1. **Scope**

Retirement Capital’s entire ISMS is within the scope of this procedure.

1. **Responsibilities**

All Managers throughout Retirement Capital are responsible for ensuring and checking for procedural compliance.

The Information Security Manager is responsible for planning and commissioning technical compliance checking.

1. **Procedure**

**Management Review** [ISO27002 Clause 18.2.2]

1. On a Quarterly basis, Manager will review operational conformance with those organisational policies and procedures that apply to the information assets for which they are responsible/whose owners report to them. Manager are not responsible for performing or commissioning technical compliance checking.
2. The review must be reported/recorded on [ISMS-C-REC 18.2.2](ISMS-C_REC_18.2.2.docx)
3. Where a non-conformance is identified, the Manager must determine the cause of the non-conformance, evaluate what action is required to ensure that the non-conformance does not re-occur, determine necessary corrective action (including obtaining any required authorisations) and take the identified action.
4. The details of the corrective actions, and confirmation of their successful implementation, should also be recorded on [ISMS-C-REC 18.2.2](ISMS-C_REC_18.2.2.docx)
5. Review reports are made available to independent reviewers carrying out independent reviews in line with [ISMS-C DOC 18.2.1](ISMS-C_DOC_18.2.1.docx).
6. Manager is also responsible for identifying non-conformances in the ordinary course of business and taking appropriate corrective action.
7. **Technical Compliance Checking** [ISO27002 Clause 18.2.3]
   1. The Information Security Manager has a schedule of Retirement Capital’s information assets (gathered under [ISMS-C DOC 8.1.1](../Control%20A8%20-%20asset%20management/ISMS-C_DOC_8.1.1.docx)) and these are prioritised by importance to Retirement Capital.
   2. All assets are checked for technical compliance with their documented configuration requirements on a quarterly basis. This includes periodic penetration testing of all websites and Internet-facing applications and connectivity.
   3. Retirement Capital requires that any person/organisation who carries out technical compliance checking has the necessary expertise.
   4. The Information Security Manager approves the technical checking plan put forward by the contracted technical compliance checking team/organisation and authorises commencement of the check plan only when satisfied that the testing will not compromise the asset or system being checked.
   5. Non-conformances are identified and dealt with as described in Section 3, above.
   6. New weaknesses or vulnerabilities uncovered as a result of the technical compliance checking are reported in line with [ISMS-C DOC 16.1.2-3](../Control%20A16%20-%20information%20security%20incident%20management/ISMS-C_DOC_16.1.2-3.docx) and dealt with in line with [ISMS-C DOC 16.1.5](../Control%20A16%20-%20information%20security%20incident%20management/ISMS-C_DOC_16.1.5.docx).

***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 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 |
|  |  |  |  |
|  |  |  |  |