Security Measures

As from the Agreement Effective Date, Pequity will implement and maintain the security measures set out below ("**Security Measures**").

1. Organisational management and staff responsible for the development, implementation and maintenance of Pequity's information security program.

2. Audit and risk assessment procedures for the purposes of periodic review and assessment of risks to Pequity's organization, monitoring and maintaining compliance with the Pequity's policies and procedures, and reporting the condition of its information security and compliance to internal senior management.

3. Data security controls which include at a minimum logical segregation of data, restricted (e.g. role based) access and monitoring, and utilisation of commercially available and industry standard encryption technologies for Customer Personal Data.

4. Logical access controls designed to manage electronic access to data and system functionality based on authority levels and job functions.

5. Password controls designed to manage and control password strength, expiration and usage.

6. System audit or event logging and related monitoring procedures to proactively record user access and system activity.

7. Physical and environmental security of data centres, server room facilities and other areas containing Customer Personal Data designed to protect information assets from unauthorised physical access or damage.

8. Operational procedures and controls to provide for configuration, monitoring and maintenance of technology and information systems, including secure disposal of systems and media to render all information or data contained therein as undecipherable or unrecoverable prior to final disposal or release from the Pequity's possession.

9. Change management procedures and tracking mechanisms designed to test, approve and monitor all material changes to the Pequity's technology and information assets.

10. Incident management procedures design to allow Pequity to investigate, respond to, mitigate and notify of events related to the Pequity's technology and information assets.

11. Network security controls that provide for the use of enterprise firewalls and intrusion detection systems designed to protect systems from intrusion and limit the scope of any successful attack.

12. Vulnerability assessment and threat protection technologies and scheduled monitoring procedures designed to identify, assess, mitigate and protect against identified security threats, viruses and other malicious code.

13. Business resiliency/continuity and disaster recovery procedures designed to maintain service and/or recovery from foreseeable emergency situations or disasters.

Pequity

Pequity may update or modify such Security Measures from time to time, provided that such updates and modifications do not materially decrease the overall security of the Services.