1. **Scope**

This procedure applies to all Retirement Capital’s information assets and, in particular, to notebook computers, PDAs, mobile phones, projectors and other portable information processing equipment available for use outside Retirement Capital’s secure perimeter, as well as removable and portable storage media. Information assets may not be removed without prior authorisation.

1. **Responsibilities**
   1. The Director (CISO) is responsible for authorising removal of portable devices and media and for carrying out spot checks to ensure compliance with this procedure.
   2. The Director (CISO) is responsible for authorising removal of fixed devices, re-configuring portable devices and maintaining loan records.
   3. The Director (CISO) is responsible for the secure disposal of information processing devices (see control section 11.2.7 of the [Manual](../Manual/001%20Information%20Security%20Manual.docx)).
   4. The Company Administrator is responsible for provision of approved courier services.
   5. Users have specific responsibilities as detailed below or in their User Agreements.
2. **Procedure** [ISO27002 Clauses 8.2.3 and 8.3.2 and 11.2.5]
   1. Removal of property:

* 1. Personnel files may only be taken offsite with the email permission of the Managing Director.
  2. Client information may only be taken offsite with the email permission of the Head of Sales.
  3. Portable projectors may only be taken offsite with the email permission of the Director (CISO).
  4. Notebooks, mobile phones and PDAs that have not been permanently allocated to an individual may only be taken offsite if the procedure set out in Section 3.4 below is followed.
  5. Any other information, hardware, software or portable and removable media, may only be taken offsite with the permission of its owner (see control section 8.1.2 in the Manual), the authorisation of the Premises Manager and if it is properly protected (see Clause 5 below).
  6. The Director (CISO) provides authorisation in the form of an e-mail that explicitly permits the removal of an identified asset for a specific purpose and a specific time period. The Premises Manager retains a log ([ISMS-C REC 8.3.1](../Control%20A8%20-%20asset%20management/ISMS-C_REC_8.3.1.docx)) of all requests made and whether they were granted or not.
  7. Information assets taken offsite, with appropriate permission, must be accompanied by a member of Retirement Capital 's employees/staff, or a contracted supplier who is subject to an appropriate external party agreement, until securely relocated. Secure locations include the homes of employees/staff] (e.g. notebooks and PDAs), law firms engaged by Retirement Capital (e.g. personnel files), approved storage facilities (e.g. archived customer files), approved bulk document scanning suppliers and any of Retirement Capital’s sites.
  8. Organisational equipment that is used for fixed-location remote working is subject to the controls in Section 6.2.2.

## **Courier services** [ISO27002 Clause 13.2.2]

1. Retirement Capital has approved agreements (in line with control section 15.1.2 of the Manual) with courier services, who were selected on the basis of suitability and value for money. Their contact details are on the company intranet and the procedure for ordering service is set out in therein.
2. Couriers are authenticated by employee badge.

## **Protection of media in transit** [ISO27002 Clause 8.3.3]

## The requirements in respect of the physical protection of media in transit (which take into account manufacturer’s specifications, environmental factors, etc.) are as follows:

* + 1. Removable electronic media: CD-ROMs must be in jewel cases
    2. Magnetic tapes: are not to be used to transfer data.
    3. USB flash sticks: must be encrypted and sent in jiffy bags or equivalent
    4. Other devices:
    5. For all restricted media, tamper proof packaging is required.
    6. For all confidential media (including backup tapes), locking boxes must be used and hand delivery to the intended recipient (see [ISMS-C DOC 8.2](../Control%20A8%20-%20asset%20management/ISMS-C_DOC_8.2.docx)) is also required.

## Notebook loan procedure (for the purpose of this procedure, ‘notebook’ includes any peripheral equipment such as printers and fax machines, as well as PDAs and mobile phones):

### Any employee/staff, or sub-contractor that needs to borrow a notebook computer on a short-term basis must first obtain business approval, in the form of an e-mail from the Premises Manager expressly approving the loan, detailing the business purpose and the period for which the loan is authorised.

### The e-mail is forwarded to the Director (CISO) with a request for a loan with effect from a specified date and time. The Director (CISO) will confirm the availability or otherwise of the required equipment within one business day.

### All notebooks and related devices have a standard configuration, defined by the Director (CISO), and which is documented in work instruction [ISMS-C DOC 11.2.4](ISMS-C_DOC_11.2.4.docx). They are only released in this configuration.

### Notebooks and related devices are signed for by the borrower and the Director (CISO) signs to accept them back.

### The Director (CISO) is responsible for monitoring returns of devices against the agreed return date and reporting non-returns to the Director (CISO) within 24 hours of the due date and time for return.

### The borrower signs the ‘mobile on the road’ User Agreement annex before the Director (CISO) releases the notebook.

### On return the notebook will be checked by the IT Department using the following guidelines:

### The Notebook will be scanned for malware, and folders and files will be checked for illegal records (see control section 8.1.3 of the Manual).

### The configuration of the notebook will be checked against the standard configuration and any changes will be reversed.

### The IT Department will ask the user whether any files saved on the C:Drive should be deleted or transferred to their desktop PC and will then ensure that all the user files are deleted from the laptop.

* + 1. The IT Department will clear the Internet History and all cookies in the browser.
  1. Any breaches of Retirement Capital’s ISMS will be reported in line with Retirement Capital’s disciplinary policy, as set out in the employee handbook.

***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 Director (CISO) on 14th November 2020 and is issued on a version-controlled basis under his/her signature.

Signature: Date: 14th November 2020

**Change History Record**

|  |  |  |  |
| --- | --- | --- | --- |
| Issue | Description of Change | Approval | Date of Issue |
| 1 | Initial issue | Gavin McCloskey | 14/11/2020 |
|  |  |  |  |
|  |  |  |  |