1. **Scope** [ISO27001 Section 15]

All external party contracts that fall within the scope of control section 15.1.2 of the [Manual](../Manual/001%20Information%20Security%20Manual.docx) are also within the scope of this procedure.

1. **Responsibilities**
2. The owners of third-party relationships are responsible for the monitoring and reviewing of the services, reports and records carried out by the third party.
3. The IT Manager is responsible for ensuring that adequate technical and other resources that might be required are made available to support the relationship owner in the monitoring and management of the relationship.
4. The Director (CISO) is responsible for carrying out regular audits of third-party performance.
5. The Chief Information Security Officer (CISO (DIRECTOR)) is responsible for regular reviews of exception and other internally generated reports relating to third party performance.
6. **Procedure**
7. The external party agreement includes reporting structures, defines acceptable levels of performance and provides monitoring, inspection and audit rights (see [ISMS-C DOC 15.2.2](ISMS-C_DOC_15.2.2.docx) and the individual third party agreement that is drawn up in accordance with ISMS-C DOC 15.2.2).
8. The relationship owner monitors performance against the service and security criteria contained in the agreement by requesting regular reports and by using ad hoc audits, ensures that reports required under the agreement are delivered as required and reviews them, and conducts regular progress meetings as required.
9. The relationship owner ensures that information security incidents experienced by the third party are reviewed jointly and that relevant information security incidents experienced internally are communicated to the third party to that appropriate steps can be taken.
10. The relationship owner identifies any problems of any sort (including operational problems, failures, faults and tracing faults, and disruptions), on either side of the relationship, and ensures that they are resolved, using the agreed escalation procedure where necessary.
11. The Director (CISO) is responsible for reviewing the third party’s internal audit trails and records of security events.
12. All review meetings must have agendas and minutes (a standard template for both is available on the Intranet), with actions necessary to resolve issues arising clearly identified.
13. On a monthly basis, the IT Manager reviews all outstanding actions in respect of deficiencies in third party services to ensure that appropriate corrective or preventative action is being taken, having regard to the fact that ultimate responsibility for the information processed by the third party remains with Retirement Capital.
14. The procedure for managing changes to third party agreements is contained in ISMS-C DOC 15.2.2.

***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: 20/06/2019

**Change History Record**

|  |  |  |  |
| --- | --- | --- | --- |
| Issue | Description of Change | Approval | Date of Issue |
| 1 | Initial issue | Gavin McCloskey | 20/06/2019 |
|  |  |  |  |
|  |  |  |  |