Statement on Risk Management and Internal Control

INTRODUCTION

This Statement on Risk Management and Internal Control ("Statement') is made following Paragraph 15.26(b) of the Bursa Securities Listing Requirements and the guidelines contained in the Statement on Risk Management and Internal Control: Guidelines for Directors of Listed Issuers. It is also made following the Hong Kong Code contained in Appendix C1 of the HK Listing Rules.

The Board of Directors ("Board") remains committed to maintaining a sound risk management and internal control system to manage risks and safeguard shareholders' investments and the Group's assets.

BOARD RESPONSIBILITY

The Board affirms its overall responsibility in establishing a sound risk management framework and internal control system for the Group as well as reviewing its adequacy and effectiveness. The Board is of the view that the risk management framework and internal control systems are designed to manage and mitigate the Group's risks within the acceptable risk parameters, rather than to eliminate all risks of failure to achieve business objectives.

The Board defines the Group's risk appetite as moderate, seeking a balance between growth and stability. This risk appetite is reviewed and approved regularly to ensure its continued relevance, considering the Group's strategic objectives and evolving risk environment.

It is important to note that due to inherent limitations, the system provides reasonable but not absolute assurance against material misstatements, losses, fraud, breaches of laws and regulations, or unforeseen emerging risks.

RISK MANAGEMENT FRAMEWORK

The Group has established an appropriate control structure and systematic process for identifying, evaluating, monitoring and managing significant risks pertinent to the achievement of its overall corporate objectives throughout the year. This process is regularly reviewed by the Board. This framework is designed to support the achievement of the Group's strategic objectives, ensuring that risk considerations are integrated into key decision-making processes.

The Audit Committee assists the Board by:

- Reviewing the adequacy and effectiveness of the Group's risk management and internal control system;
- Assessing management's identification and mitigation of significant risks;
- Reporting any significant failures or potential breaches of the Group's risk management policy to the Board.

The Audit Committee conducts quarterly reviews, drawing upon internal audit reports, management presentations, and independent assessments, covering financial reporting, operational efficiency, and regulatory compliance.

The Group Executive Committee ensures on behalf of the Board that business risks are identified, assessed, managed and monitored across the businesses of the Group. The Group Executive Committee reports quarterly to the Board on changes in the risk landscape and developments in the management of principal risks.

The Group Executive Committee has established two separate Risk Management Committees ("RMC'), one in Malaysia and one in Hong Kong, to oversee and drive improvement in risk management.

The two RMCs are responsible for overseeing the implementation of the risk management framework, reviewing the risk management processes periodically and ensuring that ongoing measures taken are adequate to manage, address and mitigate the risks identified.

The same principle applies to the Risk Management Units ("RMU"), where risk identification, mitigation and monitoring accountability rest with the respective subsidiaries within the Group. The RMU comprises key management staff from each division within the operating company.

RISK MANAGEMENT PROCESS

The risk management process is cascaded through the Group. All key management, heads of subsidiary companies and heads of departments have to identify, evaluate and manage risks associated with the business operations on an ongoing basis with defined parameters, and record the identified risks in the risk registers. This process must take place at least once a year.

For each risk identified, the management will assess the root causes, consequences and mitigating controls. An assessment is then made taking into account the probability of the risk occurring and the impact before and after mitigating controls. The content of the risk register is determined through review by the RMU and discussions with senior management.

At each RMU meeting, the overall risk profile of the operating company is assessed, significant risks are identified, the risk register is updated and action plans for mitigation are prepared. A risk assessment report comprising the action plans on significant risks is tabled to the RMC. The deliberation of risks and related mitigating responses are carried out at regular management meetings of the operating companies.

In essence, risks are dealt with and contained at the respective subsidiaries and are communicated upwards to the Board via the RMC and the Group Executive Committee.

The Group Executive Committee is assisted by the Risk Coordinators in Hong Kong and Malaysia, who act as the Group's focal points for all risk management activities within their respective regions.

IDENTIFICATION AND MANAGEMENT OF EMERGING RISKS

The Group proactively identifies and manages emerging risks through horizon scanning, scenario planning, and regular monitoring of the business environment. The RMCs are responsible for identifying and assessing potential emerging risks and developing appropriate mitigation strategies.

PRINCIPAL RISKS AND UNCERTAINTIES

Outlined below are the principal risks and uncertainties that could materially affect the Group's performance. The Board continually reviews the potential risks facing the Group and the controls in place to mitigate any adverse impact. The Board also recognises that this is not an exhaustive list of all relevant risks and uncertainties. Other factors besides those listed below could also affect the Group and give rise to material consequences.

Nature of Risk

Economic and Geopolitical Uncertainty

The Group's operations in Hong Kong, North America, and Malaysia expose it to fluctuations in the economic conditions of these regions. Ongoing uncertainty surrounding U.S. tariff policies has a direct impact on the global macroeconomic climate, potentially increasing the risk of trade barriers and contributing to a general economic downturn, either globally or within the Group's operating areas.

This challenging macroeconomic landscape creates uncertainty that could reduce consumer discretionary spending. Consequently, demand for the Group's products and services may decline, which could adversely affect profitability and operating cash flow.

Geopolitical tensions, particularly in the Middle East, also pose a risk. Such tensions could disrupt supply chains, restrict business activities, and lead to higher transportation costs, potentially impacting input prices.

Mitigating actions

- Diversification of revenue streams, including digital subscriptions and event-based monetisation.
- Implementation of cost control measures.
- Currency hedging strategies to manage foreign exchange exposure.
- Continuous market monitoring and adaptive pricing strategies.
- Strengthen supply chain resilience by diversifying sourcing locations and establishing relationships with alternative suppliers to minimise dependency on any single source.
- Leverage the Group's global presence to strategically distribute resources across different markets and product lines, reducing dependence on any single market or sector during economic uncertainties.

Nature of Risk

Market Disruption

The media landscape is undergoing a seismic shift driven by the rapid advancement of Artificial Intelligence (AI) and evolving consumer preferences, posing significant risks to the Group's traditional business model and established revenue streams.

AI-powered tools like ChatGPT, DeepSeek and etc are democratising content creation, enabling the mass production of articles, images, and even video. This proliferation of AI-generated content intensifies competition across all media platforms and drastically reduces barriers to entry for new players.

This disruption manifests in several critical ways for the Group. Firstly, the rise of AI-generated "content farms" producing low-cost, Search Engine Optimisation (SEO)-optimised material is actively diverting programmatic advertising revenue away from legitimate publishers. This erosion of digital advertising-income is directly hindering the Group's potential for digital growth.

Secondly, consumers are increasingly discerning and perceive less value in traditionally produced content when faced with a flood of readily available, often free, AI-generated alternatives. This shift in perception is impacting their willingness to pay for premium content subscriptions and other revenue-generating services.

Furthermore, the Group faces increasingly stiff competition for digital advertising revenue from large technology companies and digital native publishers. These entities, often leveraging their vast troves of user data and sophisticated targeting capabilities, can command a disproportionate share of the digital advertising market, further squeezing the Group's margins.

Mitigating actions

- Acceleration of digital transformation efforts, including AI-driven personalisation in content delivery.
- Investment in journalistic excellence and investigative reporting to maintain competitive differentiation.
- Expansion of subscription-based revenue models.
- Strengthened partnerships with content and technology providers.
- Anticipate consumer trends by using data analytics and market research to tailor product offerings and marketing strategies.

Nature of Risk

Climate Change

Environmental sustainability presents a growing strategic risk to the Group's long-term value and resilience. Climate change-driven extreme weather events can disrupt supply chains, damage infrastructure, and increase costs.

Stricter environmental regulations, carbon pricing, and resource scarcity further drive up operational expenses, impacting profitability.

Additionally, rising scrutiny on sustainability reporting demands greater transparency, with non-compliance risking fines, reputational damage, and limited access to capital. Failure to manage these risks effectively could weaken the Group's competitive position and long-term stakeholder value, requiring proactive adaptation to regulatory and market expectations.

Mitigating actions

- Invest in energy-efficient technologies and renewable energy to reduce emissions across operations.
- Partner with suppliers to cut supply chain emissions by sourcing locally, optimising logistics, and promoting sustainable practices. Prioritise vendors with strong environmental policies.
- Set clear carbon reduction targets to minimise the Group's footprint.
- Engage with communities, stakeholders, and policymakers to drive climate awareness, advocate for supportive policies, and collaborate on industry-wide initiatives.
- Assess and mitigate climate risks, developing resilience strategies for extreme weather, resource scarcity, and infrastructure impacts.
- Implement robust monitoring and reporting to track progress, ensuring transparency and compliance with evolving regulations.

Nature of Risk

Cyber Breach

The Group's operations rely heavily on secured storage, transmission, and processing of critical and sensitive data. This includes personally identifiable information and the intellectual property of our customers, as well as the essential editorial systems that underpin our publications.

Maintaining the security of customer data and the integrity of our editorial systems is paramount. However, we face escalating external threats, which are growing in sophistication and frequency. We are also aware of the potential for internal data breaches, whether accidental or malicious.

A significant breach of IT security or a system breakdown could lead to business disruption, reputational damage, litigation and loss of assets.

Mitigating actions

- Enhanced cybersecurity infrastructure, including advanced threat detection and multi-factor authentication (MFA).
- Mandatory staff training on phishing and social engineering tactics.
- Strengthened encryption protocols aligned with Malaysia's PDPA and Hong Kong's data protection regulations.
- Periodic penetration testing and continuous monitoring.
- Vendor risk assessments and cybersecurity insurance evaluations.
- Disaster recovery plans are in place to minimise disruption and ensure swift business recovery in the event of an incident.

INTERNAL AUDIT

The in-house Internal Audit ("IA") Function endeavours to enhance and protect the organisational value of the Group by providing a risk-based and objective assurance, advice and insight. The IA Function operates independently to evaluate and improve the adequacy and effectiveness of risk management, internal control systems and governance processes in a systematic and disciplined approach.

The annual internal audit plan, guided by the Internal Audit Charter, was formulated and presented to the Audit Committee for approval. The reviews conducted were designed to provide a reasonable assurance that risk management and internal control processes are in place and operating satisfactorily. For any significant gaps identified, the IA Function provides recommendations to the management to improve the design, process and procedure, where applicable. The head of IA has direct access to the Chairman of the Audit Committee, whenever deemed necessary and tabled reports to the Audit Committee quarterly.

OTHER INTERNAL CONTROL PROCESSES

Apart from the above, the other key features of the Group's internal control systems are as follows:

- The Group has established an organisational structure with clearly defined lines of roles and responsibilities, authority limits and accountability with periodic updates to align to businesses and operations requirements;

- Relevant executive directors and senior management have been delegated with specific authorities and responsibilities for monitoring the performance of designated business operating units;

- The Board reviews and approves the Group's business plans, operating and capital budgets annually. The Group's senior management meets monthly with operating companies' management to review their businesses and financial performances against the business plans and approved budgets. Key business risks relevant to each operating company are also periodically reviewed;

- Explanations of actual performance and significant variances against budgets are provided to the Board quarterly. This helps the Board and senior management to monitor the Group's business operations and plan on a timely basis to adapt to the changes in the business environment;

- Each operating company maintains internal controls and procedures appropriate to its structure and business environment whilst complying with the Group's policies, standards and guidelines;

- The Group maintains appropriate insurance programme to provide sufficient insurance coverage on its major assets and against libel suits that could result in material loss. The insurance brokers assist management in conducting a yearly risk assessment on the Group's operations, which helps the Group in assessing the adequacy of the insurance coverage;

- The Board reviews all areas of significant financial risk and approves all significant capital projects and investments after a detailed review and consideration;

- The Group has established IT Services Continuity Plans in key business units primarily aimed at handling potential IT service interruptions;

- The Group has established a Crisis Management Team in a key business unit to manage and handle significant risks or crises faced by the business unit;

- The treasury department manages the cash balances and exposure to currency transaction risks through treasury policies, risk limits and monitoring procedures;

- The Code of Conduct and Ethics serves as guiding principles for adherence by all the Group's employees on the high standards of conduct and ethical values in all business practices;

- The Group has implemented an Anti-Bribery and Corruption Policy which is regularly reviewed and updated. In adherence to this policy, the Group has implemented a range of control measures, such as conducting refresher Anti-Bribery and Corruption training and virtual self-learning video as a continuous staff awareness programme, assessing corruption risks in the company's risk profiles, requiring key managerial staff to make an annual declaration of conflicts of interest, and conducting continuous monitoring and review through the IA Function; and

- The legal department monitors compliance with relevant laws and regulations, including anti-bribery and corruption laws, which govern the Group's businesses.

WHISTLE BLOWING POLICY

The Group's Whistle Blowing Policy was revised and approved by the Board on 29 August 2024. The policy outlines the Group's commitment towards enabling its employees, as well as any third party who is not an employee, to raise concerns including but not limited to the Group's malpractices, wrongdoings or improprieties in financial reporting, accounting, auditing, internal controls, bribery or corruptions, sexual harassment, breach of confidentiality, breach of the Group's policies or failure to comply with legal or regulatory requirements. Proper arrangements have been put in place for the fair and independent investigation of such matters and with appropriate follow-up actions. All matters reported will be investigated and handled with strict confidentiality. The effectiveness of this policy is monitored and reviewed regularly by the Audit Committee.

REVIEW OF ADEQUACY AND EFFECTIVENESS

The Board has reviewed the adequacy and effectiveness of the Group's risk management framework and internal control activities to ensure that necessary actions have been or are being taken to rectify inadequacy or weaknesses identified during the year.

The Board has also received reasonable assurance from the Group CEO and the Head of Finance that the Group's system of risk management, internal control and preventive measures against corruption, in all material aspects, is operating adequately and effectively. For the financial year under review and up to the date of this Statement, there were no material control failures or adverse compliance events that have directly resulted in any material loss to the Group.

In this connection, the Board concludes that an effective system of risk management, internal control and preventive measures against corruption is in place to safeguard the shareholders' investment and the Group's assets.

REVIEW OF THIS STATEMENT BY THE EXTERNAL AUDITOR

As required by Paragraph 15.23 of the Bursa Malaysia Securities Berhad Main Market Listing Requirements, the external auditor has reviewed this Statement on Risk Management and Internal Control. Their limited assurance review was performed following Audit and Assurance Practice Guide ("AAPG") 3 issued by the Malaysian Institute of Accountants. AAPG 3 does not require the external auditor to form an opinion on the adequacy and effectiveness of the risk management and internal control systems of the Group.

This Statement on Risk Management and Internal Control was approved by the Board on 28 May 2025.