1. **Scope**

All problems and potential improvements identified within the Information Security Management System fall within the scope of this procedure.

This procedure also serves as an improvement suggestion scheme.

The objective of this procedure is to ensure that problems, non-conformances, and improvements are dealt with in an efficient and effective manner, minimising the chances of any recurrence.

This procedure aims to ensure that processes, services and controls which do not conform to specified requirements are not used, or relied upon, until they are corrected.

Complaints are subject to the same process described in this document.

1. **Responsibilities**

Every individual involved directly or indirectly with Retirement Capital is responsible for initiating and complying with this procedure as and whenever it applies and involves them.

The Information Security Manager is responsible for the overall control and operation of this procedure and for coordinating and processing all Non-Conformance Reports.

Department Managers are responsible for progressing Non-Conformance Reports that are capable of resolution within their area, and forwarding them, and others, to the Director (CISO).

1. **Procedure** [ISO27001 Clause 10]
   1. When a problem or potential improvement is identified, all Employees/Staff have a duty to inform their Manager of the issue, either verbally or by using a Non-Conformance Report ([MSS REC 10.1.1a](MSS_REC_10.1.1A.docx)).
   2. All Employees/Staff or third parties who become aware of an issue which does not meet Retirement Capital’s defined approach and standards, or which has the potential for such an adverse effect, must raise a Non-Conformance Report immediately and forward it to the appropriate Manager.
   3. The Manager will obtain a Non-Conformance Report Log ([MSS REC 10.1.1b](MSS_REC_10.1.1B.xlsx)) Number from the Director (CISO), if one has not already been assigned. For actions within their area of responsibility, Manager evaluate whether the issue is valid and its priority.
   4. The Manager determine whether the nonconformity is isolated, if there are similar nonconformities, or if the cause of the nonconformity has resulted or could result in other nonconformities.
   5. The Manager agree a course of action and timescale to correct the issue, dependent upon the effect the issue is likely to have and to what degree, including isolation/suspension of the relevant facilities/service, as deemed necessary]. The agreed actions may rectify and prevent recurrence of the issue, or the consequences can be accepted. Such actions are recorded on the Non-Conformance Report and a copy is sent to the Director (CISO).
   6. Actions to correct nonconformities will be reviewed as described in Section 3.13, below. As such, the Manager/Executive (generic/line) and the Director (CISO) will also need to agree a timeline for review and any necessary metrics for establishing whether the corrective action has been successful. These details are recorded on the Non-Conformance Report and mirrored in the copy held by the Director (CISO).
   7. If related nonconformities as identified in 3.4 above remain untreated by the action determined in 3.5 above, the Manager will raise a new non-conformance report as detailed in 3.2 above and follow this procedure accordingly.
   8. Timescales for completion should have regard to the cost/benefit of the non-conformance and other reasonable business priorities.
   9. On receipt of forms with no log number, the Director (CISO) assigns one, evaluates the report and forwards it to the appropriate Manager who will act as in Section 3.4, above.
   10. The Director (CISO) will regularly monitor the progress of outstanding Non-Conformance Reports. If any action has not been completed by the previously agreed date, she/he will agree and record new actions and/or dates. If not satisfied that achievable progress is being made, they will escalate the matter to higher line management responsible for that area.
   11. Non-Conformity Reports will be closed down by the Director (CISO) once the issue has been addressed and proof of consideration to preventive measures can be demonstrated; this may result in a review by scheduled or additional Internal Audits (see [MSS DOC 9.2](../Section%209%20-%20performance%20evaluation/MSS_DOC_9.2.docx)). This is recorded on the Non-Conformance Report and the corresponding log entry is updated.
   12. A copy of the completed form is sent to the originator (internally raised issues) for their information, (except in the cases of those generated at Internal Audit).
   13. The Director (CISO) will review the effectiveness of any corrective action taken after a time period determined on the basis of the action and the nonconformity it addresses, as described in Section 3.6, above. If the corrective action fails to adequately address the nonconformity, a new Non-Conformance Report should be raised to address it.

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