1. **Policy statement**
2. Retirement Capital acts to protect the integrity of its software and its other information assets against the introduction of malicious code (malware). Specifically:
3. Retirement Capital formally prohibits the use, on any information processing system or device it owns or operates, of any software whose procurement was not carried out through Retirement Capital’s procurement procedure. (See also control section 18.1.2 of the [Manual](../Manual/001%20Information%20Security%20Manual.docx).)
4. Software that has been obtained in line with Retirement Capital’s procurement procedure, and any other files or folders, may not be transferred or downloaded onto Retirement Capital’s network via or from external networks, or on any medium (including CD-ROMs, USB sticks), including during maintenance and emergency procedures, unless specific controls have been implemented as detailed in [ISMS-C DOC 12.2.1a](ISMS-C_DOC_12.2.1a.docx).
5. Retirement Capital formally prohibits the use of defined mobile code.
6. Monitoring, detecting and deleting unauthorised software is a requirement of the information system, and disciplinary action is to be taken against anyone in breach of the anti-malware policy.
7. Retirement Capital acts to identify and patch software and system vulnerabilities in order to reduce the risk of malware attacks (see control section 12.6 of the Manual).
8. The installation and maintenance of anti-malware software on all organisational information systems and devices is mandatory.
9. All users are required to accept, in terms of their User Agreements, the Internet Acceptable Use Policy ([ISMS-C DOC 8.1.3](../Control%20A8%20-%20asset%20management/ISMS-C_DOC_8.1.3.docx)) and the e-mail rules ([ISMS-C DOC 8.1.3a](../Control%20A8%20-%20asset%20management/ISMS-C_DOC_8.1.3a.docx)) and to receive appropriate training in detecting and responding to malware attacks, and to accept specific anti-malware prevention controls in their User Agreements.
10. Business continuity plans (control section 17 of the Manual) are required to make specific provision for recovering from malware attacks.
11. The Information Security Incident Management procedure (see control section 16 in the Manual) is required to make specific provision for responding to malware attacks.
12. Management is required to take adequate steps to ensure that it is aware of and can respond to changes in the malware threat environment

***Document Owner and Approval***

The Director (CISO) is the owner of this document and is responsible for ensuring that this policy document is reviewed in line with the review requirements stated above.

A current version of this document is available to all members of staff on the corporate intranet.

This policy was approved by the Board of Directors on 14th November 2020 and is issued on a version-controlled basis under the signature of the Managing Director.

Signature:

Date:14/11/2020

**Change History Record**

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