CYBERSECURITY POLICY

Version Approved Effective: December 12, 2024

Purpose

The purpose of this Cybersecurity Policy (or the "**Policy**") is to (1) serve as a standard for setting, reviewing and implementing the Corporation's cybersecurity expectations and (2) set forth a mechanism for enforcement of such expectations.

The information that exists within the information technology ("**IT**") network and infrastructure, including the networks and infrastructures of third parties that handle the Corporation's information (the "**Cyberspace**"), is both a valuable asset of the Corporation and subject to a multitude of legal requirements. Therefore, the Corporation requires an effective Information Security Program ("**Security Program**") to manage the information security in the Cyberspace.

This Policy serves as a framework that all employees, directors and officers shall abide by to ensure that risks to the confidentiality, integrity or availability of the Corporation's information assets ("**Information**") are managed in accordance with the agreed upon Security Program. In guiding the Corporation's ongoing operation, maintenance and effective management of its cybersecurity initiatives, this Policy will detail the roles and responsibilities of key personnel to implement and/or maintain the information security measures necessary to meet the objectives of this Policy.

Applicability

This Policy applies to all directors, officers, employees and contractors of the Corporation and any parent, holding companies and subsidiaries, regardless of the terms of their contract (collectively, "**you**"), who use the Corporation's Information or technological devices. References in this Policy to "**we**", "**us**" or "**our**" shall be interpreted as referring to the Corporation unless the context suggests otherwise.

Policy Statement

The Board of Directors of the Corporation (the "**Board**") recognizes the importance of an effective Security Program and strives to maintain the confidentiality, integrity and availability of Information in the Cyberspace. It is, therefore, the Corporation's policy to implement a Security Program that (1) implements and maintains reasonable and adequate information security measures to prevent, detect and respond to risks to the security of Information in the Cyberspace; (2) implements and maintains information security measures and procedures that comply with applicable laws, regulations and contractual obligations; and (3) uses an information security risk management approach to make appropriate choices about the information security measures that will most effectively protect the Corporation and its Information from anticipated risks.

It is also the Corporation's policy that it has the right to monitor and audit network and system usage at any time to ensure compliance with this Policy and applicable legal obligations. The Corporation views all reports of violations of this Policy seriously and shall thoroughly investigate and take appropriate action on any such reports.

Roles and Responsibilities

Committee Oversight

The Audit Committee of the Corporation (the "**Audit Committee**") will oversee this Policy and will be responsible for ensuring the implementation of the Security Program. Management shall report to the Audit Committee on the Corporation's Security Program. Such reports shall also cover any subsidiaries of the Corporation. The reports shall cover the Security Program's security measures and include an evaluation of their effectiveness in light of trends that affect the Corporation's risk profile. In addition, these reports shall include recommendations for changes to the Security Program to better address the risks to the Corporation's Information and operations or to better align to the Corporation's overall business and strategy. The reports shall also explain any breaches of security that have occurred and recommend, where appropriate, changes to the information security measures included in the Security Program to prevent the recurrence of such breaches.

Management Oversight

The Corporation hereby designates its Chief Financial Officer (the "**CFO**") as its Security Officer with the primary responsibility to implement and maintain this Policy and the Security Program. Personnel from various departments of the Corporation shall be identified under this Policy to report to the Security Officer and oversee specified components of the Security Program. Despite these designations, cybersecurity shall remain the responsibility of all business stakeholders and requires the cooperation and compliance of all personnel.

The Security Officer or the Security Officer's designee(s) shall be responsible for:

- Ensuring the Security Program includes reasonable and appropriate administrative, technical and physical safeguards to protect Information;
- Assessing, no less frequently than annually, internal and external risks to Information and maintaining related documentation, including risk assessment reports and remediation plans;
- Evaluating the effectiveness of the Security Program in addressing such risks;
- Ensuring, in collaboration with Legal, that the Security Program complies with applicable laws and regulations, particularly with regard to required reporting of security incidents and data breaches;
- Ensuring, in collaboration with Legal, that the Corporation's use of Information relating to identified or identifiable individuals (including the Corporation's personnel) is consistent with applicable laws and regulations;
- Providing for the oversight of third-party service providers that access or maintain the Corporation's electronically stored information and ensuring that such oversight meets applicable legal requirements;
- Enacting procedures to ensure that suppliers, service providers and other third parties whose own security incidents could materially affect the Corporation are legally obligated to timely report such incidents to the Corporation;
- Enacting procedures to ensure that the Corporation makes a timely materiality decision with respect to each security incident that materially affects the Corporation and timely discloses such incidents as required by law;
- Ensuring the Audit Committee is provided with the reports required under this Policy; and
- Defining and managing an exceptions process to review, approve or deny, document, monitor and periodically reassess any necessary and appropriate, business-driven requests for changes or deviations to this Policy or the Security Program.

Management Responsibilities

The Corporation's management team shall facilitate an environment whereby managing cybersecurity risk is accepted as the personal responsibility of all Corporation personnel. The below-listed personnel are also hereby designated to assist the Security Officer with regard to the following roles and responsibilities:

- IT Manager*:*
    - Network Segmentation;
    - Secure Remote Access (VPN);
    - Privileged Access Management;
    - Access Control;
    - Asset Management;
    - Web Content Filtering;

- Endpoint Hardening;
- Email Security;
- Security Monitoring;
- Mobile Device Management;
- Incident Response Plan (in collaboration with IT, Legal and Beazley Breach Response);
- Disaster Recovery Program; and
- Patch & Vulnerability Management.

- *CEO:*
  - IS Governance, Policies and Standards;
  - Cybersecurity Risk Management;
  - Deficiencies and Deviation Management; and
  - Strategic Metrics and Reporting.
- *Dorsey:*
  - Coordinating Audit/Regulatory Exercises;
  - Public Disclosure and Securities Filings;
  - Information Security Compliance (including data breach and security incident reporting, in collaboration with the Security SME); and
  - Forensics.
- *HR Manager:*
  - Information Security Awareness and Training Program;
  - Knowledge and Talent Management; and
  - Background Screening.
- *Controller:*
  - Identity Theft Red Flags;
  - Funds Transfer Safeguarding; and
  - Physical Security.

The Security Officer shall collaborate with other members of the management team to ensure that personnel are provided with adequate resources and trainings to fully understand and carry out this Policy's requirements. The Security Officer may also ask members of the management team to assist with IT security investigations in the event of a breach of this Policy. If any member of management is unaware of the best course of action in dealing with an IT-related matter, the manager shall immediately contact the Security Officer, who shall consult the Corporation's third-party IT representative and or the Corporation's cyber insurance company and response team as needed. Upon becoming aware of a potential violation of this Policy or a breach of cybersecurity, the member of management must immediately document the violation and take possession of any Corporation devices that may have suffered a security breach.

Employee Responsibility

All Corporation personnel shall exercise reasonable and sound professional judgment in using Information or computing devices connected to the Cyberspace. All Information, including physical and intellectual property stored on electric and computing devices or existing within the Cyberspace, remain the sole property of the Corporation or its licensors. Therefore, employees must refrain from using Information except as necessary to accomplish their assigned duties or as directed by management or the Corporation's directors and officers.

Employees are strictly prohibited from performing any act that would be contrary to this Policy, including but not limited to:

- accessing the Corporation's Information, information systems or accounts for any purpose other than as necessary to conduct the Corporation's business in ordinary course;
- using the Corporation's information systems in any manner that violates applicable laws or regulations, including by recording calls or conversations in violation of applicable law;
- using any third party's information systems in any manner that violates applicable laws or regulations or the terms of use under which the third party provides such information systems;

- copying or distributing copyrighted material or other intellectual property without proper legal authorization;
- installing any copyrighted software without proper approval;
- bypassing, impairing or destroying any security mechanisms employed by the Corporation's information systems, including by sharing passwords with other individuals or allowing others access to your accounts;
- disclosing or exporting Information, software, technical information, encryption software or technologies without obtaining prior consent from either management or the Corporation's third party IT group;
- disparaging or denigrating the Corporation, its personnel, subsidiaries, products or services;
- transmitting any marketing, advertising or promotional materials, including bulk or commercial mail or email, except to conduct the Corporation's business as assigned;
- impersonating any other person or organization;
- transmitting any malware or any other type of malicious or deleterious software;
- transmitting any content or data that is pejorative, offensive, lewd, pornographic, defamatory, libelous, harassing, tortious, abusive, illegal, discriminatory or otherwise inappropriate; and
- making fraudulent offers of products, items or services from any account that represents the Corporation.

All potential threats or loss of any Corporation device that may store confidential information must be promptly reported to the Security Officer.

Disclosure

Disclosure of cybersecurity and information security related matters, including material cybersecurity incidents, risk factors, risk management, governance, strategy and other disclosures shall be provided in accordance with applicable laws and regulation. The Audit Committee shall also review the Corporation's cybersecurity-related disclosures in its Annual Report on Form 10-K. See appendix A.

Regulatory Developments

The Audit Committee shall oversee, on a regular basis, the implementation and effectiveness of this Policy and the Security Program shall, annually or otherwise when applicable, assess:

- key legislative and regulatory developments that could materially impact the Corporation's cybersecurity and digital technology strategy, operations or risk exposure;
- engagement with government agencies, industry peers and other critical infrastructure sectors on cybersecurity and related resiliency;
- industry trends, benchmarking and best practices relating to cybersecurity and digital technology; and
- any relevant cybersecurity and digital technology metrics.

Reports to the Board

The Audit Committee shall report regularly to the Board concerning its matters covered under this Policy and advise the Board of any developments that the Committee believes merit Board consideration. The Audit Committee shall also annually review and assess the adequacy of this Policy and recommend any proposed changes to the Board for approval.

Enforcement

Failure to comply with this Policy or support this Policy and the mandates herein may compromise the Corporation's Information and cause irreparable harm to the Corporation, its people, clients, Information and other assets. Violations or breaches of this Policy or any associated schedules, standards or guidelines may result in suspension, discipline up to and including termination, in addition to administrative sanctions or legal actions.

_____