1. **Scope**

Retirement Capital’s Information Security Continuity Plan and all its sub-plans are within the scope of this procedure.

1. **Responsibilities**

The Information Security Manager is responsible for the testing, maintenance and re-assessment of information security continuity plans.

The Information Security Manager is responsible for ensuring that all information security issues have been included and appropriately treated in these business continuity plans and is also responsible for any revised information security continuity risk assessments that might be required through the testing process.

The Department Manager is responsible for key processes are also required to support the Information Security Continuity testing plan and ensure that all continuity plans and fallback arrangements for their assets/processes are proven to work.

1. **Procedure** (ISO27002 Clause 17.1.3)
   1. It is a requirement of the Change Control Procedure ([ISMS-C DOC 12.1.2](../Control%20A12%20-%20operations%20security/ISMS-C_DOC_12.1.2.docx)) that changes affecting information security be reflected in the information security continuity plans. Specifically, changes to personnel, addresses or telephone numbers, locations, equipment, systems, facilities, contracts or key customers, must be incorporated into updated versions of the information security continuity plan on a monthly basis.
   2. Changes in business strategy, legislation, and risk (either financial or operational) are notified to the Operations Director by the Chief Information Security Officer (CISO (DIRECTOR)) as and when they occur, and the information security continuity plans – and their test program – are updated to take account of these changes. This updating might require a new risk assessment ([ISMS-C DOC 17.1.2](ISMS-C_DOC_17.1.2.docx)).
   3. Retirement Capital’s information security continuity plan and its sub-plans are tested in line with the timetable set out in ISMS-C-REC 17.1.3.
   4. The frequency of tests is determined by the likelihood of the identified threat and its potential impact; the continuity plans for those processes that are most at risk are tested most often and the reasons are set out in the test plan, which is signed off by the Information Security Committee.
   5. All individuals identified in that part of the plan being tested are required to be involved in the planned test; the Information Security Manager keeps an attendance record and minutes of tests that identify actions arising from the testing.
   6. The results of each test are recorded, possible improvements identified and implemented and the Information Security Committee reviews the minutes of business continuity tests on a quarterly basis.

***Document Owner and Approval***

The Information Security Manager 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 procedure was approved by the Chief Information Security Officer (CISO (DIRECTOR)) 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 |
|  |  |  |  |
|  |  |  |  |