**INFORMATION SECURITY POLICY**

[Last Updated: 10 August, 2021]

PREQUEL INTERNET TRADING LTD. (“**we**” “**us**” “**our**” or “**Prequel**”) is committed to provide transparency regarding the security measures which it has implemented in order to secure and protect Personal Data (as defined under applicable law, including the EU General Data Protection Regulation (Regulation 2016/679) (“**GDPR**”)) processed by the Company for the purpose of providing its services.

This information security policy (“**Policy**”) outlines the Company’s current security practices as of the “Last Updated” date indicated above. We will keep updating this Policy from time to time, as required by applicable laws and our internal policies.

As part of our GDPR we have implemented, technical organizational monitoring protections, and established an extensive information and cyber security program, all with respect to data processed by us. We take best efforts to ensure our employees, contractors, as well clients, comply with this Policy.

**System Access Control**

Access to all data processing systems is solely via Company’s user authentication systems. Company uses simple authentication and block access in any case of failed attempts or inactivity. There is clear identification or which employees are entitled to access the data. In addition, remote access and wireless computing capabilities are restricted and require that both user and system safeguards are in place. The systems are also protected and solely authorized employees may access the systems by using a designated password.

**Data Access Control**

The access to the Personal Data is restricted to solely the employees that are required to receive access and is protected by passwords according to defined password stipulations and user names. Access to the Personal Data is secured by VPN and is highly managed by access control policies. The Company uses high level security measures to ensure that the Personal Data will not be accessed, modified, copied, used, transferred or deleted without specific authorization. The scope of authorizations is limited in each case to the absolute minimum necessary for performing tasks or functions (logistic, chronological, etc.)

All transactions where Personal Data is read, inputted, changed and deleted are logged (user identifiers, transaction details) and archived.

**Physical Access Control**

The Company secures any physical access to facilities that contain Personal Data, such as the Company’s offices and server centers. The Company secures access to its offices and ensures that solely authorized persons have access. The Company’s servers are located in a protected facility in which the physical access is controlled by professional security staff. Further, the Company has entered in to applicable and binding processing agreements with each server service provider. The Company’s servers are protected by industry best standards of security systems and measures. The Company balances its approach towards physical security by considering elements of control that include architecture, operations, systems, performance, compatibility and interoperability.

**Organizational and Operational Security**

It is the responsibility of the individuals and personnel within the Company to comply with the Company’s practices and standards. The Company educates and provides ongoing training to its employees and service providers, consultants and contractors and raises awareness, risk and assessment with regards to any processing of Personal Data. Internal security testing is carried out on a regular basis. Further, the Company’s IT team ensures security of all hardware and software available within the Company, such as: install anti-malware software on computers to protect against malicious use and malicious software (additional controls may be implemented based on risk), virus detection on endpoints, email attachment scanning, system compliance scans, information handling options for the data exporter based on data type, network security, and system and application vulnerability scanning, use secured email transfer, etc.

**Transfer Control**

The goal of transfer control is to ensure that Personal Data cannot be read, copied, modified or removed by unauthorized parties during the electronic transmission of data or during their transport or storage in the applicable data center.

**Data Retention**

Personal Data as well as raw data are deleted as soon as possible or as soon as legally required.

**Job Control**

Employees and data processors are all signed on applicable and binding agreements all of which include applicable data provisions and data security obligations. Further, as part of the employment process, employees undergo a screening process applicable per regional law. Employees are bound to follow the Company’s policies and procedures and violations shall result in disciplinary actions up to and including termination of employment. An employee will not gain access to the Personal Data until the Company has trust that the employee is well educated and responsible to handle the Personal Data, if needed, in a secure manner. In addition, the Company hold annual compliance training which include data security education.

THE INFORMATION SECURITY, LEGAL, PRIVACY AND COMPLIANCE DEPARTMENTS WORK TO IDENTIFY REGIONAL LAWS, REGULATIONS APPLICABLE TO COMPANY’S COMPLIANCE. THEREFORE, THIS SECURITY POLICY MAY BE UPDATED FROM TIME TO TIME, ACCORDING TO ANY APPLICABLE LEGISLATION OR INTERNAL POLICIES.