The Board of Directors and management of Retirement Capital, located at 18 Soho Square, London, W1D 3QL, which operates in IT services sector, are committed to preserving the confidentiality, integrity and availability of all the physical and electronic information assets throughout their organisation 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 Retirement Capital’s goals and the ISMS is intended to be an enabling mechanism for information sharing, for electronic operations, application and cloud services and for reducing information-related risks to acceptable levels.

The ISMS will encompass all functions of Retirement Capital, including:

* All Administrative functions, including the management of employee and contractor records.
* All Sales functions, including the management of customer commercial records.
* All Operational functions, including the management of customer operational records, sub-contractor records and services conducted by staff and contractors.
* All sub-contractors that hold or process information related to staff, customers, sub-contractors, contractors, customers or subjects of customers and any other sensitive information held or processed by Retirement Capital

The scope of this ISMS is all operations of Retirement Capital, including but not limited to:

* Internal information technology, including:
  + Company owned desktop and laptop computers, servers, peripherals and storage media.
  + Independently owned desktop and laptop computers, peripherals and storage media, that is used on behalf of Retirement Capital and its customers.
  + Cloud services, including Microsoft Office 365 and Google Aps that is used to store company or customer information.
  + Servers and storage media hosted by third parties that contain company or customer information.
  + Servers and storage media owned and managed by third parties that contain company or customer information.
  + All physical media (paper, DVDs, memory sticks) that contains company or customer information.
  + All company or privately-owned SmartPhones that store company or customer information.

Retirement Capital’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. The Head of Operations 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.

In particular, 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](../Manual/001%20Information%20Security%20Manual.docx) and are supported by specific documented policies and procedures.

Retirement Capital 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 Retirement Capital 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 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.

Retirement Capital has established an ISMS committee, a top-level management steering group, chaired by the Chief Information Security Officer (CISO (DIRECTOR)) and including the Managing Director and other executives to support the ISMS framework and to periodically review the security policy.

Retirement Capital is committed to achieving certification of its ISMS to ISO27001:2017.

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/Staff will receive information security awareness training and more specialised Employees/Staff will receive appropriately specialised information security training.

***the availability,***

This means that information and associated assets should be accessible to authorised users when required and therefore physically secure. The computer network must be resilient and Retirement Capital 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 authorised to access it and therefore to preventing both deliberate and accidental unauthorised access to *Retirement Capital*’s information, customer information and its systems including its network(s), website(s), extranet(s), cloud applications and services, and e-commerce systems.

***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 unauthorised modification, of either physical assets or electronic data. There must be appropriate contingency, including cloud applications and services, network(s), e-commerce system(s), website(s), extranet(s) and data backup plans and security incident reporting. Retirement Capital must comply with all relevant data-related legislation in those jurisdictions within which it operates.

***of the physical (assets)***

The physical assets of Retirement Capital 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 Retirement Capital.***

Retirement Capital 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 ISO27001:2017.

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 Retirement Capital.

***Document Owner and Approval***

The Information Security Manager is the owner of this document and is responsible for ensuring that this policy document is reviewed in line with the requirements in Clause 5.1.2 in the Manual.

A current version of this document is available to all members of staff on the Company Intranet. It does not contain confidential information and can be released to relevant external parties.

This information security policy was approved by the Board of Directors on 14th November 2020 and is issued on a version-controlled basis under the signature of the Managing Director.

Signature: Date: 14/11/2020

**Change History Record**

|  |  |  |  |
| --- | --- | --- | --- |
| Issue | Description of Change | Approval | Date of Issue |
| 1 | Initial issue | Gavin McCloskey | 14/11/2020 |
|  |  |  |  |
|  |  |  |  |