FIRST PACIFIC COMPANY LIMITED

第一太平有限公司

(Incorporated with limited liability under the laws of Bermuda)

Website: www.firstpacific.com

(Stock Code: 00142)

CYBERSECURITY POLICY

This policy supports First Pacific's Code of Conduct (Code) and must be read in conjunction with the Code.

1. INTRODUCTION

The risk of data theft, scams, and security breaches can have severe consequences such as regulatory breach, financial loss, and a detrimental impact on a company's shareholder value and reputation. First Pacific adopts strong cybersecurity measures to prevent breaches and compromises in its IT environment. With the help of highly qualified third-party cybersecurity consultants carefully selected by the company's IT Management Committee, First Pacific has established well defined cybersecurity policies for end users of the IT environment and third-party IT support or consultants.

2. PURPOSE

The purpose of this policy document is to summarize the salient features of the existing cybersecurity policy documents adopted by First Pacific for internal use which cover topics including (a) access control, data handling and storage, information exchange and disposal, (b) cybersecurity incident and data breach incident response planning (c) responsibilities and authority of First Pacific's IT Management Committee, and (d) expectations and management of IT contractors and consultants.

3. SCOPE

The company has a well circulated cybersecurity policy document formally acknowledged by all current employees of First Pacific. A separate cybersecurity policy document governs the protocols followed by third-party contractors and consultants with access to the Company's electronic systems, information, data, software and/or hardware.

Transferring Data

First Pacific recognizes the security risks of transferring confidential data internally and externally. Strong access controls reduce the risk of accidental or deliberate modification or destruction of data as well as protect against unauthorized access or dissemination. Access to information must be commensurate with an individual's business role in First Pacific and the least privilege concept, whereby the minimum access levels are granted

based upon the requirement to access that information for business needs. Some examples of instructions under the company's cybersecurity policies include:

- Refrain from transferring proprietary or confidential information to external parties with the exception of communications covered by appropriate agreements such as non-disclosure agreements;
- Required escalation of perceived security incidents, and the paths for reporting the potential breach;
- Remain diligent of phishing email attempts; and
- Require installation of company security software on devices with access to company data to enable confidential data preservation, when necessary.

Device Security

To ensure the security of all devices and information used in the business of First Pacific, people covered in the scope of this policy are required to:

- Keep all company-issued and personal devices used for Company business (including tablets, computers, and mobile devices) secured with strong passwords;
- Log into company accounts and systems through secure and private networks only via two-factor authentication;
- Ensure they do not leave their devices unattended while unlocked;
- Refrain from sharing work-related passwords with anyone; and
- Regularly update devices with the latest security software and operating systems.

Training and Disciplinary Action

All employees of First Pacific undergo regular cybersecurity training. Understanding and acknowledgment of adherence to the relevant cybersecurity policy document is part of the Human Resources Onboarding process. Annual penetration tests by IT consultants also assess the phishing email "hygiene" of employees. Violation of cybersecurity policy can lead to disciplinary action, up to and including termination based on the severity of the violation. Unintentional violations only warrant a verbal warning, while frequent violations of the same nature can lead to a written warning, and intentional violations can lead to suspension and/or termination, depending on circumstances. Cybersecurity is integral to staff performance reviews.

4. AUTHORITY

First Pacific is an investment holding company with independent IT set up to all its investments. Accordingly, the mode of cybersecurity management is adopted as befitting for the business nature, risk level, and cybersecurity goals of the organization. First Pacific's IT Management Committee, comprising the Chief Financial Officer and respective Department Heads, defines the Company's cybersecurity policies and ensures they are adopted by end-users and third-party IT consultants. This executive management committee is responsible for:

- Ensuring that the Company's data privacy and information security risk management framework, processes and policies are comprehensive, up to date and effective;
- Ensuring adequate plans are in place to address data breaches and security incidents;
- Reviewing and assessing controls and the need to strengthen further First Pacific's IT infrastructure, including any IT maintenance and control enhancement budget proposals;

- Reviewing any significant incidence reports from First Pacific's 24x7 security monitoring contractor;
- Presenting annually to the First Pacific Audit and Risk Management Committee on the Company's level of compliance with regulatory requirements, internal policy updates, standards on data protection and information security, and any breaches of cybersecurity;
- Engaging an independent consultant for biannual IT assessment of the First Pacific cybersecurity environment; and
- Choosing an executive with appropriate knowledge and experience to take on the role of Head of Cybersecurity to liaise with third-party consultants, report to the Committee on cybersecurity incidents and take responsibility for management of all cybersecurity matters.

IT Support/Consultants are required to report perceived security breach incidents as soon as practicable to the Head of Cybersecurity. In addition, IT Support/Consultants conduct annual penetration tests of First Pacific's electronic network; additionally, the same test is conducted every two years by an independent IT auditor. Employees are required to report perceived cybersecurity incidents to IT consultant where possible and to the Head of Cybersecurity. All employees are required to escalate security incidents to a higher level of management such as supervisor or department head when there is reasonable basis to believe that no appropriate action has been taken by the IT consultant and Head of Cybersecurity.

For the sake of redundancy in reporting lines, people covered under the scope of this policy are also encouraged to report cybersecurity violations via the Company's Whistleblower Policy.

Dated 31 March 2022

###