RISK MANAGEMENT POLICY

1. Introduction

Risks are events or conditions that may occur, and whose occurrence, if it does take place, has a harmful or negative impact on the achievement of the organization's business objectives. The exposure to the consequences of uncertainty constitutes a risk.

Thyrocare Technologies Limited **("Company")** like any other business entity is exposed to various risks in the normal course of its activities. No business can be conducted without accepting a certain level of risk, and any expected gain from a business activity is to be assessed against the risk that activity involves. Hence, it is the responsibility of every management to identify the possibilities of the risks, take necessary steps to protect against the risks, mitigate the risks, indemnify against the risks, and generally plan for safeguarding the business from the harmful effects of risks.

2. Objective

Risk Management is a continuous process of identifying, evaluating and assessing the inherent and potential risk, adopting the methods for its systematic reduction in order to sustainable business development.

The main objective of this Policy (as defined hereinbelow) 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, this Risk Management Policy ("**Policy**") establishes a structured and disciplined approach to risk management, including the development of the risk register, in order to guide decisions on risk evaluating & mitigation related issues.

The specific objectives of the Policy are:

a. To establish a risk intelligence framework for the Organization.
b. To establish ownership throughout the Organization and embed risk management as an integral part of the business rather than a stand-alone system.
c. To help the decision makers of the Organization explicitly take account of uncertainty, the nature of that uncertainty, and work towards a solution to address it.
d. To ensure that all the current and expected risk exposures of the Organization are identified, qualitatively and quantitatively evaluated, analysed and appropriately managed.
e. To assure demonstrable achievement of objectives and improvement of financial stability of the Organization.
f. To ensure transparency of risk management activities with respect to internal and external stakeholders.
g. To ensure compliance to appropriate regulations, wherever applicable, through the adoption of leading practices.

3. Applicability

The Policy is formulated in compliance with Regulation 17(9)(b) of SEBI (Listing Obligations and Disclosure Requirements) Regulations, 2015 **("the Listing Regulations")** and provisions of the Companies Act, 2013 **("the Act"),** which requires the Company to lay down procedures about risk assessment and risk minimization.

Also, under Section 134(3)(n) of the Act, and rules made thereunder, provides that every company must include a statement, in the Board's Report to the Shareholders indicating the development and implementation of a Risk Management Policy, thereby making it mandatory for the companies to develop and implement such a policy.

This policy applies to every part of the Company's business and functions.

4. Definitions

a) "**Board**" means the board of directors of the Company.

b) "**Risk Management**" means coordinated precautionary actions planned or taken to prevent the occurrence of risks, control their damaging impact and minimise the losses arising out of such risks.

c) "**Risk Register**" refers to the tool for recording the risks identified under various operations.

d) "Vigilance Committee" shall be the committee comprising of one or more of the following as members:

- Executive Director(s),
- Chief Financial Officer,
- Company Secretary, .
- Vigilance Officer and/or
- Any other member as may be appointed by the Vigilance Committee.

e) "Vigilance Officer" shall be the designated officer appointed by the Vigilance Committee.

5. Risk Management

Principles of Risk Management:

a) The risk management shall provide reasonable assurance in protection of business value from uncertainties and consequent losses.
b) All concerned process owners of the Company shall be responsible for identifying & mitigating key risks in their respective domain.
c) The occurrence of risk, progress of mitigation plan and its status will be monitored on periodic basis.

Risk Management envisages addressing to the following tasks in dealing with the above risks:

1) Identifying potential threats (including risks related to cyber security) and their impact on the business;
2) Assessing the likelihood of occurrence of the threats and risks;
3) Taking necessary measures to eliminate or control the factors that might lead to occurrence of such risks;
4) Planning for remedial steps in the event of occurrence of the risk;
5) Chalking out strategies to restrict the consequential damages;
6) Taking steps for mitigating or minimizing the losses and other damages; and
7) Preparing an action plan for restoring the business to its original position in the event of occurrence of the risk.

6. Risk Management Procedures

The Company's risk management process comprises of structures and guidelines which assist the Company to identify, assess, monitor and manage its business risk, including any material changes to its risk profile.

To achieve this, the Company has defined the responsibility and authority of the Company's Board of Directors as stated above, to oversee and manage the risk management process, while conferring responsibility and authority on the Company's senior management to develop and maintain the risk management program in light of the day-to-day needs of the Company. Regular communication and review of risk management practice provides the Company with important checks and balances to ensure the efficacy of its risk management process.

The key elements of the Company's risk management program are set out below.

a) Risk Identification

The purpose 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 in the form of a Risk Register. Risk Register incorporates functions, risk description, root cause, category, classification, risk assessment. The Risk Register format is annexed as "**Annexure 1**" to this Policy.

In order to identity and assess material business risks, the Company defines risks and prepares risk profiles in light of its business plans and strategies. This involves providing an overview of each material risk, making an assessment of the risk level and preparing action plans to address and manage the risk.

i. Risk Categorisation:

All the risks that have been identified shall be categorised under the following risk categories - Strategic, Operational, Reporting and Compliance risk.

- **Strategic Risk** - Risk of loss resulting from business factors. These risks adversely affect the achievement of strategic objectives and may impair overall enterprise value.
- **Operational Risk** - Risk of loss resulting from inadequate or failed processes, people and information systems.

- **Reporting Risk** - Risk of inadequate internal or external reporting due to wrong financial as well as non-financial information in the reports
- **Compliance Risk** - Risk of loss resulting from legal and regulatory factors.

ii.Risk Classification:

All the risks that have been identified shall be further classified into following types to help the Company in prioritizing the Risks

- **Asset Risk**- Risk of loss resulting from depreciation, under-utilisation or loss of control over physical assets of company. Competition Risk – Risks pertaining to the external competitors of the company such as entry of new competitors, FDI etc.
- **Compliance Risk** - Risk of loss resulting from legal and regulatory factors, such as strict privacy legislation, compliance laws, and intellectual property enforcement.
- **Contract Risk** – Risks pertaining to the contracts signed with client and subcontractors.
- **Contractor/ Vendor Risk** – Risks originating from company's relationship and dependence on third party vendors, contractors or outsourcing partners.
- **Environmental Risk** – Risks having implications on the environment, weather, pollution or risks arising due to changes in environment.
- **Expense Risk** – The risk of a change in value caused by the fact that the timing and/or the amount of expenses incurred differs from those expected, e.g. assumed for pricing basis**.**
- **Financial Risk** - All risks which have a financial implication such as adverse movements in foreign exchange rates, capital expenditure etc.
- **Foreign environment risk** - The risk arising due to exposure to foreign laws, regulation and socio-political environment.
- **Litigation Risk** - Risk of loss arising out of litigations against or litigation initiated by the company.
- **Market Risk** – Risks pertaining to external market factors such as demand uncertainty, price volatility etc.
- **People Risk** - Risks (like attrition) that are part of the personnel related processes of the company such as recruitment, skill sets and performance measurement.
- **Process Risk/ Execution Risk –** The risk arising due to lack of adequate process or inadequate execution of defined processes.
- **Project Risk** – Risks which impacts the execution of any project resulting in time and cost overrun.
- **Regulatory/Political Risk** - The risk arising due to change in regulatory policy of the country.
- **Reporting Risk** - Risk of inadequate internal or external reporting due to wrong financial as well as non-financial information in the reports.
- **Reputation Risk** – Risks having implications on the brand and reputation of the company.
- **Technology Risk** – Risks originating from usage and deployment of technology in the organisation in its operations and management such as product obsolescence because of technology gap.
- **IT Security Risk –** Risks originating from 3 threat vectors via. Emails, internet and machine.
- **Cyber Security Risk**- Risks originating from threat vectors via. Applications, Network, Data leakage and Social engineering.
- **Corporate accounting fraud Risk** arising out of misusing or misdirecting of funds, overstating revenues, understating expenses etc.

iii.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:

(i) Impact if the event occurs
(ii) 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 and high.

iv.Risk Mitigation

The following framework shall be used for implementation of risk mitigation plan:

(i) **Risk avoidance:** By not performing an activity that could carry risk. Avoidance may seem the answer to all risks, but avoiding risks also means losing out on the potential gain that accepting (retaining) the risk may have allowed.
(ii) **Risk transfer:** Mitigation by having another party to accept the risk, either partial or total, typically by contract or by hedging / insurance.
(iii) **Risk reduction:** Employing methods/solutions that reduce the severity of the loss e.g. concreting being done for preventing landslide from occurring.
(iv) **Risk retention:** Accepting the loss when it occurs. Risk retention is a viable strategy for small risks where the cost of insuring against the risk would be greater than the total losses sustained. All risks that are not avoided or transferred are retained by default.

v.***Risk Monitoring and reviewing***

Risk monitoring, reviewing, mitigating and reporting are critical components of risk management process. Once risks are identified, it is necessary to prioritize them based on the impact, dependability on other functions, effectiveness of existing controls etc.

Internal audit reviews the risk register once a year and adds any new material risk identified to the existing list. These will be taken up with respective functional head for its mitigation. Existing process of risk assessment of identified risks and its mitigation plan will be appraised to Board on an annual basis. The Policy envisages monitoring as follows:

1) Regular checking or surveillance to prevent risks caused by human acts of commission and omission.
2) Constant monitoring of the external environment to detect any possible risks that may be caused by economic, political, sociological or technological changes.
3) Periodical reporting to the Audit Committee and to the Board of Directors, to facilitate broad-based discussions and conscientious decisions if needed to improve the checks and balances, and to make the Policy more effective.
4) Implementation of decisions taken and reporting back to the Audit Committee and to the Board.

7. Risk Management Committee

The Board have formed a Risk Management Committee ("**Committee**") who shall periodically review this policy of the Company so that the management controls the risk through properly defined network.

The Board may re-constitute the composition of the Committee, as it may deem fit, from time to time.

The majority of members of Committee shall consist of members of the board of directors, with at least one independent director. The Chairperson of the Committee shall be a member of the Board of Directors and senior executives of the Company may be members of the Committee.

The meetings of the Risk Management Committee shall be conducted twice in a year and in such a manner that on a continuous basis not more than one hundred and eighty days shall elapse between any two consecutive meetings.

The day to day oversight and management of the Company's risk management program has been conferred upon the Vigilance Officer /CFO. The Vigilance Committee is responsible for ensuring that the Company maintains effective risk management and internal control systems, processes, and provides regular reports to the Committee on the effectiveness of the risk management program in identifying and addressing material business risks.

8. Amendment

Any change in the Policy shall be approved by the Board. 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 Act or the rules framed thereunder or the Listing Regulations and/or any other laws in this regard shall automatically apply to this Policy.

9. Interpretation

In any circumstance where the terms of this Policy are inconsistent with any existing or newly enacted law, rule, regulation or standard governing the Company, the said law, rule, regulation or standard will take precedence over this Policy.

10. Communication of this Policy

The Policy and the manner in which it is being implemented must be disclosed in the Board's report.

Annexure 1

Format of Risk Register

Sr. No.	Function	Risk Description	Root cause	Risk Category	Risk Classification	Risk Assessment		Comments	Remarks
						Impact Rating	Likelihood Rating		