1. **Scope** [ISO27002 Clauses 11.1.2 and 11.1.3]

All designated secure areas (see [ISMS-C DOC 11.1.11](ISMS-C_DOC_11.1.11.docx) and [ISMS-C DOC 11.2.1](ISMS-C_DOC_11.2.1.docx)) on any of Retirement Capital’s premises are subject to controlled access and usage.

1. **Responsibilities**

* 1. Every secure area has an owner (see control section 8.1.2 of the [Manual](../Manual/001%20Information%20Security%20Manual.docx)) and the owner is responsible for ensuring that prescribed controls are maintained and as otherwise specified below. The main office is a secure area.
  2. The Premises Manager is responsible for authorising access to secure areas.
  3. All employees/staff, contractors and third parties have certain responsibilities as defined below.

1. **Procedure**
   1. Secure areas must be locked at all times. The lock specification is combination lock. The owner must check the secure area at least once per day, even if no one is working in it.
   2. Access to secure areas/areas where confidential or restricted information is processed (including in conversation) or stored is restricted to authorised persons. Authorisation is provided by the Administrator.
   3. Access to secure areas requires authentication and authorised persons are issued with an ID card.
   4. The owner of a secure area is responsible for ensuring that no unsupervised working takes place within the secure area.
   5. The authentication system retains a record of accesses and these are reviewed monthly to identify any unauthorised accesses.
   6. The owner of a secure area is responsible for ensuring that photographic, video, audio or other recording equipment and mobile phone cameras, are not taken into the secure area.
   7. All employees/staff, contractors and third parties are required to wear an identification badge containing a photograph and name that is issued by the Company Administrator and are required to notify security if they encounter unescorted visitors and anyone not wearing required identification (see [ISMS-C DOC 11.1.2d](file:///C:\Users\Sarah\Documents\ISO%209001\ISO%2027001\Section6\RiskMngmt\Control-A11\ISMS-C_DOC_11.1.2D.docm)).
   8. Third party support personnel only have access to secure areas when required and this access is specifically requested, authorised and monitored All visitors are required to log in at The Office Group reception and will be escorted at all times by their host. Visitor access must be authorised by a Manager or Director.
   9. In general, the owner of a secure area and all those who are authorised to work within it, are required only to divulge details of the area and what is done in the area to other employees/staff on a need-to-know basis.

***Document Owner and Approval***

The Director (CISO) is the owner of this document and is responsible for ensuring that this procedure is reviewed in line with the review requirements of the ISMS.

A current version of this document is available to all members of staff on the corporate intranet.

This work instruction was approved by the Director (CISO) on 14th November 2020 and is issued on a version-controlled basis under his/her signature.

Signature: Date: 14/11/2020

**Change History Record**

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