D-WAVE QUANTUM INC.

CYBERSECURITY COMMITTEE CHARTER

I. Purpose

The Cybersecurity Committee (the "Committee") of the Board of Directors (the "Board") of D-Wave Quantum Inc., a Delaware corporation (the "Company"), shall assist the Board in its oversight responsibilities with respect to the Company's information technology systems (i.e., strategies, assessments, capabilities, processes, policies, controls and procedures) to:

(a) Regularly identify, assess and manage cybersecurity and privacy risks to the Company's technology and information systems and other critical assets, as well as to the confidential or personal information of the Company, its customers and its partners;

(b) respond to and manage material cybersecurity threats, including material cybersecurity incidents; and

(c) comply with legal and regulatory requirements governing cybersecurity, in collaboration with the Audit Committee.

II. Organization

The Committee shall consist of two or more directors, each of whom shall satisfy the applicable independence requirements of the Company's corporate governance guidelines, the securities exchange on which the Company's securities are listed (the "Applicable Securities Exchange"), and any other applicable regulatory requirements.

Members of the Committee shall be appointed by the Board on the recommendation of the Nominating and Governance Committee and may be removed by the Board at any time. The Committee's chair shall be designated by the Board on the recommendation of the Nominating and Governance Committee or, if not so designated, the members of the Committee shall elect a chair by a vote of the majority of the full Committee.

III. Meetings

The Committee shall meet at least four times per year on a quarterly basis or more frequently as circumstances require. Meetings shall be called by the chair of the Committee or, if there is no chair, by a majority of the members of the Committee. Any member of the Committee may participate in a meeting by means of conference telephone or other communications equipment by means of which all persons participating in the meeting can hear each other, and participation in a meeting by such means shall constitute presence in person at such meeting. Committee actions may also be taken by unanimous written consent.

The Committee may invite any other individuals to attend meetings of the Committee, as it considers appropriate. The Committee shall have access to professional advice from employees of the Company (including the chief financial officer, the chief information and security officer, the head of the Company's IT department or other person responsible for managing the Company's information security and cybersecurity), and from any Advisors (as defined in Section V below), as the Committee considers appropriate.

IV. Authority and Responsibilities

In fulfilling its duties and responsibilities hereunder, the Committee will be entitled to rely reasonably on the integrity of those persons within the Company and the professionals and experts from whom it receives information. To fulfill its responsibilities, the Committee shall:

1. Review with management on a periodic basis the Company's enterprise cybersecurity strategy and framework, including the Company's assessment of cybersecurity threats and risk, the framework for the materiality determination of cybersecurity incidents, data security programs (including data management systems and controls over Company data and systems to protect customer and other third-party data, including confidential information in the Company's possession or custody) and the Company's management and mitigation of cybersecurity and information technology risks and potential breach incidents.

2. Review with management any material cybersecurity incident and other significant cybersecurity incident as determined by the chief information and security officer and chief executive officer that has occurred, reports to or from regulators with respect thereto and steps that have been taken to mitigate against reoccurrence.

3. Evaluate the effectiveness of the Company's cyber risk management and data security programs measured against the Company's cybersecurity threat landscape, including the following program components: cybersecurity risk monitoring, effectiveness testing, integrity of information security systems and controls, implementations of new cyber technology programs, adequacy of resources and security awareness training, redundancy measures and any other safeguards used to protect the confidentiality, integrity, availability and resiliency of the Company's products, services, intellectually property and business operations.

4. In collaboration with the Audit Committee, oversee the Company's compliance with legal and regulatory requirements related to cybersecurity, including reviewing and discussing with management the applicable laws and regulations, as well as significant legislative and regulatory developments, that could materially impact the Company's cybersecurity risk exposure. Evaluate the integrity of the Company's information technology systems, processes, policies and controls to oversee compliance with applicable legal and regulatory requirements.

5. Review and discuss as appropriate with management the Company's disclosures relating to cybersecurity risks, incidents or governance.

6. Assess the effectiveness of the Company's Incident Response Plan, including detection, disclosure, investigation, remediation and post incident security measures.

7. Review with management on a periodic basis and assess the Company's information technology disaster recovery and business continuity capabilities.

8. Review and assess the Company's cybersecurity risk systems against industry benchmarks and best practices, and, after consultation with management and, if any, its Advisors, make recommendations to management on enhancements. Receive reports from management on cybersecurity and data management assessments, surveys, audits and examinations that management shall direct third-party experts to conduct on a periodic basis.

9. Receive on a periodic basis reports on the metrics used to measure, monitor and manage cyber risks posed to the Company, including those related to potential cybersecurity incidents.

10. Review the Company's information security planning and resources to manage changes in the Company's cybersecurity threat landscape. Assess the potential impact of cybersecurity risk on the Company's business, operations and reputation.

11. Review with management the Company's assessment of cybersecurity threats and risk associated with the Company's supply chain and third party risks, as well as actions the Company is taking to address such threats and risks.

12. Annually review and assess the appropriateness and adequacy of the Company's cyber insurance coverage.

13. Annually review and assess the adequacy of this Charter and recommend to the Board any changes deemed appropriate by the Committee.

14. Annually review its own performance.

15. In conjunction with management, report regularly to the Board.

16. Perform any other activities consistent with this Charter, the Company's by-laws and governing law, as the Committee or the Board deems necessary or appropriate.

V. Resources

The Committee shall have the authority, at its sole discretion, to retain or terminate independent legal counsel or any other advisors, consultants or professionals (collectively, the "Advisors") to assist the Committee in its responsibilities and shall be directly responsible for overseeing the work of such Advisors.

The chair of the Committee, at the request of any member of the Committee, may request that any officer, employee or advisor of the Company attend a meeting of the Committee or otherwise respond to Committee requests.

The Committee shall have the sole authority to determine the terms of engagement and the extent of funding necessary (and to be provided by the Company) for payment of (a) compensation to any Advisors retained to advise the Committee and (b) ordinary administrative expenses of the Committee that are necessary or appropriate in carrying out its duties.