1. **Scope**

Retirement Capital’s network

1. **Responsibilities**

The Network Manager is responsible for the network architecture and infrastructure, and for the security of systems, applications and information using the network.

The Network Manager is responsible for managing the in-house/outsourced network services in line with Clause 4 of this procedure.

The Director (CISO) is responsible for information processing facilities that communicate by means of the network.

The Director (CISO) is responsible for risk assessment.

The owners (see control section 8.1.2 of the [Manual](../Manual/001%20Information%20Security%20Manual.docx)) of network service relationships are responsible for managing those relationships.

1. **Network Controls** [ISO27702 Clause 13.1.1]
2. Risk assessments are carried out for each network within the scope of this procedure, to ensure that all information security risks have been identified and appropriate controls selected. The risk assessment is reviewed in line with the review requirements of the ISMS.
3. The network architecture reflects the risk assessment, is designed to maximise security and business efficiency, takes into account the requirements of control section 13.1.3 of the Manual and is kept under review.
4. Remote equipment is managed in line with control section 6.2 of the Manual (for mobile and teleworkers).
5. Network equipment (router, firewalls, Network Attached Storage) installed in the London Office is managed in line with ISMS DOC 13.1.2.
6. Network access control is managed in line with the requirements of control section 11.4 of the Manual.
7. Confidential and restricted information is encrypted using vsCrypt and in line with control section 10.1 of the Manual.
8. Network availability is maintained by Director (CISO).
9. Retirement Capital has deployed logging and monitoring controls, the configuration of which and reporting procedures are set out in Work Instruction ISMS-C-REC-12.4.1
10. **Network Services** [ISO27001 Clause 13.1.2]
11. Retirement Capital uses the following network services: office network and production network.
12. Risk assessments are carried out for each network service and appropriate controls including authentication, encryption and network connection controls are selected. The risk assessment is reviewed in line with the review requirements of the ISMS.
13. The identified controls are included in the external party agreement.
14. External party agreements are managed in line with the requirements of control sections 15.1 and 15.2 of the Manual.
15. Work Instruction ISMS-C-DOC-11.2.4 sets out the technical parameters and configuration requirements for connection with network services.
16. Access to network services and applications is restricted in line with ISMS-C-DOC 13.1.3.

***Document Owner and Approval***

The Network 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 Director (CISO) on 214th 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 |
|  |  |  |  |
|  |  |  |  |