

**CHARTER OF THE CYBERSECURITY RISK MANAGEMENT COMMITTEE**  
**OF THE BOARD OF DIRECTORS OF**  
**ZOOM VIDEO COMMUNICATIONS, INC.**

(Adopted on May 26, 2021)

**PURPOSE**

The purpose of the Cybersecurity Risk Management Committee (the "**Cybersecurity Committee**") of the Board of Directors (the "**Board**") of Zoom Video Communications, Inc., a Delaware corporation (the "**Company**"), shall be to assist the Board in fulfilling its oversight responsibility with respect to the management of risks related to the Company's information technology use and protection, cybersecurity, and product security.

**COMPOSITION**

- 1. Membership and Appointment.** The Cybersecurity Committee shall consist of at least two (2) members of the Board. Members of the Cybersecurity Committee shall be appointed by the Board and may be removed by the Board in its discretion.
- 2. Chairperson.** The Board may designate a chairperson of the Cybersecurity Committee. In the absence of that designation, the Cybersecurity Committee may designate a chairperson by majority vote of the Cybersecurity Committee members; provided that, the Board may replace any chairperson designated by the Cybersecurity Committee at any time.

**RESPONSIBILITIES**

The following are the principal recurring responsibilities of the Cybersecurity Committee. The Cybersecurity Committee may perform such other functions as are consistent with its purpose and applicable law, rules and regulations and as the Board may request.

- 1. Information Technology and Network Systems.** The Cybersecurity Committee shall oversee the quality and effectiveness of the Company's policies and procedures with respect to its information technology and network systems, including encryption, network security and data security, as well as access to such systems.
- 2. IT/Engineering Security Funding.** The Cybersecurity Committee shall oversee the Company's information technology senior management team relating to budgetary priorities based, in part, on assessing risk associated with various perceived threats.
- 3. Incident Response.** The Cybersecurity Committee shall review and provide oversight on the policies and procedures of the Company in preparation for responding to any data security incidents.
- 4. Disaster Recovery.** The Cybersecurity Committee shall review periodically with management the Company's disaster recovery, business continuity, and business resiliency capabilities.
- 5. Compliance Risks and Audits.** The Cybersecurity Committee shall oversee the Company's management of internal and external risks related to its information technology systems and

processes, including encryption, network security, data security, risk management frameworks, and any internal or third party audits of such systems and processes.

6. **Access Controls.** The Cybersecurity Committee shall review with management the quality and effectiveness of IT systems and processes that relate to the Company's internal access control systems, including physical, organizational, and technical security.
7. **Cyber Insurance.** The Cybersecurity Committee shall review the Company's cyber insurance policies to ensure appropriate coverage.
8. **Product Security.** The Cybersecurity Committee shall review periodically with management the risks related to the security of and access to customer data through use of the Company's products and services.

The function of the Cybersecurity Committee is primarily one of oversight. The members of the Cybersecurity Committee are not employees of the Company, and they do not perform management's functions with respect to the Company's information technology and network systems, including cybersecurity. The Cybersecurity Committee relies on the expertise and knowledge of management in carrying out its oversight responsibilities. It is not the Cybersecurity Committee's responsibility to manage the Company's systems, or ensure that the information technology and network systems and the Company's products and services are complete and effective, conform to applicable standards, or otherwise comply with applicable laws and the Company's policies.

## **MEETINGS AND PROCEDURES**

### **1. Meetings.**

- The Cybersecurity Committee will meet whenever its members deem a meeting necessary or appropriate. The Cybersecurity Committee will determine where and when to meet and provide this schedule in advance to the Board. The Cybersecurity Committee may act by written consent (which may include electronic consent) in lieu of a meeting in accordance with the Company's bylaws.
- The Cybersecurity Committee will maintain written minutes of its proceedings and actions by written consent, which minutes and actions by written consent will be filed with the minutes of the meetings of the Board.
- The Cybersecurity Committee shall meet periodically with members of management as the Cybersecurity Committee deems appropriate.
- The Cybersecurity Committee may invite to its meetings any director, officer or employee of the Company and such other persons as it deems appropriate in order to carry out its responsibilities. The Cybersecurity Committee may also exclude from its meetings any persons it deems appropriate in order to carry out its responsibilities, including non-management directors who are not members of the Cybersecurity Committee.

**2. Reporting to the Board of Directors.** From time to time, or when requested by the Board, the Chairperson of the Cybersecurity Committee will report to the Board.

**3. Authority to Retain Advisors.** The Cybersecurity Committee shall have the authority, in its sole discretion, to select and retain independent counsel and such other advisors (each an "**Advisor**") as it deems necessary or appropriate to assist with the execution of its duties as set forth in this charter. The Company will provide appropriate funding, as determined by the Cybersecurity

Committee, to pay any Advisors hired by the Cybersecurity Committee and any administrative expenses of the Cybersecurity Committee that the Cybersecurity Committee determines are necessary or appropriate in carrying out its activities.

- 4. Subcommittees.** The Cybersecurity Committee may form subcommittees for any purpose that the Cybersecurity Committee deems appropriate and may delegate to such subcommittees such power and authority as the Cybersecurity Committee deems appropriate. If designated, each such subcommittee will establish its own schedule and maintain written minutes of its meetings and actions by written consent, which minutes and actions will be filed with the minutes of the meetings of the Board. The Cybersecurity Committee shall not delegate to a subcommittee any power or authority required by law, regulation or listing standard to be exercised by the Cybersecurity Committee as a whole.
- 5. Committee Charter Review.** The Cybersecurity Committee shall review and reassess the adequacy of this charter periodically and shall submit any recommended changes to the charter to the Board for approval.
- 6. Performance Review.** The members of the Cybersecurity Committee shall review and assess the performance of the Cybersecurity Committee on an annual basis.
- 7. Authority to Investigate.** In the course of its duties, the Cybersecurity Committee shall have authority, at the Company's expense, to investigate any matter brought to its attention.
- 8. Access.** The Cybersecurity Committee shall be given full access to the chairperson of the Board and management, as well as the Company's books, records, facilities and other personnel.
- 9. Compensation.** Members of the Cybersecurity Committee shall receive such fees or other compensation, if any, for their service as Cybersecurity Committee members as may be determined by the Board in its sole discretion.