BGC GROUP, INC.
CYBERSECURITY PROGRAM POLICY STATEMENT

BGC Group, Inc. ("we" or "BGC") has approved the following global Cybersecurity Program policy statement with respect to BGC and its subsidiaries on a global basis

Commitment

We are committed to combating the threat of cyber-attacks and to securing our business through our information security programs and developing a deep understanding of cybersecurity risks, vulnerabilities, mitigations, and threats. We have a global cybersecurity process applicable to all subsidiaries and business lines.

Risk Management and Strategy

Our global cybersecurity processes form the comprehensive framework we utilize for planning, performing, managing, assessing, and improving our security controls as they relate to cybersecurity, and form part of our overall risk management system. We aim to conduct our cybersecurity program in accordance with current recognized global policies and standards for cybersecurity and information technology. These processes are managed by our cybersecurity team headed by BGC's Chief Information Security Officer (the "CISO") and supported by our business continuity teams.

We conduct periodic internal and external vulnerability audits and assessments and penetration testing and provide periodic cybersecurity training to employees. These measures include regular phishing simulations, annual general cybersecurity awareness training and data protection training. We also participate in industry-specific cybersecurity roundtables and professional groups to ensure we remain abreast of industry-wide cybersecurity developments and best practices and thereby enhance our threat identification processes and responses as necessary. Additionally, when engaging with and utilizing third-party vendors and partners for our business, we conduct various oversight assessments, including due diligence and periodic monitoring to identify potential cybersecurity threats associated with our conducting business with such vendors and partners and to ensure any corresponding risk exposure aligns with our business requirements and risk tolerances.

Incident Reporting and Escalation

We maintain an incident reporting and escalation process in the event of any observed, detected, or suspected events that we believe may qualify as a cybersecurity incident. Risks are identified based on a four-tier system, and tiers are assigned based on the service impact, user impact, financial impact, and security impact that a threat may pose. Our processes include steps to recover our systems and information through established and tested system recovery plans and business continuity plans, each based on the appropriate response associated with the corresponding tier of the identified threat. Our incident response process includes steps to notify key incident management team members who are responsible for communicating with regulatory and other governmental

authorities about cybersecurity events as applicable and as required by law. We determine the materiality of such incidents based upon a number of factors including if the incident had or may have a material impact on our business strategy, results of operations, or financial condition. This process involves a review of the nature of the incident by our cybersecurity team as well as other members of management and employees with specialized technology or financial knowledge, including our CISO, BGC's Chief Information Officer (the "CIO"), and BGC's Chief Financial Officer (the "CFO"), as applicable. In the event of a material breach, we have a process for escalation to appropriate members of our senior management, and, where appropriate, to our Board and Audit Committee. These groups also collaborate in determining the appropriate response to such events and disclosure of any material breach.

We engage third parties from time to time that assist us in the identification, assessment, and management of cybersecurity risks. We also engage cybersecurity specialists to complete assessments of our cybersecurity processes, program and practices, including our data protection practices, as well as to conduct targeted attack simulations. The feedback from these assessments and guidance from external specialists informs our overall risk management system and the development and improvement of our processes to mitigate cybersecurity risks throughout the Company.

Board Governance and Management

Our global cybersecurity processes are managed primarily by our CISO, our CIO, and our CFO. Pursuant to the Audit Committee charter, the Audit Committee oversees the management of the Company's risk management process, including the identification, prioritization, assessment and management of risks related to cybersecurity. While our Board and Audit Committee members have broad experience in risk management and in some cases technological expertise relating to cybersecurity, our CISO and CIO and management teams handle cybersecurity threat management. The CISO and CIO provide the Board and Audit Committee periodic reports regarding the Company's cybersecurity risks and threats, the status of projects to strengthen our information security systems, assessments of our information security program, and any issues associated with the emerging threat landscape. In addition, the CISO provides periodic reports to our executive officers, members of the boards of certain of our regulated entities internationally and other members of our senior management as appropriate. Material events and updates are reported to the full Board and Audit Committee annually and on an ad hoc basis where warranted based on the level of materiality of any such incidents as determined by the incident reporting and escalation process led by our CISO and CIO. Our processes are regularly evaluated by internal and external experts, with the results of those reviews reported to senior management and, where appropriate, the Board and Audit Committee.

Version: July, 2024