1. **Scope**

All removable media and documentation for systems owned or operated Retirement Capital are covered by this procedure.

1. **Responsibilities**

Users are not permitted to use any removable media other than those provided by Retirement Capital.

The Company Administrator is responsible for ensuring that Retirement Capital has adequate supplies of specified removable media.

The IT Manager is responsible for device configuration in line with the requirements of this procedure.

The Premises Manager is responsible for the security of removable media on the site, for authorisation of their removal and for spot checks to ensure this procedure is being followed.

The IT Manager is responsible for the central storage of removable media and system documentation as required by this procedure.

1. **Procedure** [ISO27002 Section 8.3]
2. Removable media will only be issued to employees/staff who have a clear business need for them. Issue of these media to sub-contractors and temporary workers must be specifically authorised by the Premises Manager.
3. Removable media drive ports are not enabled, unless authorised by IT Manager/CISO (DIRECTOR).
4. Removable media are labeled as required by [ISMS-C DOC 8.2](ISMS-C_DOC_8.2.docx).
5. Removable media may only carry information that is required for a specific purpose – in other words, once a purpose has been fulfilled, the information must be erased from the media.
6. The requirement for the authorisation of the removal of media from site(s), and the requirement for their physical protection, is set out in [ISMS-C DOC 11.2.5](../Control%20A11%20-%20physical%20and%20environmental%20security/ISMS-C_DOC_11.2.5.docx).
7. Long term storage of information must be on media, the manufacturer’s specification of which indicates that it will not degrade during the required storage period.
8. Media (including spooled media) are stored in a secure cabinet unless archived to a commercial storage facility and in accordance with the manufacturer’s instructions.
9. Spot checks will be carried out to ensure that this procedure is complied with and transgressions will be considered under Retirement Capital’s disciplinary policy.
10. Media are disposed of securely and as required by [ISMS-C DOC 11.2.7](../Control%20A11%20-%20physical%20and%20environmental%20security/ISMS-C_DOC_11.2.7.docx).
11. **Access control to program source code** [ISO27002 Clause 9.4.5]
12. The Change Manager securely stores removable media and system documentation as specified in ISMS DOC 12.3] and maintains a secure program list and access control list in which each application owner specifies who is authorised to access the related system documentation and program source libraries.
13. Program source libraries are not held in operational systems.
14. [ISMS-C-DOC 12.1.4](../Control%20A12%20-%20operations%20security/ISMS-C_DOC_12.1.4.docx) sets out procedures for the management and maintenance of program source code and program source libraries, including how updates and issues of program sources, and copying of program source libraries, are authorised.
15. An audit log is maintained of all access to program source libraries by the IT Manager using record form [ISMS-C-REC 8.1.1b](ISMS-C_REC_8.1.1b.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 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 |
|  |  |  |  |
|  |  |  |  |