TERMS OF REFERENCE OF THE RISK MANAGEMENT COMMITTEE

1.0 PURPOSE

1.1 The primary objective of the Risk Management Committee ("the Committee"), as a committee of the Board of Directors ("the Board"), is to assist the Board to effectively discharge its fiduciary responsibilities for overseeing the establishment and the effectiveness of the S P Setia Berhad and Group of Companies ("the Group")'s processes and practices on:

- Enterprise Risk Management;
- Business Continuity Management;
- Business Sustainability Management; and
- Integrity & Governance.

2.0 COMPOSITION

2.1 The Committee shall comprise at least three members, and a majority of its members must be independent non-executive directors.

2.2 The Board shall appoint an independent non-executive director from amongst one of these members as the Chairman of the Committee.

2.3 If a member retires or resigns from his position, that member ceases to be member of the Committee. The Board may appoint a successor.

3.0 REPORTING RESPONSIBILITIES

3.1 The Committee will report to the Board on the nature and extent of the functions performed by it; and may make recommendations to the Board on the matters as set out in the Committee's duties and responsibilities.

4.0 ATTENDANCE AT MEETINGS

4.1 The Chief Executive Officer ("CEO"), Chief Operating Officer ("COO"), Chief Financial Officer ("CFO"), Executive Vice Presidents ("EVPs"), and Chief Risk, Integrity and Governance Officer ("CRIGO") shall attend the Committee meetings.

4.2 Other senior management team may attend the meeting upon the invitation of the Committee.

4.3 The Company Secretary shall be the secretary of the Committee.

5.0 MEETINGS (FREQUENCY, AGENDA, MINUTES AND REPORTING)

5.1 The Committee shall meet at least 4 times a year. The Committee may call such additional meetings as the Chairman decides are necessary for the Committee to fulfil its obligations.

…2/-

5.2 The Chairman shall review the agenda for each Committee meeting prior to its issue. A notice of each meeting confirming the date, time, venue and agenda shall be forwarded to the Committee seven (7) days before the date of the meeting.

5.3 Minutes of the proceedings of Committee meetings shall be recorded by the Secretary, approved in draft form by the Chairman and circulated to all the Committee members. Wherever possible, minutes of the Committee meetings will be confirmed at the next meeting and signed by the Chairman.

5.4 The Chairman of the Committee shall report on each meeting to the Board.

6.0 QUORUM

6.1 The quorum for the meeting shall be two (2) Committee members.

7.0 AUTHORITY

7.1 The Committee is authorised by the Board to instruct any investigation within its terms of reference, which includes seeking any information it reasonably requires from any employee of the Group for the purpose of discharging its functions and responsibilities (acting lawfully and within these terms of reference).

7.2 The Committee may obtain legal or other advice from independent professionals and appoint external advisers with relevant experience and expertise to assist the committee if it considers necessary; and

7.3 The Committee can instruct the CRIGO to perform duties as necessary to support the Committee in discharging its responsibilities. The CRIGO has direct reporting line to the Committee and shall have direct access to the Chairman of the Committee.

8.0 DUTIES

8.1 In order to fulfil its roles and responsibilities to the Board, the Committee shall:

(a) **Enterprise Risk Management ("ERM")**

i. oversee and recommend the ERM policies and best practices of the Group;

ii. review and recommend changes as needed to ensure that the Group has in place at all times an ERM policy which addresses the Group's business risks which consist of strategic, operational, financial and legal/compliance risks;

iii. review and monitor the implementation and maintaining of a sound risk management framework, based on internationally recognised standards, which identifies, assesses, manages and monitors the Group's business risks;

iv. set reporting guidelines for management to report to the Committee on the effectiveness of the Group's management of its business risks;

v. review the Group and its subsidiaries' risk profiles, key risk indicators and evaluate the measures taken to mitigate the business risks; and

…3/-

vi. review and recommend the Statement on Risk Management and Internal Controls (SORMIC) to be disclosed in the Group's Annual Integrated Report.

(b) **Business Continuity Management ("BCM")**

i. oversee and recommend the BCM framework, policies and best practices of the Group, based on internationally recognised standards and relevant regulations; and

ii. ensure that the Group's BCM framework and plan documents are continuously reviewed, tested and updated to capture changes in business environment, and process improvement opportunities.

(c) **Business Sustainability Management ("BSM")**

i. oversee and recommend the BSM framework, policies and practices of the Group, which are aligned with internationally recognised standards and relevant regulations;

ii. provide oversight and guidance on the establishment and implementation of the Group's BSM strategies and initiatives; and

iii. review and recommend the Sustainability Statement to be disclosed in the Group's Annual Integrated Report.

(d) **Integrity & Governance**

i. oversee and recommend the Integrity & Governance framework, policies and business code of conducts of the Group, which are aligned with relevant laws and regulations, and internationally recognised standards;

ii. oversee management of complaints via whistleblowing channels, investigation process and outcome; and overall Integrity & Governance process and practices within the Group;

iii. review and ensure timely and accurate reporting on Integrity & Governance matters to relevant authorities/agencies; and

iv. oversee and ensure that the Group's Integrity & Governance Unit has access to the information and adequate resources which are required in order to perform its duties.

8.2 Ensure effective communication, awareness and education programmes on the ERM, BCM, BSM, and Integrity & Governance are continuously carried out by the Group.

8.3 Consider other related matters, as defined and endorsed by the Board.

8.4 The Committee is to review its duties and responsibilities on an annual basis.

9.0 OTHERS

9.1 The terms of reference shall be reviewed on an annual basis to ensure that it reflects current best practice in corporate governance, ERM as well as BCM, BSM, and Integrity & Governance. Board approval is required for any changes in the term of reference.