CONNECTUM Security Policy Summary

In providing payment services to its clients Connectum Limited (CONNECTUM, we) uses best-in-practice industry standards, proprietary security, physical security and cryptography technologies to insure information confidentiality and integrity and assets safety. This CONNECTUM Security policy summary sets forth our general approach in the implementation and compliance of our internal security standards and issues providing payment services.

CONNECTUM ensures PCI DSS compliance for all Payment card services as well as a range of other industry measures for secure payment card processing such as 3D secure, AVS and Anti Fraud Modules.

In respect of payment transactions we are always validating and verifying user credentials; strong authentication deploying two-factor authentication principle is used.

We are:

- using strong cryptography to protect data and information in rest and movement;
- performing detailed logging and its integrity of IS and Payment services data;
- using secure communication protocols;
- continuously monitoring our systems for possible vulnerabilities and attacks;
- ensuring that all of the information within our environment is managed and protected based on its value and classification. We always follow to and are in compliance with all necessary legal, regulatory and contractual requirements.

Our Information System (IS) infrastructure is being constantly tested by our highly qualified security specialists and licensed companies to ensure it's best protection.

CONNECTUM is ensured for its secure business operations and always knows what to do, even on severe destructive events or force majeure regarding its strong administrative security control which includes developed BCP.

Security at CONNECTUM is a part of every employee’s responsibilities.
All our employees are encouraged to report on any security breach or potential security breach.
CONNECTUM is supportive of an open environment for feedback and practices direct communication between staff of all levels and departments. Investigation and follow-up will be done by senior management regards all reported issues.

However we are hereby asking you as our client to perform the following actions also yourself to better protect the assets:

- keep your personalised credentials and payment instruments in secure manner;
- notify us immediately about your personalised credentials loss or compromise using the following phone number: +44 74 6855 9423 (Office working hours), or office out-of-hours 24/7 hotline number +44 77 1919 5909
- use up to date anti-malware software solutions.

Please remember, we will never ask you for your account credentials or personally identifying information via email, SMS or social media.