1. **Scope** [ISO27002 Clause 12.2.1]

Retirement Capital’s policy against malicious code ([ISMS-C DOC 12.2.1](ISMS-C_DOC_12.2.1.docx)) covers all Retirement Capital’s information assets, including hardware, software, mobile devices and peripherals including memory devices, PDAs, mobile phones and applies to all employees/staff, contractors, temporary workers and third parties who use, work with or connect to organisational information processing facilities.

1. **Responsibilities**
2. All users have specific responsibilities, defined in their User Agreements, in 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)).
3. The Director (CISO) is responsible for monitoring software and systems for breaches of the anti-malware policy or this procedure.
4. The Director (CISO) is responsible for the installation and maintenance of Retirement Capital’s selected anti-malware (see work instruction [ISMS-C DOC 12.2.1b](ISMS-C_DOC_12.2.1b.docx)) software, and for any configuration of the firewall(s) and gateway(s) (when in use), as well as for ensuring that the IT Department have adequate technical training and skills to carry out assigned tasks under this procedure.
5. The Company Administrator is responsible for ensuring that users receive adequate training on anti-malware responses, including on opening uninvited folders and attachments, and on identifying possible hoaxes.
6. The CISO (DIRECTOR) is responsible for maintenance of the business continuity framework.
7. The Director (CISO) is responsible for incident management, for gathering information about any cases of non-compliance with this policy to pass to the Company Administrator for initiation of disciplinary actions, and for Retirement Capital’s awareness of the changing malware threat environment (see control section 6.1.4.2 of the [Manual](../Manual/001%20Information%20Security%20Manual.docx)), which he/she does by subscribing to appropriate alert services and ensuring that such information is current, accurate and genuine.
8. **Procedure in respect of malicious code**
9. The criteria for selection of the anti-malware software are that it must:

* Work across all relevant platforms
* Works in cloud, hosted and on-premise environments
* High ranking performance assessments in UK and USA
* Pay by use scalable commercials

1. The anti-malware software is installed on all organisational information systems and devices, including gateways and firewalls, and is configured in line with WI ISMS-C DOC 12.2.1b, with automatic updating enabled, unless determined inappropriate for operational reasons. The anti-malware software installed on the gateway(s) conducts automated scans of all attachments and deletes or quarantines suspect files.
2. The standard build for servers, workstations and notebook computers must disable disk and CD-ROM drives, and USB ports and the configuration requirement is in WI ISMS DOC 12.2.1a.
3. Software from external parties must be inspected by the IT Department and authorised as free of viruses and in conformance with the requirements of control section 14.2.9 of the Manual before it can be loaded onto the network. A log Schedule ISMS-C DOC 8.1.1a is retained of all such software authorised for use, showing the originator of the request, the software details, and the date and time it was inspected, together with details of who carried out the inspection. The standard method for inspecting such software is detailed in WI ISMS DOC 12.2.1b which describes your manual and automated process for achieving this.
4. Retirement Capital’s Google G-Suite anti-spam filters will detect and isolate the majority of spam content, however users are educated and updated (via the intranet) of any specifically damaging or concerning Spam.
5. Retirement Capital uses XXX for monitoring software usage on its systems; unauthorised files or software are automatically investigated, and the outcomes of investigation considered for possible disciplinary action, as well as deletion. The method of carrying out these checks is specified in WI ISMS DOC 12.2.1c
6. The anti-malware supplier provides virus quarantine / removal software in case of successful attack, which runs automatically.
7. Organisation Name allows the use of specific mobile code, that operates as extensions through Google Chrome. The list of browser extensions is maintained in ISMS-C-REC-12.2.1f.
8. **User training** [ISO27002 Clause 7.2.2]
   1. User training on malware responses includes:
9. The principles and requirements of the anti-malware policy.
10. The requirements of the Internet Acceptable Use policy.
11. Identifying and responding to ‘hoax’ virus warnings, reporting them to the Director (CISO), and not passing them on.
12. Not opening attachments to e-mails that are unexpected or where the sender is unknown.
13. How to respond if a virus does successfully install itself on their workstation or laptop.
14. What protective steps are necessary in respect of portable memory media.
15. How to respond to screen and system alerts regarding viruses, spam, and mobile code.
16. Not to accept any file or folder execution requests while on the Internet.

***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 12th May 2019 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 |
|  |  |  |  |
|  |  |  |  |