STATEMENT ON RISK MANAGEMENT AND INTERNAL CONTROL

IN ACCORDANCE WITH PARAGRAPH 15.26 (b) OF THE MAIN MARKET LISTING REQUIREMENTS OF BURSA MALAYSIA SECURITIES BERHAD (BURSA SECURITIES), THE BOARD OF DIRECTORS OF LISTED COMPANIES IS REQUIRED TO INCLUDE IN THEIR ANNUAL REPORT, A "STATEMENT ABOUT THE STATE OF RISK MANAGEMENT AND INTERNAL CONTROL OF THE LISTED ISSUER AS A GROUP". THE MALAYSIAN CODE ON CORPORATE GOVERNANCE ISSUED BY SECURITIES COMMISSION MALAYSIA REQUIRES THE BOARD TO ESTABLISH AN EFFECTIVE RISK MANAGEMENT AND INTERNAL CONTROL FRAMEWORK. DIGI'S BOARD OF DIRECTORS (BOARD) IS PLEASED TO PROVIDE THE FOLLOWING STATEMENT PREPARED IN ACCORDANCE WITH THE "STATEMENT ON RISK MANAGEMENT AND INTERNAL CONTROL: GUIDELINES FOR DIRECTORS OF LISTED ISSUERS" ENDORSED BY BURSA SECURITIES. THE STATEMENT OUTLINES THE FEATURES OF DIGI'S RISK MANAGEMENT AND INTERNAL CONTROL FRAMEWORK, AND THE ADEQUACY AND EFFECTIVENESS OF THIS FRAMEWORK DURING THE FINANCIAL YEAR UNDER REVIEW.

RESPONSIBILITIES AND ACCOUNTABILITIES

The Board acknowledges its responsibility for establishing and overseeing Digi's risk management framework and internal control systems. The risk management framework is designed to identify, assess and manage risks that may impede the achievement of business objectives and strategies. The Board also acknowledges that the internal control systems are designed to manage and minimise, rather than eliminate, occurrences of material misstatement, financial losses or fraud.

The Board, through the Audit and Risk Committee (ARC), ensures that the risk management and internal control practices are adequately implemented within Digi, and observes that measures are taken in areas identified for improvement, as part of Management's continued efforts to strengthen the effectiveness of Digi's risk management and internal control system.

Management is responsible for implementing Board approved policies and procedures on risk management and internal controls by identifying and evaluating risks faced and monitoring the achievement of business goals and objectives within the risk appetite parameters.

RISK MANAGEMENT

Digi's risk management framework provides the foundation and process on how risks are managed across the Company. The process in place is broadly based on ISO 31000:2009 and aims to identify, evaluate and respond to risks that may impede the achievement of Digi's plans and business objectives.

The responsibilities of the Risk Management function, as defined in the framework, are to implement the enterprise risk management process through identifying, monitoring, reporting and/or escalating risks which may impact business objectives. The ARC and Board take an oversight role to review and deliberate on Digi's top risks. Digi's Management is responsible to identify significant risks, evaluate the organisation's risk profile and drive risk responses on a regular basis. All line managers are required to assume responsibility for risk management within their areas of responsibility and ensure that risk management is embedded in their day-to-day business processes.

STATEMENT ON RISK MANAGEMENT AND INTERNAL CONTROL CONTINUED

As part of the continuous improvement efforts to strengthen Digi's risk management processes, the effectiveness of risk practises were reviewed. Various enhancements were implemented to ensure more systematic risk identification, monitoring and reporting of new, existing and evolving risks.

Following are the key risks areas reported by Management and discussed with the ARC and Board in the financial year. Appropriate risk responses and strategies have been identified and taken to mitigate the risk exposures. As these key risks are still relevant, status of mitigations are monitored and reported to Management regularly, with oversight reporting to the ARC and Board providing them the visibility and status of key risks across Digi.

Market Risk

Digi operates in a market highly challenged by constant price competition from existing and new operators in the industry. In addition, there is also increased competition from a variety of technology and digital service providers as consumer behaviour and expectations evolve. Failure to respond to these dynamics and drive change to meet consumers' evolving demands will impact Digi's service offerings, key revenue streams and position in the market.

Financial Risk

The main risks arising from the normal course of business are foreign exchange, interest rates, liquidity and credit risks. Clearly documented policies, guidelines and control procedures are important to manage and report exposure of these risks with the objective of preserving Digi's profitability. Other challenges or uncertainties which may cause adverse impact on Digi's cash flow and financial performance includes specific taxes, spectrum fees, and penalties.

Regulatory Risk

Digi's operations are subject to various regulatory requirements like licensing, spectrum, numbering and access regulation requirements. In addition, regulatory bodies may introduce new or reform existing rules or policies to drive industry growth. If Digi fails to fulfil any of these regulatory requirements or developments, it could have a material impact on business prospects, market perception and financial performance.

Legal & Compliance Risk

Digi is required to comply with a multitude of laws and requirements by various governing authorities. These include customer registrations, data privacy and protection, competition law, accounting and financial standards. Non-compliance to these requirements could result in fines or other penalty like revocation of licenses.

Operational Risk

The provision of Digi's services depends on the quality and stability of the network and systems hence there is a risk of service interruptions or outages. In addition, Digi's network and IT systems are also vulnerable to internal and external cyber security attacks that can cause disruptions to the network and services provided to consumers as the company moves into new technologies such as cloud computing, integration of various technologies; and increased used of mobile devices.

Other operational risk which may threaten Digi's reputation and credibility is data privacy risk. Due to the rapid growth, and usage of smart and connected devices, vast amounts of confidential consumer and business data are generated. Loss, mismanagement or unauthorised disclosure of these consumers' personal data may undermine consumer confidence and/or result in regulatory fines and penalties.

1. Control Activities

- **Policies and Procedures**

  Digi has documented policies and manuals that set formal standards on how we operate as a company. It serves to ensure that Digi complies with relevant laws and risks are adequately mitigated, whilst providing guidance and direction for proper management and governance of operations and business activities. These policies and manuals are communicated company-wide and made available on the intranet for employees.

- **Profitability Assurance**

  The Profitability Assurance function carried out by the Business Planning department ensures that revenue leakage is minimised by implementing adequate controls and processes through an optimal revenue management framework. It covers the cycle of identification, assessment, mitigation and monitoring. Digi has in place automated controls to ensure that usage and profile integrity between the network, mediation, rating and billing is assured and adequately controlled. Key issues and mitigation actions are reported to Management monthly. The effectiveness and efficiency of processes and controls within the revenue cycle are reviewed regularly. In addition to assuring minimal revenue leakage, the team also monitors site and store profitability, providing key feedback to optimise the management of Digi's key assets.

- **Security**

  The Security department is responsible for compliance investigations, fraud management, authority requests, information security and physical security.

  The Fraud Management function manages and mitigates the risk of relevant fraud and related losses. Some of its key activities involve developing and designing internal fraud controls which are regularly reviewed to ensure relevance and effectiveness. Measures and continuous actions are taken to ensure telecommunication fraud is minimised and the requirement for preventive controls are embedded into business processes.

  The Information Security and Physical Security functions are responsible for achieving and maintaining confidentiality, integrity and availability of information and information processing facilities, including telecommunication systems and infrastructure and to protect against cyber-crime, fraudulent activities, information loss and other security risks and threats.

- **Controls over Financial Reporting**

  The Controls over Financial Reporting (CFR) function in the Accounting and Risk Management department plays an important role in evaluating and improving effectiveness of key controls surrounding Digi's financial reporting process. Its primary objective is to provide reasonable assurance regarding the reliability of financial reporting and preparation of financial statements. Reviews on internal controls over financial reporting is performed in accordance to Digi's Internal CFR Framework, which requires assessment on significant accounts based on materiality level; testing and evaluation of the design and operational effectiveness of key controls. The function adopts a continuous monitoring routine to follow up on unaddressed risks and non-operating controls, including periodic reporting to Management and the ARC on the status of controls on the financial reporting processes.

STATEMENT ON RISK MANAGEMENT AND INTERNAL CONTROL CONTINUED

2. Authority

- **Organisation Structure**

  Digi's well-defined organisational structure ensures clear lines of reporting, proper segregation of duties, assignment of authority and accountability within the organisation. Aligned to Digi's long-term ambitions, the organisation structure was refreshed to strengthen the overall ability to deliver on the company's next phase of growth. In June 2017, the Network and IT divisions converged to form a larger, more cohesive Technology division to solidify overall technical competencies and services delivery. This division is led by the Chief Technology Officer. In August 2017, a new Chief Financial Officer was appointed to further strengthen the Finance organisation with innovative practices to support Digi's digital ambitions.

- **Board and Management Committees**

  Board Committees have been set up to assist the Board to perform its oversight function, namely the ARC, Nomination Committee, and Remuneration Committee. These Board Committees have been delegated specific responsibilities all of which are governed by clearly defined Terms of Reference. The Terms of Reference of these Committees are accessible in the Corporate Governance section of Digi's website at www.digi.com.my/investors.

  Various Management Committees comprising key Management members have been established to oversee the areas of business operations assigned to them under their respective documented mandates. The Committees are:

  - The Vendor and Investment Committee (VIC) governs the approval process regarding material capital investments and operating expenditure for Digi including the review and approval of the vendor evaluation criteria and vendor selection. The VIC meets once every two weeks and is chaired by the Investment Controller with selected Management as participants of the Forum.
  - The Regulatory Steering Committee (RSC) provides direction and makes decisions on regulatory matters and/or related topics that have a significant impact to Digi. The RSC meets monthly, and is chaired by the CEO with key Management as RSC members.
  - The Risk Management Forum reviews and deliberates on the significant risks reported across Digi and makes decisions on the coordinated action plans necessary to mitigate risks. The quarterly Forum is chaired by the CFO with selected Management participating as Forum members.

- **Assignment of Authority**

  Digi has an established Delegation Authority Matrix (DAM) to provide a framework of authority and accountability. The DAM outlines approval authority for strategic, capital and operational expenditure. The DAM is reviewed and approved by the Board in line with changes in business needs.

3. Ethics and Compliance

- **Code of Conduct**

  The Code of Conduct (the Code) is a vital and integral part of Digi's governance regime that defines the core principles and ethical standards in conducting business and engagements with all stakeholders, and compliance with relevant law and regulations. The Code applies to the members of the Board, employees and those acting on behalf of Digi. All employees are required to sign and confirm that they have read, understood and will adhere to the Code. The Company has established communication channels that allow concerns of non-adherence to the Code to be anonymously reported.

- **Compliance**

  The Ethics and Compliance Officer supports the CEO and the Board in ensuring that:

  - The Code reflects good business practices and relevant laws, regulations and widely recognised treaties.
  - The Code is implemented consistently and effectively through the sharing of knowledge and measures for quality assurance.
  - Compliance incidents are consistently and effectively managed.

Reports on material breaches of the Code are made to the ARC on a quarterly basis.

4. Monitoring

- **Management and Board Oversight**

  Management meetings are held on a weekly basis to identify, discuss, approve and resolve strategic, operational, financial and key management issues pertaining to Digi's day-to-day business. Significant changes in the business and the external environment are reported by the Management to the Board on an on-going basis and/or during Board meetings.

- **Internal Audit Function**

  The Internal Audit department is independent as it has no involvement in Digi's operations and reports directly to the ARC. The Internal Audit function thereby provides independent assurance on the effectiveness of Digi's internal control system. The purpose, authority and responsibility of the Internal Audit department are reflected in the Internal Audit Charter, which is reviewed and approved by the ARC annually.

  The Internal Audit department assists both the ARC and Board by conducting reviews of key business processes to assess the adequacy and effectiveness of internal control and risk management, and compliance with regulations and Digi's policies and manuals. The audit reports, including significant findings and recommendations for improvements, and Management's responses to the recommendations are highlighted to Management and reported to the ARC on a quarterly basis. Implementation status of actions taken by Management to address improvement areas highlighted is also monitored by the ARC to ensure they are addressed timely.

  The Internal Audit department's activities and practices conform to The Institute of Internal Auditor's International Standards for the Professional Practice of Internal Auditing.

  Further information on the Internal Audit department's activities are detailed in the Audit and Risk Committee Report on pages 79 to 82 of this Annual Report.

STATEMENT ON RISK MANAGEMENT AND INTERNAL CONTROL CONTINUED

REVIEW OF THIS STATEMENT BY EXTERNAL AUDITORS

The external auditors have performed limited assurance procedures on this Statement on Risk Management and Internal Control pursuant to the scope set out in Recommended Practice Guide (RPG) 5 (Revised), Guidance for Auditors on Engagements to Report on the Statement on Risk Management and Internal Control included in the Annual Report issued by the Malaysian Institute of Accountants (MIA) for inclusion in the Annual Report of the Group for the year ended 31 December 2017, and reported to the Board that nothing has come to their attention that cause them to believe the statement intended to be included in the Annual Report is not prepared, in all material respects, in accordance with the disclosures required by paragraphs 41 and 42 of the Guidelines, nor is the Statement factually inaccurate.

RPG 5 does not require the external auditors to consider whether the Directors' Statement on Risk Management and Internal Control covers all risks and controls, or to form an opinion on the adequacy and effectiveness of the Group's risk management and internal control system including the assessment and opinion by the Directors and Management thereon. The report from the external auditor was made solely for, and directed solely to the Board of Directors in connection with their compliance with the listing requirements of Bursa Malaysia Securities Berhad and for no other purposes or parties. The external auditors do not assume responsibility to any person other than the Board of Directors in respect of any aspect of this report.

CONCLUSION

The Board has received assurance from the CEO and CFO that Digi's risk management and internal control framework is operating adequately and effectively, in all material aspects, during the financial year under review and up to the date of this Statement. Taking into consideration the assurance from Management and relevant assurance providers, the Board is of the view that the risk management and internal control practices and processes are operating adequately and effectively to safeguard the shareholders' investment, customer's interests, and Digi's assets.