CID HOLDCO, INC.

CYBERSECURITY AND TECHNOLOGY COMMITTEE CHARTER

I. PURPOSE. The Cybersecurity and Technology Committee (the "Committee") of the Board of Directors (the "Board") of CID Holdco, Inc. (the "Company") is established to assist the Board in fulfilling its oversight responsibilities with respect to:

(a) management's enterprise-wide risk assessment and risk management practices related to cybersecurity, data privacy, and technology; (b) the Company's technology systems and capabilities, including strategies, investments, resilience, innovation, and operational security; (c) compliance with applicable legal, regulatory, and industry obligations related to information security and cyber risk; (d) ensuring appropriate coordination with the Audit Committee in matters that could impact internal control over financial reporting or financial disclosures; and (e) monitoring the Company's compliance with cybersecurity disclosure obligations under SEC Regulation S-K Item 106 and Form 8-K Item 1.05, including material incident disclosure and cybersecurity governance reporting.

II. MEMBERSHIP. The Committee shall consist of at least three members of the Board, all of whom shall be "independent" under the applicable listing standards of The Nasdaq Stock Market LLC and meet any other qualifications established by the Board. At least one member of the Committee shall also be a member of the Audit Committee to facilitate coordination. The members and Chair of the Committee shall be appointed by the Board and may be removed by the Board in its discretion.

At least one member of the Committee should have experience or expertise in cybersecurity, information technology, or technology risk management, as determined by the Board.

The Committee shall coordinate regularly with the Audit Committee and Nominating and Corporate Governance Committee to ensure comprehensive oversight of technology-related risk, internal control implications, and director-level competency on cybersecurity.

III. MEETINGS AND PROCEDURES. The Committee shall meet at least four times per year or more frequently as deemed necessary by the Committee Chair. Meetings may be held in person, telephonically, or via video conference. The Committee may request any officer or employee of the Company, outside counsel, or advisors to attend a meeting of the Committee or meet with any members of the Committee. The Committee shall maintain minutes of its meetings and report regularly to the Board.

The Committee shall provide a summary report of its meetings and significant findings to the full Board following each meeting and shall promptly escalate critical issues, including material incidents, to the full Board and Audit Committee.

The Committee shall have the authority to form and delegate responsibilities to subcommittees when appropriate, provided that such subcommittees are composed entirely of independent directors.

IV. DUTIES AND RESPONSIBILITIES. The Committee shall:

1. Review with management the Company's cybersecurity threat landscape, policies, controls, and incident response preparedness, including escalation procedures to the Board, tabletop exercise testing, and periodic simulations.
2. Review reports and metrics on cybersecurity incidents, breaches (actual or attempted), and the Company's response thereto.
3. Evaluate the Company's compliance with cybersecurity and data privacy laws, including SEC, state, and international regulations, and industry standards.
4. Review the adequacy and effectiveness of the Company's technology architecture, platforms, and operational resilience.
5. Review and oversee major technology-related projects, digital initiatives, and infrastructure investments.
6. Oversee the Company's disaster recovery, business continuity, and data backup processes.
7. Discuss with management the Company's cyber insurance coverage and review its adequacy.
8. Coordinate with the Audit Committee with respect to any matters that may impact internal controls, financial reporting, or cybersecurity disclosures.
9. Evaluate the Company's cybersecurity workforce, training programs (including executive and board-level cybersecurity education), budget, and third-party vendor and supply chain risk management processes.
10. Review and approve policies for oversight of risks arising from use of AI, machine learning, and other emerging technologies.
11. Ensure appropriate disclosures are made in public filings relating to cybersecurity oversight and risk management.
12. Review and recommend for Board approval updates to this Charter on an annual basis.
13. Monitor the Company's compliance with cybersecurity disclosure obligations under SEC Regulation S-K Item 106 and Form 8-K Item 1.05, including timely disclosure of material cybersecurity incidents and governance structures.
14. Oversee management's third-party risk management practices, including risk assessment and monitoring of key technology vendors and supply chain cybersecurity vulnerabilities.
15. Review the Company's training programs and culture-building efforts relating to cybersecurity awareness, including for executives and directors.

V. AUTHORITY AND RESOURCES. The Committee shall have the authority, at the Company's expense, to retain independent advisors, including legal counsel, consultants, and cybersecurity experts, as it deems necessary to carry out its responsibilities. The Company shall

provide appropriate funding for payment of compensation to such advisors and for ordinary administrative expenses of the Committee.

The Committee shall have full access to all books, records, facilities, and personnel of the Company and may request any officer or employee to attend meetings or provide relevant information.

VI. PERFORMANCE EVALUATION. The Committee shall annually conduct a self-evaluation of its performance and effectiveness and report the results to the Board. It shall also review and assess the adequacy of this Charter annually and recommend any proposed changes to the Board for approval. The Committee shall ensure that its charter remains aligned with SEC rulemaking, Nasdaq listing requirements, and evolving industry best practices in cybersecurity oversight.

VII. DISCLOSURE. This Charter shall be made available on the Company's website and as required in public filings with the SEC, including the proxy statement and Form 10-K, in compliance with applicable Nasdaq and SEC regulations.