

**NCC GROUP PLC**  
**("Company")**

**CYBER SECURITY COMMITTEE: TERMS OF REFERENCE**  
**(Approved 18 July 2022)**

**1. Definitions**

In these terms of reference:

- **"Board"** means the Board of Directors of the Company;
  - **"Committee"** means the Cyber Security Committee of the Board;
- and
- **"Group"** means the Company and its subsidiaries.

**2. Membership**

- 2.1 The Committee shall comprise at least three members. Members of the Committee shall be appointed by the Board on the recommendation of the Nomination Committee and in consultation with the Chair of the Committee.
- 2.2 The Director of Global Governance, the Global Chief Information Security Officer ("**GCISO**"), and the Chief Data Protection & Governance Officer ("**CDPGO**") shall be standing attendees. Only members of the Committee have the right to attend Committee meetings. However, other individuals may be invited to attend for all or part of any meeting, as and when appropriate and necessary.
- 2.3 Appointments to the Committee shall be for a period of up to three years, which may be extended for further periods of up to three years, provided the director still meets the criteria for membership of the Committee.
- 2.4 The Board, on the recommendation of the Nomination Committee, shall appoint the Chair of the Committee, who shall either be the Company Chair or an independent non-executive director of the Company. In the absence of the Chair of the Committee and/or an appointed deputy, the remaining members present shall elect one of their number to chair the meeting.

**3. Secretary**

The Company Secretary, or his/her nominee shall act as the Secretary of the Committee.

**4. Quorum**

The quorum necessary for the transaction of business shall be two members. A duly convened meeting of the Committee at which a quorum is present shall be competent to exercise all or any of the authorities, powers and discretions vested in, or exercisable by the Committee.

**5. Frequency of meetings**

The Committee shall meet at least three times a year at appropriate times and as otherwise required.

## **6. Notice of meetings**

- 6.1 Meetings of the Committee shall be summoned by the Secretary of the Committee at the request of any of its members or the Director of Global Governance.
- 6.2 Unless otherwise agreed, notice of each meeting (confirming the venue, time and date, together with an agenda of items to be discussed) shall be forwarded to each member of the Committee, any other person required to attend and all other non-executive directors no later than five working days before the date of the meeting (where reasonably practicable). Supporting papers shall be sent to Committee members and to other attendees, as appropriate, at the same time.

## **7. Minutes of meetings**

- 7.1 The Secretary of the Committee shall minute the proceedings of Committee meetings, including recording the names of those present and in attendance.
- 7.2 Draft minutes of Committee meetings shall be circulated promptly to all members of the Committee and, once agreed, to all other members of the Board, unless it would be inappropriate to do so.

## **8. AGM**

The Chair of the Committee shall attend the AGM prepared to respond to any shareholder questions on the Committee's activities.

## **9. Duties**

The Committee shall:

- 9.1 Oversee and advise the Board on the current cyber and data security risk landscape and exposure of the Group and future cyber and data security risk strategies, providing oversight of, but not limited to:
- Cyber security
  - Global data protection legislation and regulation
  - System and data security and integrity
  - IT disaster recovery
  - IT change management
- 9.2 Be appraised of, and review the effectiveness of the Group's ability to identify, monitor and manage new cyber and data security risks;
- 9.3 Regularly review the cyber risk posed by third parties including outsourced IT providers and other third-party partners;
- 9.4 Review at least annually the adequacy of the Group's cyber security breach response plan, through:
- Planned response exercises
  - Providing challenge to lessons learned
  - Sponsor and support corrective actions, where deemed appropriate
- 9.5 Have oversight of, and review reports related to any cyber or IT security incidents, the status of risk profiles and the adequacy and status of lessons learned and proposed actions;
- 9.6 Have oversight of, and review reports related to data security incidents and

breaches and the adequacy and status of lessons learned and proposed actions;

- 9.7 Approve and have oversight over the cyber security assurance programme to support the identification of risks and provide direction in strategy and investment;
- 9.8 Review and consider regular update reports from the GCISO and CDPGO;
- 9.9 Provide a supportive environment to facilitate the right of direct access to the Committee by the GCISO and CDPGO;
- 9.10 Consider and recommend actions in respect of all cyber and data security risk issues escalated by the GCISO and CDPGO, or other colleagues as appropriate;
- 9.11 Review the effectiveness of the Company's IT control environment, related to service and product offerings to analyse potential vulnerabilities that could be exploited;
- 9.12 Periodically review and assess what are the Group's most valuable intangible assets and the most sensitive Group and customer information and assess whether the controls in place sufficiently protect those assets and information;
- 9.13 Assess the adequacy of resources and funding for cyber and data security activities;
- 9.14 Oversee cyber security due diligence undertaken as part of an acquisition and advise the Board of the risk exposure and related action plans; and
- 9.15 Annually review and assess the adequacy of the Group's cyber insurance cover.

## **10. Other matters**

The Committee shall:

- 10.1.1 Have access to sufficient resources in order to carry out its duties, including access to the Company Secretariat for assistance as required;
- 10.1.2 Be provided with appropriate and timely training, both in the form of an induction programme for new members and on an on-going basis for all members; and
- 10.1.3 Oversee any investigation of activities which are within its terms of reference.

## **11. Reporting responsibilities**

- 11.1 The Chair of the Committee shall report formally to the Board on its proceedings after each meeting on all matters within its duties and responsibilities.
- 11.2 The Committee shall make recommendations to the Board it deems appropriate on any area within its remit where action or improvement is needed.
- 11.3 The Committee shall produce an annual report to shareholders on its activities, which will form part of the Company's annual report and accounts.

## **12. Self-appraisal**

The Committee shall, at least once a year, review its own performance, constitution and terms of reference to ensure it is operating effectively, and recommend any changes it considers necessary to the Board for approval.

**13. Authority**

The Committee is authorised by the Board to:

- 13.1 Seek any information it requires from any employee of the Company in order to perform its duties;
- 13.2 Obtain, at the Company's expense, outside legal or other professional advice on any matters within its terms of reference; and
- 13.3 Call any employee to be questioned at a meeting of the Committee as and when required.