Digital Strategy Group

1. Purpose of Charter

The Board has established a Digital Strategy Group, which reports to the Board. The purpose of this Charter is to set out the roles and responsibilities as well as the structure, composition and membership of the Digital Strategy Group.

2. Role and Responsibilities of the Digital Strategy Group

The role of the Group is to assist the Board in fulfilling its corporate governance responsibilities with regards to:

- Oversight of appropriate levels of investment in infrastructure and people as it relates to digital strategy and innovation, to continue to drive the combination of imagination, courage and capital that will excite our customers and deliver returns for our shareholders.
- The reliability and integrity of digital operations across people, processes and technology with the ultimate aim of striving of being the world's leading retailer of products to our customers.
- Internal and external service levels across technology infrastructure including online sales, websites, online customer service and fulfilment.
- Review of cyber security and risk management as it relates to digital operations, including 3rd party logistics and fulfilment providers.
- Evaluation of incident response and disaster recovery plans in the event of a fault or failure across digital operations and infrastructure.
- Systems and processes for the collection, security and use of customer data across the businesses.
- Review and support of an innovation agenda and focus on what is next to both futureproof our business and better serve our customers across the Group.

3. Membership

The Group is appointed by the Board. The Board shall appoint the Group from time to time and review the composition of the Group annually.

The following rules apply to the membership of the Group:

- There will be at least three members, all of whom are non-executive Directors and a
- majority of whom are independent Directors;
- All members will be financially literate;
- At least one member must be a qualified and experienced digital technology expert; and
- The Chair Group must be an independent Director who is not also Chairman of the Board.

It is the responsibility of the Chair of the Group (with the assistance of the Company Secretary) to schedule all Group meetings and to provide the Group members with a written agenda.

The Company Secretary is to attend all Group meetings to ensure minutes are taken of each meeting.

4. Meetings

The Group will meet as frequently as required to undertake its role effectively and, in any event, at least 6 times per annum. Additional meetings may be requested through the Group Chair by any member, the Company Secretary, or the relevant partner from the external auditor. A quorum for a Group meeting is two members. Each member will have one vote and the Chair of the Group will not have a second or casting vote.

Recommendations of the Group are to be referred to the Board for approval.

5. Access to Information and Independent Advice

The Group has the authority to seek any information it requires from any employee of the Company and all employees must comply with any such reasonable requests. The Group has the right to obtain information, interview management and internal and external auditors (with or without management present).

The Group may seek such independent legal, financial or other advice as it considers necessary or appropriate.

6. Duties and Responsibilities

Overview

The function of the Group is oversight. Group members are entitled to rely on Management for matters within their responsibility and on external professionals on matters within their areas of expertise. Group members may assume the accuracy of information provided by such persons, so long as the members are not aware of any reasonable grounds upon which such reliance or assumption may not be appropriate.

Management is responsible for:

- The preparation, presentation and integrity of the Group's cyber security reports;
- Implementing, managing and maintaining appropriate enterprise-wide cyber security processes, including penetration testing, training of staff and application of software security updates;
- Implementing, managing and maintaining appropriate disaster recovery processes, systems, policies and procedures, reporting protocols and internal controls;
- Implementing and maintaining a ticket management system for both internal and external customer service requests, and managing the Service Level Agreement within defined thresholds; and
- The preparation, presentation and integrity of the information provided to the Group, including regular summarised progress updates to the Board or Group on how the above issues and risks (including tax) are trending.

Management can employ an external 3rd party for security and penetration testing. The Board is responsible for ensuring the integrity and independence of any 3rd party security auditor.

Understanding the Business

The Group should understand the Company's structure and operations in order to be in a position to confirm with Management:

- the reliability and integrity of information;
- the integrity of the Group's internal controls;

- the structure and compliance with audit, accounting and financial reporting obligations;
- that the significant enterprise-wide risks faced by the Company have been identified; and
- that appropriate mitigation plans have been implemented.

Enterprise-wide Risk Management

The Group confirms that Management has established and operates an enterprise-wide risk management system which is designed to identify, assess, monitor and manage risk throughout the Group. On a periodic basis, but not less than once per annum, management is required to provide the Group with a paper detailing each organisational risk identified, its potential impact on the business and the risk mitigation strategies employed.

The Group uses this reporting as a basis for ensuring that enterprise-wide risk is properly managed. Moreover, at each meeting of the Board, Management is required to notify the Board of any changes to the underlying risk profile of any risk item and/or whether or not any new risk items have been identified.

The Group will:

- Review the Company's assessment of material risks and form an opinion on the adequacy and effectiveness of the risk assessment.
- Consider the effectiveness of the Company's internal controls and relevant reports from the external auditor.
- Review the Company's risk profile as developed by Management and monitor emerging risks and changes in the Company's risk profile.
- Report any material changes in risk profile to the Board.
- Where the Group identifies opportunities to create value by taking on further or different risks, make recommendations to the Board on the strategies that could be undertaken to capitalise on the identified opportunities.

Evaluation of Policies and Controls

The Group will consider the adequacy and effectiveness of the Company's administrative, operating, policies and internal control framework through communication with Management.

To assist in the Group's oversight of the Company's internal control framework, Management will carry out or engage parties to carry out periodic internal control testing to assure the Board that the internal control framework (for the abovementioned matters) is robust and report on these matters to the Group on a periodic basis.

Assessment of Systems of Digital Risk Management and Internal Control

The Group will:

- Discuss with Management and the external digital and technology security auditor the Company's infrastructure, operational and process controls, including the policies and procedures to assess, monitor and supervise digital risk and compliance programs for the purpose of forming a view as to the effectiveness of these controls, policies, procedures and programs.
- Discuss with management the Company's technology and digital processes, policies and methods for the purpose of forming a view as to the appropriateness (as opposed to the acceptability) and objectivity of these policies and methods.

- Review all reports produced by the external technology auditor and Management's response to the matters raised therein and become satisfied that they applied properly maintained in accordance with statutory requirements.
- Obtain reports from time to time on the critical technology, digital and cyber policies and practices of the Company that have been discussed with Management.
- Make any recommendations to the Board, as appropriate, in connection with the items listed above.

Legal and Regulatory Compliance
The Group will, in conjunction with the Board, monitor the Group's compliance with all relevant statutory and regulatory obligations relating to technology and digital operations, including the Company's continuous disclosure obligations and all internal policies and procedures.

The Group will consider the effects on the Company of any new or proposed technology or digital practices, principles or developments, disclosure requirements and legislative or regulatory requirements.

The Group will:

- Require the external technology auditor to confirm in writing that they have complied with all professional and regulatory requirements relating to auditor independence prior to the completion of each year's accounts. The report will also delineate all relationships between the external auditor and the Company and describe the external auditor's internal quality control procedures. The report is an addition to any other declaration that the external auditor must provide pursuant to the Corporations Act.

On an annual basis, the Group will review a report from the external technology auditor describing:

- any material issues raised by the most recent quality control, or peer review, and any steps taken to deal with any such issues; and
- all relationships between the external auditor and the Company or Management (to assess the auditor's independence).

Prohibited Services from an External Auditor
It is noted for clarity that the Group's external auditor, as appointed by the Audit and Risk Group, must not perform management consulting, IT systems design or implementation, valuation services (except where related solely to tax affairs), bookkeeping, accounting and payroll services, broker, dealer or investment advisory services, litigation or legal advocacy services, recruitment and human resource services, internal audit services, actuarial services, acquisition valuations or valuations for purchase price allocations, fairness opinions and preparation of sale documentation.

7. Annual Review

To determine whether it is functioning effectively, once each year:

- The Group's performance and effectiveness will be evaluated;
- The Group's membership will be reviewed; and
- This charter will be reviewed.