statutory requirements.

e. Information Technology and Cybersecurity Risks

Risks associated with information systems, cyber threats, data breaches, ransomware attacks, system failures, technology obsolescence, and digital transformation initiatives.

f. Human Resource Risks

Risks relating to talent acquisition, employee retention, succession planning, industrial relations, employee health and safety, and workforce capability.

g. Environmental, Social and Governance (ESG) Risks

Risks arising from environmental impacts, climate-related issues, social responsibilities, ethical business practices, corporate governance, and stakeholder expectations.

h. Reputational Risks

Risks that may adversely affect the Company's brand, market reputation, customer confidence, investor trust, or stakeholder relationships.

The above categories are indicative and may be modified or expanded by the Company based on evolving business requirements.

14. Business Continuity & Crisis Management

The Company shall establish and maintain appropriate Business Continuity Plans (BCPs) and Crisis Management procedures to ensure continuity of critical business operations during disruptions.

The framework shall include:

- identification of critical business processes;
- assessment of potential disruption scenarios;
- disaster recovery arrangements;
- crisis response protocols;
- emergency communication mechanisms;
- periodic testing and review of business continuity plans; and
- Continuous improvement based on lessons learned from actual incidents or simulation exercises.

Business continuity planning shall be reviewed periodically to ensure operational resilience.

15. Cyber Security & Information Security Risks

The Company recognizes cybersecurity and information security as critical components of enterprise risk management.

Accordingly, the Company shall endeavour to:

- protect information assets against unauthorized access, disclosure, alteration, or destruction;
- implement appropriate cybersecurity controls and security technologies;
- comply with applicable data protection and information security laws and regulations;
- conduct periodic vulnerability assessments and security reviews;
- provide cybersecurity awareness training to employees;
- establish incident response and recovery procedures for cyber incidents; and
- Periodically review cybersecurity risks in light of emerging threats and technological developments.

Material cybersecurity incidents shall be reported to the appropriate management and governance bodies in accordance with applicable laws and internal procedures.

16. ESG & Sustainability Risks

The Company acknowledges the increasing significance of Environmental, Social and Governance (ESG) considerations in long-term value creation.

Accordingly, the Company shall endeavour to identify, assess, and manage risks relating to:

- climate change and environmental impacts;
- resource efficiency and waste management;
- occupational health and safety;
- human rights and labour practices;

- diversity, equity, and inclusion;
- ethical business conduct;
- responsible supply chain management;
- community engagement; and
- Evolving sustainability-related regulatory requirements.

The Company shall integrate ESG considerations into its overall risk management framework wherever applicable.

17. Subsidiary Risk Management

The principles of this Policy shall, to the extent applicable, extend to the Company's subsidiaries.

The management of each subsidiary shall:

- establish appropriate risk management processes consistent with the nature and scale of its operations;
- identify and manage material business risks;
- report significant risks to the Holding Company through established governance channels;
- comply with applicable statutory and regulatory requirements; and
- Support consolidated enterprise risk reporting.

The Board and the Risk Management Committee may periodically review significant risks relating to subsidiaries as part of the overall enterprise risk management framework.

18. Review of Policy

This Policy shall be reviewed by the Risk Management Committee periodically and at least once every year, or earlier if required due to changes in applicable laws, regulations, business operations, or the Company's risk profile.

Any recommendations for modification shall be placed before the Board for its consideration and approval.

19. Disclosure

The Company shall make such disclosures relating to risk management as may be required under the Companies Act, 2013, the SEBI (Listing Obligations and Disclosure Requirements) Regulations, 2015, and other applicable laws.

The Board's Report shall include disclosures relating to the development, implementation, and effectiveness of the Company's risk management framework, wherever required under applicable law.

The Company shall also make such disclosures on its website or through stock exchange filings, where mandated by applicable regulatory requirements.

20. Amendment

The Board of Directors may amend, modify, revise, substitute, or rescind any provision of this Policy from time to time based on recommendations of the Risk Management Committee or to ensure compliance with applicable laws, regulatory requirements, or business needs.

In the event of any inconsistency between this Policy and any applicable law or regulation, the provisions of such law or regulation shall prevail to the extent of the inconsistency. The Policy shall thereafter be deemed to have been modified to the extent necessary to ensure such compliance.