

Controls Against Malicious Code Procedure

Reference: CES DOC 4.2

DocumentKits Issue No: 1.0

Organisation Issue No:

DocumentKits Issue Date: 20/05/2020

Organisation Issue Date:

1. Scope

Organisation Name's [Policy Against Malicious Code \(Malware\) \(CES DOC 4.1\)](#) covers all Organisation Name'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 within the [Scope Statement \(CES DOC 1\)](#).

2. Responsibilities

2.1 Users have specific responsibilities, defined in their user agreements, in the Internet Acceptable Use Policy

"(insert document reference/link)"

and the email rules

"(insert document reference/link)"

2.2 The Head of IT (CIO) is responsible for monitoring software and systems for breaches of the anti-malware policy or this procedure.

2.3 The Head of IT (CIO) is responsible for installing and maintaining Organisation Name's selected anti-malware (see the [Antivirus Software Work Instruction \(CES DOC 4.3\)](#)) software, and for the configuration of the firewall(s) and gateway(s) (see the [Firewall Configuration Procedure \(CES DOC 1.1\)](#)), as well as for ensuring that the IT Department has adequate technical training and skills to carry out assigned tasks under this procedure.

<<2.4-2.5 removed for sample purposes>>

3. Procedure in respect of malicious code

3.1 The criteria for selection of the anti-malware software, application whitelisting and/or application sandboxing are that they must:

"set out your criteria, taking into account this checklist: spyware, Trojans, worms, viruses, spam, email, Instant Messaging (IM), notebook computers, PDAs, mobile phones, portable memory media (USB sticks, other specified removable media), plus robustness, reliability, at least daily updates, effectiveness, other specific criteria of your own"

Organisation Name's approved software is:

"insert name of software vendor and product selected."

3.2 The anti-malware software is installed on all organisational information systems and devices, including gateways and firewalls, and is configured in line with the [Antivirus Software Work Instruction \(CES DOC 4.3\)](#), with automatic updating enabled. The anti-malware software installed on the gateway(s) conducts automated scans of all attachments and deletes or quarantines suspect files.

3.3 The anti-malware software is configured to scan files automatically upon access when downloaded and opened, as well as when accessed from a network folder.

3.4 The anti-malware software scans web pages automatically when accessed via a web browser, and prevents connections to malicious or potentially malicious websites on the Internet
"by blacklisting"

unless there is a clear and documented business reason.

"A log is kept in [add reference]"

to allow the connection.

3.5 The firewall(s) are configured to halt download of software from the Internet (see the [Firewall Configuration Procedure \(CES DOC 1.1\)](#)).

3.6 The standard build for servers, workstations and notebook computers ensures that portable and removable media are scanned for malware upon access. This is achieved by

"name of software"

<<3.7-3.12 removed for sample purposes>>

4. User training

4.1 User training on malware responses includes:

4.1.1 The principles and requirements of the anti-malware policy ([Policy Against Malicious Code \(Malware\) \(CES DOC 4.1\)](#)).

4.1.2 The requirements of the Internet Acceptable Use Policy.

4.1.3 Identifying and responding to 'hoax' virus warnings, reporting them to the Information Security Manager, and not passing them on.

4.1.4 Not opening attachments to emails that are unexpected or where the sender is unknown.

<<4.1.5-4.1.9 removed for sample purposes>>

Document owner and approval

The Information Security Manager is the owner of this document and is responsible for ensuring that it is reviewed in line with the requirements of the management system.

The current version of this document is available to

"Specify which members of staff this document is intended for"

and is published

"Describe the location(s) - electronic and physical - where this document is available"

Its approval status can be viewed in the [Master List of Document Approval](#).