POLICY ON RISK MANAGEMENT AND INTERNAL CONTROLS

1. INTRODUCTION

In recognition of the diverse array of risks both general and industry/country specific that shape our business landscape, risk management forms an integral aspect of corporate ethos and governance policies at Pegasus Hotels of Ceylon PLC. We recognize the paramount importance of enterprise risk management (ERM) as a unifying process that paves the way for effective risk management initiatives across our diverse business activities. This Policy outlines the framework for managing risks and establishing internal controls within the Company. It aims to safeguard assets, ensure the reliability of financial reporting, promote compliance with laws and regulations, and support the achievement of strategic objectives.

2. OBJECTIVES

At Pegasus Hotels of Ceylon PLC, with steadfast commitment, we have integrated ERM into the fabric of our organization, leveraging its inherent benefits to enhance the overall quality of our operations.

By adopting ERM, the Company aims to strengthen its governance mechanisms, fortify its strategic planning, and instill unwavering confidence in its ability to deliver exceptional results. As we continue on our journey, we remain committed to fostering risk awareness, promoting proactive management, and empowering our organization to seize opportunities while navigating potential challenges.

As part of our business plan implementation, the Company has made enterprise risk management integral to all our business activities.

Our risk management process supports:
- Corporate governance
- Quality of business planning
- Audit planning
- Project planning and implementation
- Building confidence across various stakeholder groups

3. RISK MANAGEMENT FRAMEWORK

3.1 Categorization of Risks

The Management categorizes risk into three types to create a common language for better communication, knowledge-sharing and comparison;

- Business Environment Risk
- Strategic Risk

- Business Process Risk

3.2 Identifying Risk Drivers

Risk Drivers are key factors that contribute to risk creation while Risk Indicators are deviations from set goals or KPIs which are promptly identified through ongoing reviews and monitoring conducted by the Management. This process helps us to manage risk proactively and effectively.

3.3 Risk Assessment

The likelihood of occurrence and the probability of the outcomes of the identified risks shown above are analysed using qualitative and quantitative methods. The Management uses the Risk Grid to determine the contribution of each risk to the aggregate risk profile in terms of its impact on the achievement of the Company’s objectives and these are prioritized accordingly.

3.4 Risk Response

Once risk events are identified, the risk responses could involve:

- Risk Acceptance
- Risk Avoidance
- Risk Transfer/ share
- Risk Minimisation

The first line of defense involves timely supervision and monitoring of risk management by Heads of Departments. Action plans are reviewed and monitored by management teams, with identified risks reassessed. The Audit Committee, and Board of Directors are updated on action plan status and outcomes.

3.5 Risk Reporting and Monitoring

Regularly monitor and review risks to ensure they remain within acceptable tolerance levels.

3.6 Internal Control Framework

The key components of the Company’s internal control framework involves:

3.6.1 Control Environment: The Company maintains a well-defined organizational structure with clearly delineated reporting lines and responsibilities. The senior management emphasize ethics and integrity in every aspect of operations, promoting a zero-tolerance policy towards unethical behaviour. The senior management actively demonstrate commitment to maintaining a strong control environment through regular communications. Their visible leadership sets a positive example for all employees, reinforcing the importance of internal controls and compliance with policies and procedures.

3.6.2 **Risk Assessment:** Carried out based on the established enterprise risk management process.

3.6.3 **Control Activities**: The processes shall be governed by clearly laid out process manuals.

3.6.4 **Information and Communication**: Effective communication shall be established across the Company through online platforms and e mails.

3.6.5 **Monitoring and Review**: Regularly monitoring and evaluation shall be carried out by the Group Internal Auditor.

4. GOVERNANCE STRUCTURE

The Risk Management Governance Structure includes a reporting framework for better Corporate Governance oversight by the Board. The functions of each party involved in the Governance Structure are as follows;

Board of Directors

- Review, approve and have oversight on the ERM framework and risk management strategies of the Company.
- Support senior management in implementing risk management actions.
- Approve Business Plan.
- Review Reports, risk dashboard and summary of risk register.

Audit Committee

- Considers adequacy of risk management and internal control framework.
- Review risk management reports, dashboard/risk register.
- Review reports from internal and external auditors.

Management Team

- Considers new and emerging risks.
- Develop/monitor suitable action plans to mitigate/manage risks.
- Considers actions to improve risk management process.
- Provide representation on compliances.

Risk Owners

- Responsible for day-to-day monitoring/supervision of risk and risk mitigation actions.
- Required to evaluate status of risk and effectiveness of risk mitigation action plans.

5. IMPLEMENTATION AND POLICY REVISION

The implementation of this Policy is the responsibility of the Board of Directors and this Policy must be reviewed at least once in every two years. It may be amended at any time with the approval of the Board of Directors of the Company.

****