BRICKHILL CAPITAL (CY) LIMITED

INFORMATION TECHNOLOGY POLICY

1. Introduction

This policy aims to depict the procedures for the Information Technology (hereafter “IT”) function of Brickhill Capital (CY) Limited (hereafter the Company).

The IT policy ensures that the Company is providing financial services efficiently, honestly and fairly as required under European law as well as CySEC regulations.

All Brickhill Capital (CY) Limited employees are expected to conduct their business activities honestly, transparently and with integrity and any suspicion of bribery or corruption is considered a potential compliance breach and must be reported and managed in accordance with the Incident, Breach and Escalation Policy.

2. Purpose

The purpose of this document is to ensure that appropriate measures are put in place to protect corporate information and the Information Technology systems, services and equipment of Brickhill Capital (CY) Limited and associated infrastructure.

The objectives of the Information Security Policy are:

- To secure Brickhill Capital (CY) Limited assets against theft, fraud, malicious or accidental damage, breach of privacy or confidentiality; and
- To protect Brickhill Capital (CY) Limited from damage or liability arising from the use of its facilities for purposes contrary to CySEC regulations, the permitted law or company policy.
- To document how we effectively safeguard and controls over the IT systems that we used to deliver our licensed services are secure and reliable and that our arrangements ensure we perform efficiently and associated risks are managed (such as human error, technical failure and malicious conduct).
- To ensure data and system security – and prevent errors or system failure
- To ensure that we have proper back up and a business continuity plan
- To ensure we have proper legal arrangements with any third-party software providers, including licensees for software and contracts for any required maintenance and support
- Document the regular reviews that are done on our IT systems and anticipate increase in demand so that our resource remains appropriate for the scale and complexity of our licensed business.

3. Scope

This policy applies to all Brickhill Capital (CY) Limited staff, contractors, associates or any other persons otherwise affiliated but not employed by Brickhill Capital (CY) Limited, who

may utilize Brickhill Capital (CY) Limited Technology infrastructure and/or access the Company's applications with respect to the security and privacy of information.
The department will be internally managed by the Head of Information Technology and the Company will also receive outsourced support from SPA DATA4U LTD, a third-party provider, whose main duty is to ensure the Security and Integrity of:

- the network used by the Company
- the trading platform which is used by the Company's personnel and clients
- the servers and personal computers of Company's personnel

The Head of the Department is reporting to the Senior Management of the Company who is responsible for the supervision of the Department. In addition, the Department is also monitored by the Compliance Officer and the Internal Auditor of the Company in order to ensure that the procedures followed by the Company are duly in line with sections of Record Keeping and Business Continuity Policy of the Company's Internal Procedures Manual.

4. Procedures

a) Staff Security

The department provides to its staff with access to computing and communications services to support of its business activities. These facilities include access to email, internet, file and print services, an integrates data network across all offices.

Users are responsible for maintaining the use and security of their assigned User ID's and all activity associated with that ID. Knowing disclosing passwords to others will be deemed a breach of policy and could be referred to disciplinary procedures. The Company expects its staff, contactors and associates to take all reasonable steps to ensure the integrity and security of the technology systems and data.

In order to identify and address bribery and corruption risks, the Company ensures the ongoing training of employees operating in areas of high risk and uses standard clauses relating to bribery act issues for inclusion in key contractual documentation.

Where temporary access is required for a specific purpose, but not restricted to, contract workers and 'test' accounts, a user is expiry date based on the completion date of the required tasks must be used to ensure the temporary account is not accessible after the date.

In the case of ongoing maintenance and support from 3rd party companies, access must only be granted to the relevant facilities within the system and be restricted to only the systems for which they provide support

b) Information Technology Security/Software Security

For the Company, due to the nature of its operations and activities, Information Technology Security is an important issue, and the Department is having in place procedures to ensure the efficient and effective application of the Information Technology Security. The Company must implement a suitable environment that protects the integrity, availability and confidentiality of Brickhill Capital (CY) Limited data by using logical controls and processes.

The following actions are taken by the Department:

Software Security

- All users of the network are supplied with a User Account for authentication and allocation of appropriate access rights network facilities including software. Access to such network facilities and software is also controlled by the use of secure passwords which must be changed every 90 days. All Brickhill Capital (CY) Limited staff PCs and laptops must be set with an inactivity screensaver which requires a unique password to reactivate the underlying session and has an idle time of no more than 10 minutes before activation.
- As a means of allocating appropriate software packages to specific users, the use of an application deployment tool should be used. This can grant individuals or groups access to various programs and services in accordance to their duties and requirements through their user account. Any software deployment that may cause harm or impact the IT resources of Brickhill Capital (CY) Limited in an adverse manner including, but not restricted to, scanning, gaining un-authorised access, exploiting vulnerabilities to take advantage of exploits, will be looked upon as inappropriate and treated as a direct attempt to compromise Brickhill Capital (CY) Limited computing facilities and / or infrastructure and will be dealt with accordingly
- Access to servers and networks firewalls is restricted only to authorized Information Technology personnel. The Information Technology personnel are being granted the access either for configuration tasks or at regular intervals for the monitoring of the servers and networks

End-Point Security and Antivirus Software

- All Standard Operating Environment (SOE), the Company issued PCs and laptops have end-point security software installed which has an automatic pattern update feature enabled. This is to ensure that the software is kept updated for the latest threats and antivirus systems in place checking all incoming email into the organisation.
- This SOE will include all the software required for staff to complete their duties. Requests for new software must be submitted to Technical support for assessment and where appropriate they will be added to the SOE via a centralised system.
- Constant updating of the antivirus software that is in use for protecting the personal computers in use by the Company’s personnel. The update is performed hourly to ensure maximum security and protection.
- Regular updates of the servers thus ensuring the maximum security of the data stored. The maximum security is essential for protection of the data in terms of both malicious attacks and the loss of data due to ‘Significant Business Interruptions’. The updates are both operating system and application updates.

Passwords

- Passwords are provided to users of the different software in use by the Company. It is the responsibility of the personnel for all transactions/actions made while their password is in use. For security reasons, no user is allowed to access the server/network with another user's account and password.
- Staff passwords are to meet complexity rules as set by the Identity and Access Management System. These complexity rules will include a minimum password length, character requirements and suitable password expiry period.
- In the event that access is required to Brickhill Capital (CY) Limited data that is held under a specific staff members user id and password and that staff member is unavailable to access the data due to unforeseen circumstances, a request to have the password reset may be made with the authorisation of the Head of Human resources or delegated officer. This will only be considered when all other avenues to access the data have been exhausted. At the completion of the task accessing the required data, the password MUST be reset again and the staff member notified as soon as is practical.
- It is essential that those requiring access to the Company's computing facilities be issued with a unique login and password. The password is not to be shared with, or used by, any other individual and failing to comply will be treated as a serious breach of system security which may result in disciplinary action.

c) Physical Security

The Company must ensure that the physical ITS devices are kept safe from inappropriate access. This includes the physical access to the server room, switch and patch panel cabinets, and any other ITS devices in both restricted and public access areas.

- All offices, computer rooms and work areas containing confidential information, or access to confidential information must be physically protected. This means that the area must be supervised, so that the information is not left unattended, and when unattended the area must be locked, or the information locked away.
- It is a requirement that any PC / Laptop / Portable computer be logged out or locked when not in use. Technology systems employed in the Company will automatically lock computers that have not detected use after 15 minutes of inactivity.

d) Building Security

The Department through an electronic access control system ensures that business security is in place as required by Law that all Company's premises are controlled, monitored and are secure. Access to the buildings is only through access cards provided to all relevant people and it is their responsibility for the safeguarding of the access cards.

  - Access to computer work areas must be restricted by keys, cipher locks or proximity access cards during office hours and can only be accessible by authorised individuals after hours
- Combinations or access details must be changed / deleted when a staff member leaves or loses their card or key.
- If door and keys have been used for other purposes, key cylinders must be replaced with a brand-new lock and keys restricted to an absolute minimal number of persons.
- Access to restricted computer work areas can only be given when an authorised staff member is inside and can and will supervise the visitor's movements completely or hand over to successive staff.
- When unattended and after hours, doors must be secured.
- Access to restricted computer work areas will be protected by video surveillance. Other workers must not attempt to enter restricted areas in the Company’s facilities for which they have not received access authorisation.

5. Software licensing

Brickhill Capital (CY) Limited will make all reasonable efforts to ensure that all software used to provide our services will be appropriately and fully licensed with our vendors. Regular review and adjustments will be made to ensure continued compliance and to reduce overspend on licensing.

6. Confidential Data Security

To ensure the confidentiality and security of staff personal information contained on the Brickhill Capital (CY) Limited technology facilities, it is essential that only those authorised to access such data are permitted to do so. Those who are permitted to access such information are granted appropriate access.

Anyone who gains access to such personal information through methods other than those permitted by their roles shall be deemed as unauthorised and subject to disciplinary action.
Staff should be aware of their legal and corporate responsibilities in relation to appropriate use, sharing or releasing of information to another party. Any other party receiving restricted information must be authorised to do so and that the receivers of the data also adopt information security measures to ensure the safety and integrity of the data.

7. Communications Security

Communications can take various forms which include, but are not restricted to, voice via land line, voice via mobile phone, voice via computer network (VOIP), email, electronic file transfer, wireless access, Virtual Private Network (VPN) connections, dial up modem, Infra-Red, Bluetooth and ITS network infrastructure.

8. Removal of Equipment

No computer equipment can be removed from the Brickhill Capital (CY) Limited facilities unless specific authorisation has been received by the Head of Technology or Chief Information Officer. This does not apply to laptop or notebook computers where one of their primary purposes is to allow the custodian to work while away from their normal working location.

Any equipment taken from Brickhill Capital (CY) Limited facilities without appropriate authorisation will be in direct violation of this policy and appropriate misconduct and / or legal action will be taken.

9. Asset Disposal

When disposing of technology assets such as computers, laptops, printers etc, the disposal must be co-ordinated with Brickhill Capital (CY) Limited technical support personnel to ensure that all data is removed using appropriate data removal tools. This process will also remove any and all software installed by the Company to ensure compliance with software licensing agreements.

10. Incident Management

Specify how any breaches of security relating to the information systems will be identified and handled.

a) Reporting Security Problems

Any suspected inappropriate or illegal usage of Brickhill Capital (CY) Limited Information services network and equipment should be reported to the Service Desk or division head immediately. This information will then be reported to the Compliance for investigation.

b) Escalation

The escalation process for the rating of each reported event will be determined by the Information Technology department member in conjunction with a Compliance department member taking into account the event itself and other priorities at that time.

c) Monitoring and Reporting

Brickhill Capital (CY) Limited will implement where appropriate system level monitoring that will review system logs and flag events to a ticketing system and in some cases, an operational dashboard for technical teams to review and action.

Brickhill Capital (CY) Limited will engage a third party to manage and monitor network devices who will mitigate and report security breaches or performance problems at the network level.

Brickhill Capital (CY) Limited will conduct yearly audits with a security provider to review and test aspects of Company’s infrastructure for security vulnerabilities.

11. Business Continuity

How to ensure that there will be minimal disruption to Information Technology services in the event of a disaster or the implementation of changes to systems and/or associated infrastructure.

a) Backup Requirements

All major systems within Brickhill Capital (CY) Limited computing infrastructure are backed up on a regular basis. Information Technology Services have a Backup Strategy which details the frequency of backups. It is also strongly advised that all users save their work to their network drive as this drive is backed up and any loss or damage to files can often be rectified by the restoration of the files from an existing backup.

b) Change Control

To ensure that the Technology facilities and services running within the Brickhill Capital (CY) Limited infrastructure are maintained and kept running at maximum performance and functionality, it is often a requirement to perform maintenance and upgrades to equipment. To ensure that there is minimal disruption to essential services, appropriate Change Control procedures are to be followed. This is to ensure that the disruption is kept to a minimum and appropriate deployment and roll back procedures exist should there be issues during the system changes.

c) Redundant Systems

To reduce the impact to critical systems caused by underlining failures the system design of these systems will take into consideration methods and means to support failover to secondary systems.

d) System capacity

In order to ensure that systems continue to operate at appropriate levels of performance system metrics will be collected and monitored by a centralised monitoring solution. Any breach of performance thresholds will be reported to the technical service team for review with upgrades to be planned where appropriate. Brickhill Capital (CY) Limited systems were possible will be hosted on cloud infrastructure allowing for the rapid increase of resource or removal of over allocated resources to manage costs.

When this is not available appropriate levels of spare compute resources will be provisioned to ensure expansion, capacity is available when required. This can be cost prohibitive for some environments and for these systems the monitored thresholds will be widened to account for expected upgrade provisioning time when required.

12. Technology systems that deliver the License Service

Brickhill Capital (CY) Limited will use a number internal and third party managed systems and services to deliver our licensed services to our clients. These systems will be fully licensed and all have appropriate service and/or support agreements in place where applicable. Where possible pro-active monitoring will be put in place to ensure quality and reliability of these systems.

a) Pricing and Execution systems

Pricing & execution systems will be configured in a redundant manner. Multiple aggregation providers will be available to our internal environments for this purpose. These systems will have multiple underlining liquidity providers to ensure pricing is accurate and timely. Monitoring systems will be in place to proactively ensure the speed and health of these systems.

b) Onboarding systems

Brickhill Capital (CY) Limited uses the globally recognised CRM product Salesforce to collect and hold information required to complete KYC/AML checks on its clients. Data transfers between this system and Brickhill Capital (CY) Limited will be encrypted using up to date industry standard encrypting keys and ciphers. Brickhill Capital (CY) Limited will engage with electronic verification providers for screening during the onboarding process.

c) Funding and Withdrawal systems

Brickhill Capital (CY) Limited will make available multiple payment and withdrawal methods to its clients. Anti-fraud protections will be implemented to reduce risk of fraud. Funding trend data will be analysed with a suspicious activity report generated daily for review. Any information in transit will be encrypted using up to date industry standard encrypting keys and ciphers. No Payment Card Industry (PCI) data will be saved to Brickhill Capital (CY) Limitedtd systems. Brickhill Capital (CY) Limitedwill instead utilise PCI compliant payment gateway providers to process payments.

d) Back Office systems

Brickhill Capital (CY) Limited will use a fully licensed back office system to handle settlements, reconciliations, counter party risk management, client margining, accounting, fees and charges.

e) Reporting and Risk management systems

Brickhill Capital (CY) Limited will maintain data storage systems to house all transaction data for regulatory and internal reporting purposes. These systems will feed into our proprietary Risk management platform to provide real time aggravated dashboards used by our trading teams to make trading decisions.

f) Integration systems

Brickhill Capital (CY) Limited will use an enterprise level service bus to handle the transfer of information though out each of the core systems. This data in standardised and transmitted in a transactional manner to ensure no loss of messages.

13. Implementation, Review and Monitoring

Brickhill Capital (CY) Limited ensures the effective implementation of this Policy to ensure that all employees are aware of their obligations regarding IT Security. All relevant new starters must read this policy when they join.

This Policy is reviewed to monitor its effectiveness and to consider its suitability, adequacy and identify any deficiencies. Where necessary, it will be updated to ensure that the Policy is in line with all regulations, updates and notifications to keep Brickhill Capital (CY) Limited compliant and performing to their best ability. Review and assessment of this Policy will be carried out at least annually or whenever a material change occurs. Any changes to this Policy will be communicated down to the business.

Compliance with this Policy ensures Brickhill Capital (CY) Limited meets its obligations. Apart from what has already been covered off in the policy, the Company’s Compliance department will also monitor this Policy’s use and effectiveness through ensuring that:

- all Brickhill Capital (CY) Limited employees attest annually that they understand and comply with this Policy;
- Review to ensure that the current policy reflects correctly the IT Systems that Brickhill Capital (CY) Limited uses.