1. **Scope**

All supplier relationships with Retirement Capital involving information assets are within the scope of this policy.

This includes suppliers involved in the storage, transmission and processing of information, even where the information is encrypted or otherwise generally inaccessible to the supplier.

Retirement Capital has (or may have) external party agreements with the following categories of organisations, all of whom are covered by this procedure; risks may be assessed for external parties as individual organisations or as categories, depending on the level of risk involved:

1. Service providers.
2. Managed security services.
3. Customers.
4. Outsourcing suppliers (facilities, operations, IT systems, data collection, call centers, others).
5. Consultants and auditors.
6. Developers and suppliers of IT systems and services.
7. Cleaning, catering and other outsourced support services.
8. Temporary personnel, placement and other (casual) short-term appointments.
9. **Responsibilities**
10. The Information Security Manager is responsible for ensuring that all relationships take information security into account at the first instance.
11. All relationship owners(see control section 8.1.2 of the [Manual](../Manual/001%20Information%20Security%20Manual.docx)) responsible for services in any of the above categories are required to ensure that external parties have entered into a formal external party agreement under the procedure described in [ISMS-C DOC 15.2.2](ISMS-C_DOC_15.2.2.docx).
12. Relationship owners are responsible for ensuring that the security controls, service definitions and delivery levels included in external party agreements are implemented, maintained and operated by the external party.
13. The Information Security Manager is responsible for carrying out risk assessments (see [RM-ISMS DOC 6.1.2](../Section%206%20-%20planning/RM-ISMS_DOC_6.1.2.docx)) where required by this procedure.
14. **Procedure** [ISO27002 Section 15.1.1]
15. Retirement Capital treats information security within supplier relationships as an extension of the ISMS.
16. All supplier relationships are subject to a risk assessment prior to any exchange or delivery of information assets.
17. Retirement Capital takes the following into account when considering and conducting supplier agreements:
    1. The business case for supply chain security
    2. Information risk within the supply chain, and associated threats
    3. The nature of the relationship – acquisition or supply of information assets
    4. Organisational capability of assuring information security, with regard to both Retirement Capital and the supplier
    5. System lifecycle processes for the assurance of information security
    6. ISMS processes and controls in relation to system lifecycle processes
    7. ISMS processes and controls in relation to security of the supply chain
    8. Essential security practices within the supply chain
18. Procedures for managing supplier agreements are documented ([ISMS-C DOC 15.1.2](ISMS-C_DOC_15.1.2.docx)).
19. Procedures for information security in supplier agreements are documented ([ISMS-C DOC 15.2.2](ISMS-C_DOC_15.2.2.docx)).

***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 12th June 2019 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 |
|  |  |  |  |
|  |  |  |  |