1. **Scope** [ISO27002 Clause 6.2.2]

All teleworkers who use organisational or their own resources to connect to organisational facilities are subject to the requirements of this procedure.

1. **Responsibilities**

Once all the prerequisites for the setting up of a teleworking site have been completed, authorisation of teleworker access follows the same procedure as laid down for office-based users.

The IT Manager is responsible for the configuration of required computing equipment.

The Network Manager is responsible for network configuration and for providing remote network connectivity and user support.

The Premises Manager is responsible for the site survey and implementation of necessary physical improvements and controls.

The Procurement Manager is responsible for any new equipment purchased.

The Information Security Manager is responsible for the risk assessment.

Teleworkers have specific responsibilities, as set out in their User Agreements.

The Finance Director (CFO) is responsible for ensuring that insurance requirements are met.

1. **Procedure**
   1. The proposed site must be surveyed and the risks assessed before a decision can be made as to whether or not to authorise creation of a teleworker facility and, if it is to be authorised, to decide what controls will be necessary.
   2. The findings of the site survey and the details of the requirements gathered in [ISMS-C REC 6.2.2b](ISMS-C_REC_6.2.2B.docx) are used as input into a risk assessment. The risk assessment determines the controls that are necessary for each teleworking location. The Information Security Manager documents the required controls in the output from the risk assessment.
   3. The teleworking site is brought into conformity with the required specification, in terms of any necessary physical security improvements, and the provision of home network and connectivity infrastructure.
   4. Any necessary changes to the network are made to ensure that Retirement Capital’s access control policy ([ISMS-C DOC 9.1.1](../Control%20A9%20-%20access%20control/ISMS-C_DOC_9.1.1.docx)) is not breached by the teleworker. Once these steps have all been accomplished, the teleworker facility can be authorised.
   5. The teleworker undergoes necessary training and then signs a teleworker User Agreement ([ISMS-C DOC 6.2.2a](ISMS-C_DOC_6.2.2a.docx)) which sets out all the obligations and requirements in respect of the teleworking facility.

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