INFRONICS SYSTEMS LIMITED

Risk Management Policy

INTRODUCTION:

Risk management is attempting to identify and then manage threats that could severely impact or bring down the organization. Generally, this involves reviewing operations of the organization, identifying potential threats to the organization and the likelihood of their occurrence, and then taking appropriate actions to address the most likely threats. Risk management is an integral component of good corporate governance and fundamental in achieving the company's strategic and operational objectives. It improves decision-making, defines opportunities and mitigates material events that may impact shareholder value.

Infronics Systems Limited ("the Company") desires to refine its organizational wide capabilities in risk management so as to ensure a consistent, efficient and effective assessment of risks in the achievement of the organization's objectives. The Company's risk management policy provides the framework to manage the risks associated with its activities. It is designed to identify, assess, monitor and manage risk.

OBJECTIVES:

The Risk Management Policy forms an integral part of the internal control and corporate governance framework of Infronics Systems Limited. The Company's Risk Management Policy endeavors to support its objectives among others by –

- To ensure that all the current and future material risk exposures of the company are identified, assessed, quantified, appropriately mitigated, minimized and managed i.e to ensure adequate systems for risk management.
- Ensuring sustainable business growth with stability and promoting a proactive approach in reporting, evaluating and resolving risks associated with the business;
- Improving decision making, planning and prioritization by comprehensive and structured understanding of business activities, volatility and opportunities/ threats;
- Evaluating the likelihood and impact of major adverse events;
- Developing responses to either prevent such events from occurring or manage and minimize the impact of such event, if it does occur;
- Identifying any unmitigated risks and formulating action plans for addressing such risks;
- Compliance with provisions of relevant legislations;
- To assure business growth with financial stability;
- Identification of Internal and external risks specifically faced by the Company in particular including financial, legal, regulatory, environment, cyber security risk and any risk as may be determined by the Committee;
- To ensure systematic and uniform assessment of risk.

STATUTORY REQUIREMENTS:

The Companies Act, 2013 and the SEBI Listing Obligations and Disclosure Requirements) Regulations, 2015, ("LODR - 2015") have also incorporated various provisions in relation to Risk Management policy, procedure and practices.
Section 134(3)(n) of the Companies Act, 2013 requires a statement to be included in the report of the board of directors ("Board") of the Company, indicating 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.

Further, the provisions of Section 177(4)(vii) of the Companies Act, 2013 require that every Audit Committee shall act in accordance with the terms of reference specified in writing by the Board which shall inter alia include evaluation of risk management systems.

In line with the above requirements, it is therefore required for the Company to frame and adopt a "Risk Management Policy" ("Policy") of the Company.

ROLES AND RESPONSIBILITIES OF THE BOARD:

- Approve and review the Risk Management Policy;
- Define the Company's risk appetite Identify and assess internal and external risks in particular including financial, operational, sectoral, sustainability, information, cyber security risks or any other risk that may impact the Company in achieving its strategic objectives or may threaten the existence of the Company;
- Define the role and responsibility of the Risk Management Committee and delegate monitoring and reviewing of the risk management plan to the Risk Management Committee and such other functions as it may deem fit; which also shall specifically cover the function related to the Cyber Security;
- Oversee the development and implementation of risk management framework and maintain an adequate monitoring and reporting mechanism;
- Formulate risk management strategy to manage and mitigate the identified risks;
- Ensure risk management is integrated into board reporting and annual reporting mechanisms;
- Convene any board-committees that are deemed necessary to ensure risk is adequately managed and resolved where possible.

RISK MANAGEMENT PROCESS

I. Risk Analysis:
Risk analysis involves consideration of the sources of risk, their consequences and the likelihood that those consequences may occur. The control measures and procedures to control risk are identified and their effectiveness is assessed. The impact and likelihood of an event and its associated consequences are assessed in the context of the existing controls.

II. Risk Identification:
Risk Identification is obligatory on all vertical and functional heads that with the inputs from their team members are required to report the material risks to the Board along with their considered views and recommendations for risk mitigation. Analysis of all the risks thus identified shall be carried out by the Board through participation of the vertical/functional heads.

III. Risk Assessment:
Risk evaluation involves comparing the level of risk found during the analysis process against the predefined risk weights so as to assess their potential severity of loss and to the probability of occurrence. Risk weights of High / Medium / Low can be assigned based on parameters for each operating activity. The output of the risk evaluation is a prioritized list of risks for further action. If

the resulting risks fall into the low or acceptable risk categories they may be accepted with minimal further treatment.

IV. Risk Response

Risk response involves identifying the range of options for treating risk, assessing those options, preparing risk treatment plans and implementing them. Options include avoiding the risk, reducing the likelihood of the occurrence, reducing the consequences, transferring the risk, and retaining the risk. Gaps will then be identified between what mitigating steps are in place and what is desired. The action plans adopted will be documented and its implementation tracked as part of the reporting process. Ownership and responsibility for each of those risk mitigation steps will then be assigned. This will be captured in a 'Risk Assessment and Control Matrix' which comprises the key top risks.

V. Reporting

The Board should provide assurance to the Audit Committee with regards to the financial records, risk management and internal compliance. Risks will be continuously monitored and reviewed; and the effectiveness of the controls in place and of the risk action plans is assessed to ensure changing circumstances do not alter risk priorities.

VI. Policy Review

The policy shall be reviewed as and when necessary, considering the changing industry dynamics and evolving complexity to ensure its effectiveness and continued relevance to the business. Feedback on the implementation and effectiveness of the policy will be obtained from the risk reporting process, internal audits, and other available information.

****