1. **Scope**
2. All significant, non-routine changes to organisational information processing facilities (hardware or software) are subject to change control.
3. The documentation change control requirements for ISMS policies and procedures are set out in [ISMS DOC 7.5.3](../Section%207%20-%20support/MSS_DOC_7.5.3.docx).
4. **Responsibilities**

Department Managers are responsible for submitting system change requests to the Director (CISO), using the Change Request Form, [ISMS-C REC 12.1.2](ISMS-C_REC_12.1.2.docx).

The Director (CISO) is responsible for ensuring that all change requests are managed in line with this procedure.

The Director (CISO) is responsible for authorising the transfer from the test environment to the operational (live) environment.

The Director (CISO) is responsible for maintaining the test environment.

The Director (CISO) is responsible for testing operational software updates and new implementations.

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

The Operations Director is responsible for ensuring that changes which might affect business continuity plans are accounted for in those plans.

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

The owner is responsible for updating system documentation and procedures.

1. **General Procedure** ISO27002 Clause 12.1.2, 14.2.2, Part 12.5.1 and a link to 15.2.2
2. The following changes are considered routine or insignificant and are therefore not subject to this procedure:

* Anti-virus updates
* Vulnerability patching, hot fixes
* Software upgrades

1. The originator of a change request completes the change request form (ISMS-C REC 12.1.2) and obtains both the Department Manager and Director (CISO) technical approvals for the change, taking into account the costs of the exercise, the potential benefits, etc.
2. Once the change request has these two approvals, the change request is passed to the Company Administrator where it is logged ([ISMS-C REC 12.1.2a](ISMS-C_REC_12.1.2a.docx)). Copies of all change requests are retained to provide an audit trail.
3. The Director (CISO) is then responsible for carrying out a risk assessment (see control section 4.4 of the [Manual](../Manual/001%20Information%20Security%20Manual.docx)) to identify potential risks, their impacts and then (with the Director (CISO)) to identify and cost the required controls in line with Retirement Capital’s risk management framework.
4. The Director (CISO) is responsible then for authorising the change to go ahead. No change implementation work is done until the change is agreed. Where required by a risk assessment, fallback procedures or a roll-back strategy must be prepared and the Operations Director briefed on the planned actions.
5. A testing plan, complete with clear acceptance criteria including business, technical and load criteria must be documented prior to commencing the change testing in line with [ISMS-C DOC 12.1.3](ISMS-C_DOC_12.1.3.docx).
6. Testing takes place in the test environment, which is an exact simulation of the operational environment. The Head of Systems Testing is responsible for maintaining the test environment and the configuration documentation.
7. The individual responsible for testing the change must be identified and fully briefed.
8. If necessary, the testing plan can include a dry run of the change in the development environment.
9. Business unit representatives (approved by the originating Manager) must accept the changes prior to completion of testing.
10. Once the change is proved to be effective (working in line with the test criteria) the Director (CISO) authorises its transfer to the operational environment, ensuring that business processes are not disturbed and that business continuity plans are updated.
11. Software updates are version controlled as stated in [ISMS-C REC 8.1.1a](../Control%20A8%20-%20asset%20management/ISMS-C_REC_8.1.1a.docx), system documentation is updated and old documentation is archived.
12. Operating procedures and documentation are updated for the changes to the software.

***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: 14/11/2020

**Change History Record**

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