1 ANNEX C – PRA IT DATA SYSTEMS SECURITY COMPLIANCE POLICY

PRA has a separate IT Data Systems Security Compliance policy aligned with the Principles of Business in relation to its Employees and Advisors and they are required to conduct their operations and activities in such a manner that they do not constitute a security risk to PRA and its Clients' intellectual property and data.

1.1 IT Data Systems Security Compliance Policy -

1.1.1 Overview

Our Data Systems Security Compliance Policy establishes our commitment to manage our engagement with any and all external Contractors, Consultants and Partners correctly and securely. We will treat the information of our customers, stakeholders, employees and other interested parties with the utmost care and confidentiality and ensure that any consultant we engage does the same.

With this policy we outline how we gather, store, handle/ delete/destroy (when and where necessary and appropriate) securely and safely in compliance with all relevant laws.

1.1.2 Scope

This policy refers to all digital and physical/printed information from all parties that interact with Employees and Advisors of PRA. This information can be stored in email systems, on databases and in file storage both on premise and in the cloud, and for physical data in locked and secure premises.

All Employees and Advisors, and any other external entity/entities which interacts with and exchanges data with PRA are covered by this policy.

1.1.3 Policy Elements for Data Security

Our company in its day to day work generally collects information regarding physical sites and assets as opposed to people. Where we reference people in reports it would be only to determine who is responsible or who was a contact at specific physical sites. No data beyond company email and phone for business contact purposes are kept for these people and this data is not recorded in public reports.

Our company holds extended personal information on employees, sub-contractors, and Associates/Consultants/Advisors that we engage with from time to time. Information can include all personal details, banking details, passport/ID, and visa details (among other things). All information is held with the full knowledge and cooperation of the relevant parties and is treated carefully. We store this in a business cloud solution (MS365) with appropriate access controls (only permitted employees can access it) and password policies.

Once we are storing personal information the following rules apply globally.

Our data will be:

- Accurate and kept up to date
- Collected only with the consent of the owner of the data for the purposes of engaging their services and nothing else
- Processed by PRA only within our legal boundaries
- Protected against any unauthorized or illegal access by internal and external parties by means of strict access control on a need to know basis.

Our data will NOT be:

- Communicated informally in any way
- Stored for longer than required
- Transferred outside of this company without the express permission of the owner of the data
- Distributed to any party without the express permission of the owner of the data (exempting legal requests from law enforcement authorities).

Our Obligations to the owners of the data are as follows:

- Inform them what data we hold and why
- Inform them as to who will have access to their data and why
- Have provisions in cases of lost, corrupted, or compromised data
- Allow people to request that we modify, erase, reduce or correct personal data contained in our databases at any time and without financial penalty.

1.2 Actions under the IT Data Systems Security Compliance policy

1.2.1 Advisors

To exercise data protection, we will implement the following for Advisors:

- Provide links to online IT security training that should be undertaken
- Restrict and monitor access to sensitive data through appropriate permissions and regularly audit these permissions
- Consultants will be given specific access to only the projects that they are working on and only for the duration of the project
- Where consultants are editing PRA related documents held in Microsoft 365 (MS365), all editing should be done through online tools so that local copies are not made.
- Where it is absolutely necessary to hold a local copy of a PRA document, the machine (desktop or laptop) should have bitlocker or equivalent encryption tool enabled to secure the data at rest. All such machines should have screen-locks enabled with password access required after 30 minutes of inactivity.
- Strong passwords will be required, and two factor authentication enabled.
- On ANY machine that holds a local copy of PRA data a local firewall and local upto date Anti-virus system must be enabled and active and bitlocker or equivalent encryption tool enabled to ensure encryption at rest.

1.2.2 Employees

To exercise data protection, we will implement the following for all Employees

- Restrict and monitor access to sensitive data through appropriate permissions and regularly audit these permissions
- Ensure that all access to Microsoft 365 (MS365) and to desktop and laptop machines is done through centralised Azure AD domain accounts.
- Establish an audit system to report on administrator activity in Microsoft 365 (MS365) that reports monthly
- Ensure that the office Firewall router is checked and patched monthly.
- Collect data only with consent and understanding of its use.
- All privileged remote access to PRA/its client network should follow security best practices (e.g., using secure protocols or connections along with MFA).
- Usage of insecure protocols or services are to be avoided at all costs.
- Train employees in data security and requirements.
- Utilize best in class data storage systems with strong passwords (that regularly change) and implement multifactor access for admin accounts.
- Establish clear procedures for reporting data breaches and data misuse.
- Establish best in class data protection practices (including but not limited to, document shredding, secure locks, data encryption, frequent backups, access authorization etc.).
- All desktops and laptops will be disposed of through a certified secure IT hardware disposal company

These data protection provisions will be available on our website.

1.3 PRA IT Systems

1.3.1 Data storage

All data will be stored in Microsoft 365 (MS365). Data servers are run by Microsoft and comply with all necessary laws and security standards. All server patching, security, AV, and physical access issues are managed by Microsoft.

- Data from this system can be mirrored to office desktop machines and /or company laptop machines. Office desktop machines will run Microsoft Windows 10 Pro or higher, the latest Apple OS machines with bitlocker [Mac equivalent FileVault] enabled.
- Office laptop machines will run Microsoft Windows 10 Pro or higher, the latest Apple OS machines with bitlocker [Mac equivalent FileVault] enabled.

Data shared with Advisors that are not direct employees will be subject to the "IT Data Systems Security Compliance Policy"

1.3.2 Desktop and Laptop Company Machines

The OS standard for all PRA company machines will be Windows 10 Pro or higher, the latest Apple OS. bitlocker [Mac equivalent FileVault] will be enabled on all drives. Access to the machine will be through Azure AD domain accounts which do not have local admin access. A local admin account will remain on the machine for admin purposes with a strong password secured in 1Password for admins only.

- Screensavers should automatically lock after 30 minutes and require a password/PIN to unlock.
- Automatic updates for the OS and all applications will be enabled.

1.3.3 System Security

ESET antivirus will be standard across all desktops and laptops and will be managed centrally through ESET Cloud Administrator.

- Local firewalls (Windows Defender) will be enabled by default on all machines.
- Security vulnerability scans will be conducted annually on external interfaces.

1.4 Disciplinary Consequences

All principles described in this policy must be strictly followed by Employees, Sub-contractors, and Associates/ Consultants / Advisors of Pacific Risk Advisors Ltd and any other related Group Companies.

A breach of data protection guidelines will invoke disciplinary action X, Y, Z and up-to possible termination of employment /contract and legal action .