1. **Scope**

Any event that might interrupt one (or more) of Retirement Capital’s information security processes is within the scope of this procedure.

1. **Responsibilities**

The Information Security Manager is responsible for ensuring that all information security issues have been included and appropriately treated in these information security continuity plans and is also responsible for information security continuity risk assessments.

Department Managers are responsible for key processes and the owners of those processes are also responsible for identifying the information security continuity risks to their processes and then identifying and implementing the steps necessary for their continuity.

1. **Procedure** [ISO27002 Clause 17.1.1]
   1. Retirement Capital’s critical information security processes and controls are identified and listed in order of importance (in an information security process risk log ISMS DOC 17.1.4), and their component information assets cross-referenced to the asset inventory created in line with the requirements of [ISMS-C DOC 8.1.1](../Control%20A8%20-%20asset%20management/ISMS-C_DOC_8.1.1.docx), all as required by [ISMS-C DOC 17.1.1](ISMS-C_DOC_17.1.1.docx).
   2. Within the context of Retirement Capital’s risk management framework ([RM-ISMS DOC 6.1.1](../Section%206%20-%20planning/RM-ISMS_DOC_6.1.1.docx)), the risk assessment procedure ([RM-ISMS DOC 6.1.2](../Section%206%20-%20planning/RM-ISMS_DOC_6.1.2.docx)) is applied to identify the risks to these information security critical processes.
   3. Possible information security continuity impacts are, as required by ISMS DOC 17.1, identified for each of the risks and these possible impacts assessed, taking into account time aspects, scale of damage and period of time required for recovery. Where there are linkages between assets, processes, vulnerabilities or risks, these are considered to identify the circumstances in which the impacts may be worsened by the linkages.
   4. For each of the identified risks, there is a decision as to whether it should be accepted, rejected, transferred or controlled. Control options are considered, as required by RM-ISMS DOC 6.1.2, and reasons for the final choices are documented.
   5. Where a control cannot function during a continuity event, compensating controls may be chosen and recorded in line with 3.4 above.
   6. Retirement Capital will then prioritise its information security continuity planning activities in the light of the assessment of risks, tackling first those risks whose significance is considered greatest.

**Document Owner and Approval**

The Operations Director 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 |
|  |  |  |  |
|  |  |  |  |