DATA STORAGE CORPORATION
CYBERSECURITY AND RISK COMMITTEE CHARTER

Adopted on March 27, 2024

Committee's Purpose

The Cybersecurity and Risk Committee (the "Committee") is established by the Board of Directors (the "Board") to assist the Board in overseeing the company's cybersecurity posture and risk management strategies. The Committee's primary duties include reviewing the company's policies and practices regarding information security, data protection, and risk assessment and mitigation, ensuring alignment with business objectives and compliance with legal and regulatory requirements.

Committee Membership

- **Composition**: The Committee shall consist of at least two directors appointed by the Board, who possess knowledge of cybersecurity and risk management.
- **Chairperson**: The Board shall appoint a Chairperson of the Committee, who will lead the Committee's activities and report to the Board.
- **Term**: Members serve at the pleasure of the Board for such term or terms as the Board may determine or until their successors shall be duly elected and qualified.
-

Meetings

- **Frequency**: The Committee shall meet at least quarterly, or more frequently as circumstances dictate.
- **Special Meetings**: Special meetings may be convened as required to address specific issues that arise between regular meetings.
- **Quorum**: A majority of the members of the Committee shall constitute a quorum for the transaction of business.
- **Independence**: Each member of the Committee shall be "independent" as defined by the listing standards of the Nasdaq Stock Market.

Responsibilities and Duties

1. **Cybersecurity Oversight**:
    - Review and approve the company's cybersecurity strategy and policies.
    - Review with management the Company's cybersecurity threat landscape, risks, and data security programs, and the Company's management and mitigation of cybersecurity risks and potential breach incidents
    - Oversee the establishment and maintenance of a cybersecurity governance framework.
    - Review reports on significant cybersecurity incidents and the responses to those incidents.
    - Review reports and key metrics from management on the Company's cybersecurity, technology and information systems and related risk management programs.

2. **Risk Management**:
    - Oversee the company's overall risk management framework and policies.

- Review and assess major financial, operational, compliance, reputational, and strategic risks.
- Ensure integration of risk management with corporate strategy and compliance.

3. **Compliance and Reporting**:
    - Oversee compliance with legal and regulatory requirements relating to cybersecurity and risk management.
    - Review with management the Company's compliance with applicable information security and data protection laws and industry standards
    - Review and approve disclosures related to cybersecurity and risk in public filings.

4. **Vendor and Third-Party Risk Management**:
    - Oversee policies and procedures for managing risks associated with third-party vendors, including cybersecurity risks.

5. **Education and Advocacy**:
    - Ensure Board members receive regular updates on cybersecurity and risk management trends, threats, and best practices.

Authority

The Committee has the authority to conduct or authorize investigations into any matters within its scope of responsibility, with full access to all books, records, facilities, and personnel of the company. The Committee has the authority to engage independent counsel and other advisers as it deems necessary to carry out its duties.

Reporting

The Committee will regularly report to the Board on its findings and recommendations, including any proposed changes to the company's policies and procedures related to cybersecurity and risk management.

Review and Amendment of the Charter

The Committee shall review and reassess the adequacy of this Charter annually and recommend any proposed changes to the Board for approval. The Board may amend or revise the Charter at any time.