1. **Scope**

Retirement Capital maintains the security of its information processing facilities and information assets in relation to external parties. All external parties who need to access any organisational information assets are subject to this procedure. 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/office service providers.
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. 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 this procedure and that transitions (of information, information processing facilities, and any other information assets or personnel) are planned and executed without a reduction in the level of security that existed prior to commencement of the transition.
11. 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.
12. The Information Security Manager is responsible for carrying out risk assessments (see RM-ISMS DOC 6.1.2) where required by this procedure.
13. **Procedure** [ISO27002 Section 15.1.2]
14. Where there is a business need for working with external parties, Retirement Capital ensures that its information security is not reduced; access to organisational assets is not granted until a risk assessment (RM-ISMS DOC 6.1.2) has been completed, appropriate controls identified and implemented.
15. **Risk Identification**
16. Retirement Capital carries out a risk assessment (in line with the requirements of procedure RM-ISMS DOC 6.1.2) to identify risks related to external party access.
17. The risk assessment identifies (in addition to the requirements of RM-ISMS DOC 6.1.2) and documents, for each external party:
18. The information processing facilities and information assets the external party will access.
19. The type of access the third party will have – physical access and/or logical access (identifying the assets that will be accessed), whether the access is taking place on site or off site and the exact location from which access will be made.
20. The value and classification (see control section 8.2 of the Manual) of the information that will be accessed.
21. The information assets that the external party are not intended to access and which may require additional controls to secure.
22. The external party’s personnel (see control section 7.1 of the Manual), including their contractors and partners, who will or might be involved.
23. How external party personnel are to be authenticated (see control section 9 of the Manual).
24. How the external party will process, communicate and store information.
25. The impact to the external party of access not being available when required, or of inaccurate or misleading information being entered, received or shared.
26. How Retirement Capital’s information security incident management procedure (see control section 16 of the Manual) will be extended to incorporate information security incidents involving the external party.
27. Any legal, regulatory or other contractual issues that should be taken into account with respect to the external party.
28. How the interests of other stakeholders might be affected by any decisions.
29. Controls are selected in line with the requirements of RM-ISMS DOC 6.1.1
30. Retirement Capital implements those controls that are within its own power, and in line with the requirements of Section 3.2 of the Manual (the implementation phase)
31. Retirement Capital agrees with the external party those controls that the external party is required to implement and documents them in an agreement (drawn up by Retirement Capital’s legal advisers) that the third-party signs. The obligations on the external party include ensuring that all its personnel are aware of their obligations.
32. The agreements between Retirement Capital and external parties (whether suppliers or customers[[1]](#footnote-1)) are created by Retirement Capital’s legal advisers, (who are required to specifically include or provide documented reasons for excluding any of the items on the checklist below, and the requirement for which may have been identified through the risk assessment, from any such contract):
33. The Information Security Policy (Section 5.1.1 of the Manual).
34. The controls identified as required through the risk assessment process (see 4 above), which may include procedures and technical controls.
35. A clear definition and/or description of the product or service to be provided, and a description of information (including its classification) to be made available.
36. Requirements for user and administrator education, training and awareness (see Section 7.2.2 of the Manual).
37. Provisions for personnel transfer.
38. Description of responsibilities regarding software and hardware installation, maintenance and de-commissioning.
39. Clearly defined reporting process, reporting structure, reporting formats, escalation procedures and the requirement for the external party to adequately resource the compliance, monitoring and reporting activities.
40. A specified change management process (see control section 12.1.2 in the Manual).
41. Physical controls, including secure perimeters (see control section 11 of the Manual).
42. Controls against malware (see control section 12.2 of the Manual).
43. Access control policy (see control section 9 of the Manual).
44. Information security incident management (see control section 16 of the Manual) and agreement violation management procedures.
45. The target level for service and security, unacceptable service and security levels, definition of verifiable performance and security criteria, monitoring and reporting.
46. The right to monitor and audit performance (including of the third party’s processes for change management, vulnerability identification and information security incident management), to revoke activities, and to use external auditors.
47. Service continuity requirements.
48. Liabilities on both sides, legal responsibilities and how legal responsibilities (including data protection and privacy) are to be met.
49. The protection of IPR and copyright.
50. Controls over any allowed sub-contractors.
51. Conditions for termination / re-negotiation of agreements, including contingency plans.
52. **Information transfer agreements** [ISO27002 Clause 13.2.2]

Additional controls must (subject to an individual risk assessment in relation to each proposed agreement) be considered where the contract is for the transfer of information or software:

1. Specific management responsibilities and procedures on each side for notifying transmission, dispatch and receipt and any specific controls associated with each action.
2. Procedures to ensure non-repudiation and to ensure traceability.
3. The required standards for packaging (see [ISMS-C DOC 11.2.5](../Control%20A11%20-%20physical%20and%20environmental%20security/ISMS-C_DOC_11.2.5.docx)) and means of transmission.
4. The agreed labeling system (see [ISMS-C DOC 8.2](../Control%20A8%20-%20asset%20management/ISMS-C_DOC_8.2.docx)).
5. Courier selection and identification methods (see [ISMS-C DOC 11.2.5](../Control%20A11%20-%20physical%20and%20environmental%20security/ISMS-C_DOC_11.2.5.docx)).
6. Escrow agreements.
7. How information security incidents (loss of or damage to an information asset in transit) will be managed.
8. Data protection, copyright, software licensing (see control section 15.1 of the Manual).
9. Any technical standards that are required for recording or reading software or information.
10. Any other special controls, such as cryptography (see control section 10.1 of the Manual).
11. **Managing changes to third party services** [ISO27002 Clause 15.2.2]

Retirement Capital may need to agree changes to external party contracts and agreements to take account of changes that it makes to, or as a result of:

1. the services it currently offers to its clients;
2. new applications and systems it has developed or acquired;
3. modifications, changes or updates to its own policies and procedures;
4. new or amended controls arising from new risk assessments or information security incidents.
   1. The external party may need to request changes to the contract in order to implement:
5. Changes or improvements to their networks or other infrastructure.
6. New or improved technologies, new products or new releases of current products.
7. New development tools, methodologies and environments.
8. New physical locations or physical services.
9. New vendors or other suppliers of hardware, software or services.
   1. Any changes that may be required are subject to a new risk assessment (taking into account the criticality of the business systems involved) and review of the selected controls (see Clauses 4.1 and 5 above).
   2. New controls, or changes to existing controls are identified, authorised, agreed with the third party, and made the subject of an agreed variation [insert here a reference to exactly how contract variations are handled] to the existing contract.
   3. The relationship owner is responsible for ensuring that the revised controls are implemented and incorporated into the existing review and monitoring arrangements.

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

1. [↑](#footnote-ref-1)