PENGUIN™ SOLUTIONS

Penguin Solutions, Inc. Cybersecurity and Technology Risk Management Committee Charter

1.0 Purpose

The Cybersecurity and Technology Risk Management Committee (the "Committee") of the Board of Directors (the "Board") of Penguin Solutions, Inc. (the "Company") is chartered to act on behalf of the Board in fulfilling the Board's oversight responsibility with respect to the Company's information technology ("IT") use and data security, including, but not limited to, enterprise cybersecurity, generative artificial intelligence ("AI"), privacy, data collection and protection, and compliance with information security and data protection laws. The Committee serves the Board and is subject to its control and direction. Nothing herein is intended to expand applicable standards of liability under state or federal law for directors of a corporation.

2.0 Membership

The Committee shall consist of at least three (3) members of the Board. Each member shall have working familiarity, knowledge and competencies in relevant areas, including data privacy, public policy, AI, IT strategy, IT development and deployment, or IT risk assessment and management, including information security management. At least one member shall be deemed independent by the Board. The Board shall recommend nominees for appointment to the Committee annually and as vacancies or newly created positions occur. Committee members shall be appointed by the Board and may be removed by the Board at any time. The Board shall designate the Chair of the Committee. All directors who are not members of the Committee may attend meetings of the Committee, observe, and participate in discussions, but they shall not be entitled to vote on Committee matters.

3.0 Responsibilities

In addition to any other responsibilities which may be assigned from time to time by the Board, the Committee is responsible for the following matters.

3.1 Information technology and enterprise cybersecurity

The Committee shall oversee the Company's global IT strategy, including the quality and effectiveness of the Company's policies and procedures with respect to its IT systems, enterprise cybersecurity, AI, and privacy.

3.2 Data collection

The Committee shall oversee the systems, controls, and procedures used by the Company and business partners engaged by the Company to collect, create, use, maintain, process, and protect personal information and/or any information or assets of the Company's customers, employees, and business partners (collectively, "Company Information Assets").

3.3 Data protection

The Committee shall oversee policies, procedures, plans, and execution intended to provide security, confidentiality, availability, and integrity of Company Information Assets.

3.4 Product oversight

The Committee shall provide high level guidance on the risk of compromise of any of the Company's products and services (including software), and processes and control procedures put in place to mitigate such risks.

3.5 New acquisition IT and data integration

The Committee shall oversee planning and risk mitigation in relation to the integration of new acquisitions' IT systems and data.

3.6 Incident response

The Committee shall oversee any policies and procedures of the Company that pertain to the Company's response to any material incidents.

3.7 Disaster recovery

The Committee shall periodically review with management the Company's disaster recovery capabilities.

3.8 Legal compliance and internal audits

The Committee shall oversee the Company's compliance with applicable information security and data protection laws and industry standards, and shall oversee any internal audits of the Company's IT systems and processes.

3.9 Risk education and culture

The Committee shall oversee the Company's education of employees regarding cybersecurity, AI, privacy, and related risks.

3.10 Cyber insurance

The Committee may review the Company's cyber insurance policies to ensure appropriate coverage.

4.0 Knowledge management and reporting

4.1 Knowledge management

The Committee members shall take reasonable and appropriate steps to maintain current knowledge of changing cybersecurity threats, countermeasures, and other information relevant to cybersecurity and technology risk oversight.

4.2 Reporting

In addition to the Chief Information Officer's (the "CIO") annual report to the full Board regarding the Company's cybersecurity and technology program and material risks, the CIO will regularly, but no less than three times a year, provide reports to this Committee with respect to cybersecurity and technology risks and program management. These reports shall include coverage of: (a) the confidentiality of sensitive Company information and the integrity and security of the Company's information systems; (b) the Company's cybersecurity and AI policies and procedures; (c) material cybersecurity and technology risks to the Company; (d) the overall effectiveness of the Company's cybersecurity program; and (e) material cybersecurity events involving the Company during the time period addressed by the report. The CIO shall also make available key metrics about the cybersecurity program.

5.0 Advisors, investigations, and delegation of authority

The Committee may request that the Company's CIO and other appropriate Company personnel work with the Committee to review the plans and implementation, as well as to check on any identified issues. The Committee has the sole authority to retain and terminate any advisers, including cybersecurity, AI, or data privacy experts and legal counsel, including sole authority to approve all such advisers' fees and other retention terms.

The Committee shall have the authority to conduct or authorize investigations into or studies of any matters within the Committee's scope of responsibilities. The Committee may delegate its authority to subcommittees or the Chair of the Committee when it deems appropriate and in the best interests of the Company.

6.0 Procedures

The Committee shall meet as often as it determines is appropriate to carry out its responsibilities under this Charter. The Chair of the Committee, in consultation with the other Committee members, shall determine the frequency and length of the Committee meetings and shall set meeting agendas consistent with this Charter. A majority of the members of the Committee shall constitute a quorum and determinations of the Committee shall be made by a majority of the members present at a duly convened meeting. The Committee shall review and evaluate its performance, including reviewing compliance with the Charter, at least once every other year.