1. **Scope**

All operational software (operating systems, applications, program libraries and cloud systems) that are, or are intended to be, installed on organisational information processing systems, and used for the operation of the business, is within the scope of this procedure.

1. **Responsibilities**

The Director (CISO) is responsible for developing and maintaining the development environments.

The Click here to enter text. is responsible for maintaining the test environment.

The Software and Engineering Manager is responsible for maintaining the test environment.

The Director (CISO) is responsible for the operational (live) environment.

The Director (CISO) is responsible for installing operational software updates or new implementations.

The Software and Engineering Manager is responsible for managing the transfer of software from development to test to operational environments.

The Director (CISO) is responsible for the central storage of system documentation as required by [ISMS-C DOC 8.3](../Control%20A8%20-%20asset%20management/ISMS-C_DOC_8.3.docx).

1. **Procedure** ISO27002 Clause 12.5.1
2. Retirement Capital’s operational software is listed in the asset inventory [(ISMS-C REC 8.1.1a](../Control%20A8%20-%20asset%20management/ISMS-C_REC_8.1.1a.docx)) (see control section 8.1.1 of the [Manual](../Manual/001%20Information%20Security%20Manual.docx)) and each item of operational software has an identified owner (see control section 8.1.2 of the Manual), who is the trained administrator of that item of software. Only the owner may perform software updates, and then only with the prior authorisation of the Director (CISO) after the completion of satisfactory testing. Authorisation should be provided by email.
3. Systems that are running operational software may not also run development software or code or compilers (see also control section 12.1.4 of the Manual).
4. Pre-implementation testing of operational software is carried out in the test environment accordance with [ISMS-C DOC 12.1.3](ISMS-C_DOC_12.1.3.docx) and all corresponding program source libraries are updated.
5. The Director (CISO) maintains a configuration control schedule (ISMS-C REC-14.2.2a) Identify how it links to the asset inventory ISMS-C REC 8.1.1a and to the Change Manager’s method of storing system documentation in ISMS-C DOC 8.3 for all operational software and an audit log for all to updates to operational program libraries (ISMS-C DOC 14.2.2b).
6. Software change management is carried out in line with [ISMS-C DOC 12.1.2](ISMS-C_DOC_12.1.2.docx).
7. Previous versions of operational software are retained for a minimum of one year, as an archive, as a contingency.
8. Physical or logical access is only given to suppliers who have a business need as an Retirement Capital partner and in line with the requirements of [ISMS-C DOC 13.1.3a](../Control%20A13%20-%20communications%20security/ISMS-C_DOC_13.1.3a.docx).

***Document Owner and Approval***

The Software and Engineering 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 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 |
|  |  |  |  |
|  |  |  |  |