NCC GROUP PLC
("Company")

CYBER SECURITY COMMITTEE: TERMS OF REFERENCE
(approved 21 May 2020)

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 chairman of the Committee.

2.2 The Director of Global Governance, the Chief Information Security Officer ("**CISO**"), and the Data Protection Officer ("**DPO**") 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 chairman of the Committee, who shall be either the Company chairman or an independent non-executive director of the Company. In the absence of the chairman 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 CISO.

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 chairman 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 risk exposure of the Group and future cyber risk strategy, providing oversight of IT centric related risks, including cyber, GDPR, system and data security and integrity, IT disaster recovery and IT change management;

9.2 review at least annually the Group’s cyber security breach response plan;

9.3 review reports on any cyber or IT security incidents and the status of risk profiles and the adequacy and status of proposed actions;

9.4 receive and consider the regular reports from the CISO and DPO;

9.5 ensure the CISO and DPO are given the right of direct access to the Committee;

9.6 consider and recommend actions in respect of all cyber risk issues escalated by the CISO and DPO, or other colleagues as appropriate;

9.7 keep under review the effectiveness of the Company’s controls, services and products to analyse potential vulnerabilities that could be exploited;

9.8 regularly 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;

9.9 review the Group’s ability to identify and manage new cyber risks;

9.10 assess the adequacy of resources and funding for cyber security activities;

9.11 regularly review the cyber risk posed by third parties including outsourced IT and other partners;

9.12 oversee cyber security due diligence undertaken as part of an acquisition and advise the Board of the risk exposure; and

9.13 annually 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 chairman 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 whatever 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 at maximum effectiveness, and recommend any changes it considers necessary to the Board for approval.

13. Authority

The Committee is authorised by the Board:

13.1 to seek any information it requires from any employee of the Company in order to perform its duties;

13.2 to obtain, at the Company's expense, outside legal or other professional advice on any matters within its terms of reference;

13.3 to call any employee to be questioned at a meeting of the Committee as and when required.