

AVERY DENNISON CORPORATION
CYBERSECURITY COMMITTEE CHARTER*

Purpose

The Cybersecurity Committee (“Committee”) is appointed by the Board of Directors (the “Board”) to assist with its oversight of the Company’s strategies, policies and risk management practices related to cybersecurity and information security.

Committee Membership

The Committee shall consist of no fewer than three members. At least two members of the Committee shall meet the independence requirements of the New York Stock Exchange and the rules and regulations of the Securities and Exchange Commission. The Chair and members of the Committee shall be appointed by the Board on the recommendation of the Governance Committee. Committee members may be replaced by the Board.

Committee Meetings

The Committee shall meet as often as it determines to be necessary, but not less frequently than twice a year. The Company’s Chief Information Security Officer (CISO) will regularly, but no less than twice a year, report to the Committee regarding the matters within the scope of the Committee’s oversight responsibilities as described below. The Committee may request any other officer or employee of the Company or the Company’s outside counsel, financial advisor or other external advisor to attend a meeting of the Committee or to meet with any members of, or consultants to, the Committee.

The Committee shall have the authority, to the extent it deems necessary or appropriate, to retain independent legal, financial or other advisors. The Company shall provide for appropriate funding, as determined by the Committee, for payment of compensation to any advisors engaged by the Committee and for payment of ordinary administrative expenses of the Committee that are necessary or appropriate in carrying out its duties.

The Committee shall make periodic reports to the Board. The Committee shall review and reassess the adequacy of this Charter annually and recommend any proposed changes to the Board for approval. The Committee shall annually review its own performance.

The Committee, to the extent it deems necessary or appropriate, shall have oversight of the Company’s cybersecurity risk management program and review regular reports from Company management on cybersecurity and other risks related to the Company’s information security, including making recommendations to the Board regarding:

- (a) The Company’s cybersecurity governance, strategy and significant initiatives, including alignment thereof with the Company’s business strategies and priorities, market practices, and lessons learned from notable incidents affecting other companies.

* First adopted effective February 3, 2026.

- (b) The capabilities and effectiveness of the Company's cybersecurity risk management program, including its integration and alignment with the Company's enterprise risk management program and the Company's plans, policies, practices and controls related to information security, including the impact thereon of artificial intelligence, the prevention and detection of cybersecurity events, incident response, disaster recovery and business continuity.
- (c) The systems and procedures used by the Company to collect, create, use, maintain, process and protect any personal information of its customers, employees and business partners.
- (d) Key legislative and regulatory developments in the U.S. and international jurisdictions that could materially impact the Company's cybersecurity risk and strategy.
- (e) Key performance indicators (KPIs) related to the Company's cybersecurity preparedness.
- (f) Such other matters that management or the Board desires to have reviewed by the Committee.

Additional Committee Authority

The Committee shall have such other duties as may be lawfully delegated to it from time to time by the Board. The Committee may form and delegate authority to subcommittees when appropriate.