EXICOM TELE-SYSTEMS LIMITED

RISK MANAGEMENT POLICY

Effective from September 27, 2023

RISK MANAGEMENT POLICY

1. PREFACE

1.1 OBJECTIVE

The main objective of this Risk Management Policy ("Policy") is to ensure sustainable business growth with stability and to promote a pro-active approach in reporting, evaluating, and resolving risks associated with the business.

In order to achieve the key objective, the Policy establishes a structured and disciplined approach to Risk Management in order to guide decisions on risk evaluating & mitigation related issues. The Policy is in compliance with the Regulation 17(9) of SEBI (Listing Obligations and Disclosure Requirements) Regulations, 2015, as amended ("SEBI Listing Regulations") and Section 134 (3) of Companies Act, 2013, as amended, which requires the Company to lay down procedures about risk assessment and risk minimization.

Given the Company's operations in the Critical Power and Electric Vehicle Supply Equipment (EVSE) sectors, which are characterized by rapid technological evolution, supply chain dependencies, and evolving regulatory frameworks, Exicom recognizes the need for a dynamic and forward-looking risk management framework.

1.2 APPLICABILITY

This Policy applies to every part of Exicom Tele-Systems Limited's (the "Company") business and functions.

2. DEFINITIONS

2.1 "Company" means Exicom Tele-Systems Limited.

2.2 "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.

2.3 "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.

2.4. "Risk Management Committee" means the Committee formed by the Board.

2.5. “Risk Assessment” means the overall process of risk analysis and evaluation.

2.6. “Chief Risk Officer (CRO)" means a senior executive (if appointed) responsible for coordination of risk management activities across the organization.

3. RISK MANAGEMENT

Principles of Risk Management:

3.1 The Risk Management framework shall provide reasonable assurance in protection of business value from uncertainties and consequent losses.

3.2 All concerned process owners of the company shall be responsible for identifying &mitigating key Risks in their respective domain.

3.3 The occurrence of Risk, progress of mitigation plan and its status will be monitored on periodic basis.

3.4 Risk management shall be embedded into strategic planning, capital allocation and project approval processes, particularly for large infrastructure and EVSE projects.

4. RISK MANAGEMENT PROCEDURES

General Risk management process generally includes the following key activities: Risk Identification, Risk Assessment, Risk Mitigation and Monitoring & Reporting.

4.1 Framework for Risk Identification

The purpose of framework of Risk identification is to identify the events that can have an adverse impact on the achievement of the business objectives. All Risks identified are documented and shall include internal and external risks including financial, operational, sectoral, sustainability (particularly ESG related risks), information, cybersecurity risks, technology obsolescence, supply chain and vendor risks, and regulatory/policy risks specific to the EV and power sectors. Risk documentation shall include risk description, category, classification, mitigation plan, responsible function / department and review frequency.

4.2 Risk Assessment

Assessment involves quantification of the impact of Risks to determine potential severity and probability of occurrence. Each identified Risk is assessed on two factors which determine the Risk exposure:

A. Impact if the event occurs
B. Likelihood of event occurrence

Risk Categories: It is necessary that Risks are assessed after taking into account the existing controls, so as to ascertain the current level of Risk. Based on the above assessments, each of the Risks can be categorized as – *low, medium, high or*

critical.

Risk scoring shall be applied consistently across the organization with a documented matrix for Impact and Likelihood to ensure comparability.

4.3 Measures for Risk Mitigation

All identified Risks should be mitigated using any of the following Risk mitigation plan:

a) *Risk avoidance*: By not performing an activity that could carry Risk. Avoidance may limit opportunities and shall be considered where residual exposure exceeds the Company's risk appetite.

b) *Risk transfer*: Mitigation by contract, insurance, or hedging; use of robust contractual terms with suppliers and customers to allocate risk.

c) *Risk reduction*: Employing methods/solutions that reduce the severity or likelihood of the loss (for e.g., redundant suppliers, stronger QA processes, manufacturing controls).

d) *Risk retention*: Accepting the loss when it occurs. Risk retention is a viable strategy for low impact Risks where the cost of mitigation exceeds expected loss.

e) Develop systems and processes for internal control of identified risks, including technical standards for product design, QA, and cybersecurity controls.

f) Business continuity and disaster recovery plans for critical functions, including remote monitoring and data centre redundancy for EVSE operations.

All mitigation actions must include: owner, target completion date, estimated cost and success criteria.

5. KEY RISKS AND CONCERNS

a. Operational and Liquidity risks

Critical power and EV charging projects typically involve long development cycles, which can lead to significant delays in revenue realization. Such delays may directly impact the Company's cash flow and liquidity, potentially hindering its operational efficiency and profitability.

Given the capital-intensive nature of these projects, dependencies on government payments, and customer receivables can amplify cash-flow volatility. The Company should explicitly monitor receivable ageing, retention releases, and contract milestone dependencies.

The timely execution and turnover depend not only on technical expertise and operational capabilities but also on the availability and efficient deployment of skilled personnel. External factors such as site readiness to enable deployments may also influence project execution timelines. Any gaps in these areas could negatively affect the Company's performance in the near term, impacting both project delivery timelines and overall business outcomes.

The Company should maintain a pipeline of trained field engineers and implement succession planning for key technical roles.

b. Strategy & Competition risks

We operate in a competitive and rapidly changing market and compete with both domestic as well as international Companies. The evolving industry landscape, characterized by comparatively low EV adoption in certain markets and the potential shift toward alternative technologies such as hydrogen, flex fuels, and hybrid solutions, poses emerging strategic challenges. Economics of scale enjoyed by competitors and the increasing pace of technological disruption may affect our operations, thereby impacting market share, business growth, and long-term competitiveness.

Rapid technological advancements including interoperability standards, bidirectional charging, and faster charging technologies may render existing product offerings less competitive. The Company shall continue to invest in R&D and strategic partnerships to mitigate these risk.

c. External Risk Factors

External risks factors include mainly the following:

- Economic Environment and Market conditions:
  Macroeconomic fluctuations and changes in demand patterns may influence project viability, cost structures, and investment cycles.
- Fluctuations in Foreign Exchange
  Volatility in exchange rates can impact input costs and profitability, particularly for imported components and overseas contracts.
- Political Environment
  Any deterioration in trade relations with key countries, such as China, could lead to adverse duty implications or supply chain disruptions, thereby affecting cost competitiveness and project timelines
- Competition
  Intensified competition from both domestic and international players may exert pricing pressure and impact margins.
- Revenue Concentration
  Dependence on limited customers or segments may expose the Company to concentration risk in the event of market shifts or regulatory changes.
- Inflation and Cost structure
  Rising input costs, particularly of key raw materials and electronic components, may affect margins. Additionally, a spike in warranty claims due to faulty EV chargers could further impact cost structure and profitability if not effectively mitigated through quality control and supplier management.

- Technology Obsolescence
  Rapid technological shifts including the transition toward megawatt charging infrastructure may render existing technologies less competitive if the Company fails to adapt swiftly. The Government's push for increasing local content further necessitates accelerated localization of critical components, as competitors move toward greater in-house manufacturing capabilities. Continuous investment in R&D and supply chain integration is essential to stay aligned with these industry advancements.

d. Internal Risk Factors

Internal risks factors mainly includes:
- Financial Reporting Risks
- Contractual Compliance
- Compliance with Local laws
- Quality and Project Management
- Environmental Management
- Human Resource Management
- Culture and values
- Cybersecurity vulnerabilities

e. *Other Identified Project and Operational Risks*

In addition to the risks identified above, the Company recognizes the following key risk areas relevant to its projects and operations:

- Experience and Capability Risk
- Time Over-run Risk
- Cost Over-run Risk
- Funding Risk
- Statutory Approvals Risk
- Off-take / Demand Risk
- Market Risk
- Pricing Level and Sustainability Risk
- Force Majeure Risk

6. ROLES AND ACCOUNTABILITIES IN RISK MANAGEMENT

Each employee within the organization plays a role in managing risks, particularly in identifying potential risks. The management team is accountable for creating risk mitigation strategies and ensuring the implementation of risk reduction measures. Risk management should be seamlessly integrated into the organization's broader planning and operational activities.

a. Board of Directors

Directors shall ensure the establishment, implementation, and ongoing maintenance of a risk management system consistent with this Policy. The responsibility for allocating specific roles in relation to risk management lies with the Managing Director & CEO, or the Board.

b. Project In Charge / Business Unit Head

The Business Unit Heads shall be accountable for managing risks in their respective business units. They must ensure compliance with all contractual commitments, recognizing that any deviation may expose the project and the Company to significant risks, including adverse impacts on profitability. Their duties extend to identifying risks, developing mitigation measures, and ensuring business objectives are achieved.

Business Unit Heads shall provide risk updates and ensure that project contracts contain appropriate performance guarantees and payment security mechanisms.

c. Chief Financial Officer

The CFO of the Company shall ensure the financial soundness of the Company and oversee the preparation of a comprehensive risk management plan for every commercial venture. In doing so, the CFO shall obtain inputs and advice from the Internal Auditor on relevant risk management issues.

The CFO shall oversee liquidity stress testing and maintain contingency financing arrangements for major projects.

d. Internal Audit

The purpose of the Internal Audit function is to provide an independent and objective evaluation of the Company's key financial and operational controls, as well as the effectiveness of its risk management practices.

The Internal Auditor shall be responsible for implementing this Policy in critical areas of the Company, maintaining an ongoing program for risk reassessment, and updating the Organization's Risk Register. These focus

areas will be derived from the risk management plan developed by Senior Executives. In addition, the Internal Auditor shall provide advice to the Risk Management Committee on matters relating to financial stability, occupational health and safety, and workers' compensation.

The Internal Auditor shall also review and test cybersecurity controls, vendor due diligence, and data protection measures, particularly for the Company's connected charging infrastructure and digital platforms. In addition, the Internal Audit shall monitor the effectiveness of supply chain risk management, ensure the adequacy of business continuity and disaster recovery plans, and verify that corrective actions arising from prior audits or risk reviews are implemented in a timely manner.

e. External Audit

The External Auditor, if appointed, is responsible for expressing an independent opinion on the truth and fairness of the Company's annual financial report. In fulfilling this responsibility, the External Auditor shall also evaluate the effectiveness of risk management practices and key internal control systems.

The External Auditor shall communicate significant deficiencies or material weaknesses identified during the audit to the Audit Committee, in accordance with applicable auditing standards. Further, the External Auditor shall review the Company's risk management disclosures and confirm consistency between the financial statements, internal control reports, and management representations.

7. BUSINESS CONTINUITY PLANNING AT EXICOM

In the event of an emergency or disaster, all necessary measures will be activated to ensure the uninterrupted operation of the business. The primary objective is to protect core business functions and safeguard the organization against any disruptions. The key components of Exicom's Business Continuity Plan include:

a) High Availability: Exicom ensures that its critical business systems & IT applications remain continuously accessible, even in the event of local failures or disruptions. These failures could stem from disruptions in business processes, physical infrastructure, or IT systems. Exicom's infrastructure is designed to be resilient, ensuring minimal downtime and uninterrupted access to essential internal and operational systems.

b) Continuous Operations: Exicom emphasizes the ability to maintain operations during both unexpected disruptions and planned activities, such as system maintenance or scheduled backups. This approach ensures that business processes continue smoothly without significant interruptions, regardless of the circumstances.

c) Disaster Recovery: Exicom has a robust Disaster Recovery Plan in place to restore operations in the event that the primary data center or operational site becomes non-operational. Should a disaster occur, Exicom's recovery strategy allows for quick data restoration and a seamless transition to an alternative site, ensuring the business can continue without prolonged downtime.

Additionally, the Business Continuity Plan shall specifically address potential disruptions in the EV charging network, manufacturing and supply of critical power systems, and availability of imported components. The Company shall conduct periodic mock drills, maintain redundant data connectivity for remote monitoring systems, and define clear Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs) for mission-critical applications.

8. MONITORING AND REVIEWING RISKS

The Company shall record the framework and processes for effective identification, monitoring, mitigation of the Risks.

Risk Management Committee to review the Risks at least once a year and add any new material Risk identified to the existing list considering changing industry dynamics and evolving complexity. These will be taken up with respective functional head for its mitigation.

The Risk Management Committee shall review key and high-priority risks periodically, as deemed appropriate, based on materiality and evolving nature of risks, and shall ensure a comprehensive review of all risks is conducted at regular intervals.

Existing process of Risk Assessment of identified Risks and its mitigation plan will be appraised by the Risk Management Committee to Board on an annual basis including recommendations made by the Committee and actions taken on it.

The Risk Management Committee shall coordinate its activities with other committees in instances where there is any overlap with activities of such committees as per the framework laid down by the Board of Directors. Further, the Committee shall review appointment, removal, and terms of remuneration of Chief Risk Officer, if any.

The Committee shall also review cyber risk dashboards, ESG-related risk metrics, and regulatory compliance trends to ensure proactive mitigation and timely disclosures as required under SEBI Listing Regulations.

9. RISK MANAGEMENT CHARTER

The Risk Management Policy shall be read along with the Risk Management Charter, adopted by the Board of Directors in its meeting held on 23rd May 2025, The Charter clearly defines and emphasizes the roles, responsibilities, and duties of the Risk Management Committee, while also placing strong focus on the Company's risk management framework. It outlines the processes for risk assessment and mitigation, establishes the Company's risk appetite and tolerance, and provides oversight for derivative transactions, thereby defining the structured framework within which the Company conducts its risk management activities.

The Charter shall be reviewed annually to align with emerging sectoral risks such as cybersecurity, environmental compliance, and energy transition mandates, as well as any updates in SEBI or Companies Act provisions.

10. AMENDMENT AND REVIEW OF THE POLICY

Any change in the Policy shall be approved by the board of directors ("Board") of the Company. The Board shall have the right to withdraw and / or amend any part of this Policy or the entire Policy, at any time, as it deems fit, or from time to time, and the decision of the Board in this respect shall be final and binding.
Any subsequent amendment/modification in the Companies Act, 2013 or the Rules framed thereunder or the SEBI Listing Regulations and/or any other laws in this regard shall automatically apply to this Policy.

This policy shall be reviewed at least once every two (2) years by the Risk Committee, or earlier if there are material changes in the regulatory environment, business model or industry structure. The Committee shall recommend revisions to the Board for approval, ensuring continued adequacy, effectiveness, and alignment with Exicom's strategic and operational objectives.

11. COMMUNICATION:

This Policy shall be posted on the website of the Company.

A copy of this Policy shall also be disseminated internally to all employees and communicated through training or awareness programs to ensure effective implementation.

Name of the Policy	Approving Authority	Approval/ Revision Date	Version
Risk Management Policy	Board of Directors	27-09-2023	V1 - Adoption
		28-05-2024	V2 – Review
		10-11-2025	V3 – Revision