Information Security Policy

The Board of Directors and management of Exclusive Change Capital Ltd, located at 56 Theodorou Potamianou, 4th Floor, Aphrodite building, 4155, Limassol, Cyprus, which [operates in financial services sector], are committed to preserving the confidentiality, integrity and availability of all the physical and electronic information assets throughout their organization in order to preserve its competitive edge, cash-flow, profitability, legal, regulatory and contractual compliance and commercial image. Information and information security requirements will continue to be aligned with Exclusive Change Capital Ltd's goals and the ISMS is intended to be an enabling mechanism for information sharing, for electronic operations, [for e-trading] and for reducing information-related risks to acceptable levels.

Exclusive Change Capital Ltd's current strategic business plan and risk management framework provide the context for identifying, assessing, evaluating, and controlling information-related risks through the establishment and maintenance of an ISMS. The Risk Assessment, Statement of Applicability and Risk Treatment Plan identify how information-related risks are controlled. Head of Risk and external consultant (when applicable) is responsible for the management and maintenance of the risk treatment plan. Additional risk assessments may, where necessary, be carried out to determine appropriate controls for specific risks.

Business continuity and contingency plans, data backup procedures, avoidance of viruses and hackers, access control to systems and information security incident reporting are fundamental to this policy. Control objectives for each of these areas are contained in the Manual and are supported by specific documented policies and procedures.

Exclusive Change Capital Ltd aims to achieve specific, defined information security objectives, which are developed in accordance with the business objectives, the context of the organisation, the results of risk assessments and the risk treatment plan.

All Employees/Staff of Exclusive Change Capital Ltd [and certain external parties identified in the ISMS] are expected to comply with this policy and with the ISMS that implements this policy. All Employees/Staff, and certain external parties, will receive appropriate training. The consequences of breaching the information security policy are set out in the Organization's disciplinary policy and in contracts and agreements with third parties.

The ISMS is subject to continuous, systematic review and improvement.

Exclusive Change Capital Ltd has established [a top-level management steering group/ Information Security Committee, chaired by Chief Executive Officer (CEO)/Chief Information Security Officer (CISO) and including the Information Security Manager and [other executives/specialists/risk specialists] to support the ISMS framework and to periodically review the security policy.]

Exclusive Change Capital Ltd is committed to achieving certification of its ISMS to ISO27001:2013.

This policy will be reviewed to respond to any changes in the risk assessment or risk treatment plan and at least annually.

In this policy, 'information security' is defined as:

Preserving

This means that management, all full time or part time *[employees/staff]*, sub-contractors, project consultants and any external parties have, and will be made aware of, their responsibilities (which are defined in their job descriptions or contracts) to preserve information security, to report security breaches (in line with the policy and procedures identified in Section 16 of the Manual) and to act in accordance with the requirements of the ISMS. All *Employees* will receive information security awareness training and more specialized *Employees* will receive appropriately specialized information security training.

the availability,

This means that information and associated assets should be accessible to authorized users when required and therefore physically secure. The computer network must be resilient and *Exclusive Change Capital Ltd* must be able to *[detect and]* respond rapidly to incidents (such as viruses and other malware) that threaten the continued availability of assets, systems and information. There must be appropriate business continuity plans.

confidentiality

This involves ensuring that information is only accessible to those authorized to access it and therefore to preventing both deliberate and accidental unauthorized access to *Exclusive Change Capital Ltd*'s information *[and proprietary knowledge]* and its systems *[including its network(s), website(s), extranet(s), and e-trading systems], catering also various GDPR specific control/compliance requirements.]*

and integrity

This involves safeguarding the accuracy and completeness of information and processing methods, and therefore requires preventing deliberate or accidental, partial or complete, destruction or unauthorized modification, of either physical assets or electronic data. There must be appropriate contingency *[including for network(s), e-commerce system(s), website(s), extranet(s)]* and data backup plans and security incident reporting. *Exclusive Change Capital Ltd* must comply with all relevant data-related legislation in those jurisdictions within which it operates.

of the physical (assets)

The physical assets of Exclusive Change Capital Ltd including, but not limited to, computer hardware, data cabling, telephone systems, filing systems and physical data files.

and information assets

The information assets include information printed or written on paper, transmitted by post or shown in films, or spoken in conversation, as well as information stored electronically on servers, website(s), extranet(s), intranet(s), PCs, laptops, mobile phones and PDAs, as well as on CD ROMs, floppy disks, USB sticks, backup tapes and any other digital or magnetic media, and information transmitted electronically by any means. In this context, 'data' also includes the sets of instructions that tell the system(s) how to manipulate information (i.e. the software: operating systems, applications, utilities, etc.).

of Exclusive Change Capital Ltd.

Exclusive Change Capital Ltd and [such partners that are part of our integrated network and have signed up to our security policy and have accepted our ISMS].

The ISMS is the Information Security Management System, of which this policy, the Information Security Manual ('the Manual') and other supporting and related documentation is a part, and which has been designed in accordance with the specification contained in ISO27001:2013.

A **SECURITY BREACH** is any incident or activity that causes, or may cause, a break down in the availability, confidentiality, or integrity of the physical or electronic information assets of Exclusive Change Capital Ltd.