4.0 System security

4.1 Privacy and access control

Class' entire system is based on the concept of access on a need-to-know basis only. This is coupled with the use of privileges based on individual credentials. These are mapped in a highly granular fashion to ensure an individual user has access to only the data that they are entitled to view and modify. Clients are entirely partitioned off from each-other.

Physical access to the data storage devices is similarly restricted to an as-required basis.

The "access on a need-to-know basis" principle is also applied to Class staff.

4.2 Intrusion protection – cyber-crime and hacking

The term Intrusion in this context applies to Systems and the Communications Channels that connect users to those systems.

As well as the access control mechanisms described above, a number of other measures are implemented to prevent intrusion:

- Firewalls – limit access to required protocols only
- Proactive patch and update installation for key security related components
- Use of Anti-Virus software

All connections containing private session data are protected using a 128-bit encrypted channel. The protocols used also confirm the servers' identities though the use of site certificates.

4.3 Layered architecture

The use of a layered architecture (with a clear separation of User Interface, Business Logic and Data Access code) protects against most opportunistic intrusion techniques such as SQL injection. Appropriate validation is also used to guard against such attacks.

4.4 Penetration testing

Whilst Class has implemented many architectural and operational measures to prevent security breaches, it is best practice to conduct Penetration Tests to verify the efficacy of those measures empirically.

As such, Class ensures Penetration Tests are conducted on a regular basis.