1. **Scope**

All Retirement Capital’s information systems are within the scope of this procedure.

1. **Responsibilities**

The Director (CISO) is responsible for monitoring vulnerabilities and vendors’ releases of patches and fixes and installing operational software updates, patches and fixes on the operational systems.

The Director (CISO) is responsible for maintaining the test environment, known as TEST and UAT.

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

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

Owners are responsible for tracking likely vulnerabilities in and patches available for their assets.

The Director (CISO) is responsible for vulnerability risk assessment.

1. **Procedure** [ISO27002 Clause 12.6.1]
2. Identified vulnerabilities for organisational assets are prioritised by Customer Affecting then Internal Operations Affecting and Retirement Capital has established the following timeline requirements for reacting to notifications of relevant vulnerabilities:

* Customer affecting: notification within 8 hours
* Internal operations affecting within one working day

1. High value or high-risk systems are treated ahead of other systems.
2. All vulnerabilities that fall into Customer Affecting will first be assessed for seriousness and required controls (patching; turning off/removing services affected by the vulnerability; adapting or adding access controls; increased monitoring; awareness raising).
3. The required controls will be actioned through the change management procedure ([ISMS-C DOC 12.1.2](ISMS-C_DOC_12.1.2.docx)) if they require major changes in software or configuration, or through the incident response procedure ([ISMS-C DOC 16.1.5](../Control%20A16%20-%20information%20security%20incident%20management/ISMS-C_DOC_16.1.5.docx)) if they are only patches or updates.
4. Available patches must be risk assessed, taking into account the balance between risks in installing and not installing, before the final decision as to necessary controls can be made.
5. Patches must be tested, as laid down in [ISMS-C DOC 12.1.3](ISMS-C_DOC_12.1.3.docx).
6. Vulnerability control decisions are tracked (and can be audited) through either the change management procedure (ISMS-C DOC 12.1.2) or the incident response procedure (ISMS-C DOC 16.1.5).
7. The Director (CISO) receives monthly reports on vulnerability management, including information about the number of identified vulnerabilities in each organisational asset, what additional controls are in place, what outstanding issues there are, and how the picture has changed since the previous meeting

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