CS DISCO, INC.

CHARTER OF THE CYBERSECURITY AND RISK COMMITTEE OF THE BOARD OF DIRECTORS

PURPOSE

The general purpose of the Cybersecurity and Risk Committee (the "Committee") of the Board of Directors (the "Board") of CS Disco, Inc. (the "Company") is to:

- oversee the Company's enterprise-wide cybersecurity, information security and data privacy risk management, including with respect to customer litigation materials, attorney-client privileged content and other sensitive data processed on the Company's platform;
- oversee management's processes for identifying, assessing, managing and mitigating risks relating to cybersecurity, information technology and third-party and vendor risk;
- oversee the Company's incident response planning, preparedness and resilience with respect to cybersecurity incidents;
- oversee the Company's enterprise risk management framework and risk appetite, including the identification of principal and emerging risks facing the Company;
- oversee the Company's compliance with applicable data protection, privacy and cybersecurity-related laws, regulations and disclosure requirements; and
- coordinate with the Audit Committee and other committees of the Board to promote comprehensive, non-duplicative oversight of the Company's risk management framework.

COMPOSITION

The members of the Committee, including the Chairperson, will be members of the Board appointed by, and serving at the discretion of, the Board. Vacancies occurring on the Committee will be filled by the Board. Resignation or removal of a Committee member from the Board for any reason will automatically constitute resignation or removal from the Committee.

The Committee will consist of at least two members of the Board. Each member of the Committee will satisfy the independence and other requirements imposed by applicable law and stock exchange listing requirements, and any other qualifications determined by the Board. At least one member of the Committee should have relevant cybersecurity, information technology or technology-risk expertise (including, for example, prior experience as a chief information security officer or chief technology officer, relevant professional certifications, or comparable public company committee service), to the extent practicable and consistent with the overall composition of the Board.

AUTHORITY

The Committee will have access to all Company books, records, facilities and personnel as deemed necessary or appropriate by any member of the Committee. If the Committee concludes that it must retain legal, cybersecurity, technology, risk management or other outside advisors, it may do so and determine compensation for those advisors at the Company's expense. The Committee may also pay any ordinary administrative expenses it deems appropriate in carrying out its duties at the expense of the Company. The Committee will have authority to require that any of the Company's personnel or outside advisors attend any meeting of the Committee or meet with any member of the Committee or any of its advisors.

Subject to any limitations approved by the Committee, the Chairperson has the delegated authority to act on behalf of the Committee in connection with (1) approval of the retention of outside service providers and advisors (including negotiation and execution of their engagement letters), (2) approval of payment of expenses incurred by the Committee described in the previous paragraph, and (3) as may otherwise be determined by the Committee. The Committee also may form and delegate authority to one or more subcommittees consisting of one or more members of the Board (whether or not he, she or they are on the Committee) to the extent allowed under applicable law and stock exchange listing requirements. The Committee retains concurrent authority to approve any matter that has been delegated to the Chairperson or a subcommittee. Although the Committee may act on any issue that has been delegated to the Chairperson or a subcommittee, doing so will not limit or restrict future action by the Chairperson or subcommittee on any matters delegated to it. Any action or decision of the Chairperson or a subcommittee will be presented to the full Committee at its next scheduled meeting. By approving this Charter, the Board delegates authority to the Committee with respect to the matters set forth herein.

The Committee's primary authority is that of oversight. The members of the Committee are not employees of the Company, and they do not perform management's functions. The Committee relies on the expertise and knowledge of management, including the Company's Chief Information Security Officer ("CISO"), Chief Compliance Officer and such other appropriate officers, in carrying out its oversight. Management, including the CISO, is responsible for implementing and maintaining the Company's cybersecurity risk assessment and management processes, information security policies and practices, enterprise risk management processes, and internal controls regarding information security. It is not the Committee's responsibility to design or implement the Company's cybersecurity program, to eliminate the Company's exposure to risk, to guarantee that the Company will not experience a cybersecurity incident, or to guarantee the effectiveness of the Company's information security or risk management policies and practices.

Coordination with Audit Committee. The Committee will coordinate with the Audit Committee regarding the Company's risk management framework and will work to ensure that risk oversight responsibilities are not duplicated or left uncovered between the Committee and the Audit Committee, including through periodic joint meetings as the Committee and the Audit Committee consider appropriate. For the avoidance of doubt, the Committee's oversight of the Company's regulatory compliance program under this Charter is limited to matters relating to data protection, privacy and cybersecurity, and does not extend to the Company's general legal compliance program or Code of Business Conduct and Ethics, which remain within the Audit Committee's charter.

The Committee's authority includes the following matters; provided, however, that this list is intended to be a guide and to remain flexible to account for changing circumstances and needs. Accordingly, the Committee may depart from or supplement such list consistent with the purpose of the Committee as set herein, and establish policies and procedures, to the extent permitted by applicable law and stock exchange listing requirements. The Board will retain the right to act on all such matters without limiting the Committee's authority, subject to compliance with applicable law and stock exchange listing requirements.

Security Architecture and Technical Risk Management

1. Cybersecurity Risk Assessment and Management. The Committee will oversee management's processes for identifying, assessing, managing and mitigating risks relating to information security and cybersecurity, including the Company's policies, procedures, plans and information technology systems designed to maintain the security, confidentiality, availability and integrity of information.

2. Security Architecture. The Committee will periodically review reports from the CISO regarding the design and effectiveness of the Company's information security program and control architecture, including the threat landscape, vulnerability management activities, and the results of penetration testing and other security assessments.

3. Platform and Product Security. The Committee will oversee Management's processes with respect to the cybersecurity of the Company's customer-facing platforms and products, including periodically reviewing reports from management regarding platform and product security risks, testing, and security certifications.

4. Budget and Resources. The Committee will review and report to the Board with respect to the budget and resources allocated to cybersecurity and information security.

Incident Response and Resilience

5. Incident Response Planning. The Committee will review and oversee the Company's incident response plan, including the results of tabletop exercises and other testing of the plan, and the Company's business continuity and disaster recovery capabilities as they relate to information security.

6. Incident Escalation and Reporting. The Committee will review the effectiveness of the Company's escalation protocols for the prompt reporting of cybersecurity incidents to management, the Committee and, where appropriate, the full Board. Management will promptly notify the Chairperson of the Committee of any cybersecurity incident that is reasonably likely to be material to the Company.

7. Remediation. The Committee will review with management the root cause of, and remediation efforts relating to, any material cybersecurity incident.

Third-Party and Vendor Risk

8. Vendor Risk Management. The Committee will oversee the Company's vendor and third-party risk management program, including due diligence and ongoing monitoring of subprocessors, cloud infrastructure providers and other vendors that store, process or transmit Company or customer data, including customer litigation materials and privileged content.

9. Contractual Requirements. The Committee will periodically review the Company's practices for imposing and monitoring compliance with contractual security and data-handling requirements applicable to material vendors and subprocessors.

Enterprise Risk and Compliance

10. Risk Appetite, Tolerance and Strategy. The Committee will advise the Board on the Company's overall risk appetite and tolerance, and on the likelihood, impact and mitigation of the principal risks facing the Company, and will recommend related risk and insurance policies for the Board's approval.

11. Cyber and Technology Insurance. The Committee will periodically review the adequacy of the Company's technology errors and omissions, cyber liability and any related insurance coverage in light of the Company's risk profile and will advise the Board and management on its review. The Committee will coordinate with the Audit Committee regarding any overlap with the Audit Committee's oversight of insurance matters.

12. Artificial Intelligence Risk. The Committee will periodically review with management the cybersecurity, data privacy and operational risks arising from the Company's development, deployment and use of artificial intelligence and machine learning technologies, and will oversee management's processes for identifying, assessing, managing and mitigating such risks.

13. Principal and Emerging Risk Identification. The Committee will review management's processes for identifying and monitoring principal and emerging risks across the enterprise, including operational, legal, reputational and third-party risks not otherwise assigned to another committee of the Board, and will assist the Board's assessment of those risks.

14. Enterprise Risk Management Framework. The Committee will oversee the design and effectiveness of the Company's overall risk management and internal control systems, in coordination with the Audit

Committee's oversight of internal control over financial reporting.

15. Regulatory Compliance Program. The Committee will oversee the adequacy and effectiveness of the Company's compliance program and function as it relates to data protection, privacy and cybersecurity matters, including monitoring and response to related regulatory examinations, inquiries and orders.

16. Compliance Officer Reporting. The Committee will receive periodic reports from the Chief Compliance Officer (or equivalent) on the compliance program, material compliance risks, and the results of compliance monitoring and audits, in each case as they relate to data protection, privacy and cybersecurity matters.

17. Coordination on Risk Allocation. The Committee will periodically review, together with the Board and other committees, how risk oversight responsibilities are allocated across the Board's committees, and will recommend changes to such allocation as the Company's risk profile evolves. The Committee will advise the Compensation Committee, at that committee's request, on whether risk-related adjustments to incentive compensation or clawback provisions are warranted, provided that responsibility for compensation decisions remains with the Compensation Committee.

Data Privacy and Cybersecurity Regulatory Matters

18. Privacy Compliance. The Committee will oversee the Company's compliance with applicable data protection and privacy laws, rules and regulations, including as they relate to customer and case data processed by the Company.

19. Regulatory Engagement and Disclosure. The Committee will review with management any material correspondence with regulators concerning cybersecurity or data privacy matters and will review with management any disclosures in the Company's reports filed with the Securities and Exchange Commission relating to cybersecurity risk management, strategy and governance.

Other Matters

20. CISO Reporting Line. The Company's CISO will have a direct reporting line and right of access to the Chairperson of the Committee between scheduled meetings on material developments.

21. Committee Self-Assessment. The Committee will evaluate its performance and the adequacy of this Charter periodically as the Committee deems appropriate, or as frequently as may be required by the SEC and stock exchange listing standards.

22. General Authority. The Committee will perform such other functions and have such other powers as may be necessary or appropriate in the discharge of any of the foregoing.

MEETINGS AND MINUTES

The Committee will meet at least four times per year, and otherwise whenever its members deem a meeting necessary or appropriate. The Committee will determine where and when to meet.

Unless otherwise determined by the Committee, each regularly scheduled meeting will include a private session with the Company's CISO, without other members of management present, to permit candid reporting on the Company's security posture, incident history and resourcing needs. To foster open communication, the Committee may also meet periodically with other members of management, including the Chief Compliance Officer, in separate executive sessions. From time to time, or when requested by the Board, the Chairperson of the Committee will report to the Board on the Committee's activities, discussions and actions.

The Committee will maintain written minutes of its meetings and regularly report to the Board on its actions and recommendations. The Committee may act by unanimous written consent; when it does so, those actions will be filed in the minute book.

PUBLICATION

The Company will make this Charter freely available to stockholders on request and will publish it on the Company's website.

Adopted by the Board of Directors: October 21, 2026