

February 2025

INTERNAL

Anti-Malware Policy

FUNDS  AXIS

Policy title:	Anti-Malware Policy
----------------------	---------------------

Issue	1.1
Approved by:	Trevor Dempster
Approval Date:	February 2025
Next Review Date:	February 2026

Scope:	The policy applies to Funds-Axis Limited and all contractors and other people working on behalf of the company.
Associated documentation:	<ul style="list-style-type: none"> \ Mobile Device Policy \ Acceptable Use Policy \ Electronic Messaging Policy \ Software Policy
Responsibility for Implementation & Training:	<p>Day to day responsibility for implementation: ISO</p> <p>Day to day responsibility for training: ISO</p>

Distribution methods:	<p>Methods used to communicate this policy:</p> <ul style="list-style-type: none"> \ Training
------------------------------	--

1. Introduction

The threat posed by malware has never been more serious than it is today. Funds-Axis systems and users are under a constant bombardment of attempts to circumvent security to make gain or to disrupt the normal operation of the organisation.

This threat can come from sources including:

- \ Organised gangs attempting to steal money or commit blackmail
- \ Competitor organisations trying to obtain confidential information
- \ Politically motivated groups
- \ Rogue employees within the organisation
- \ Nation state sponsored “cyber warfare” units
- \ Individuals exercising curiosity or testing their skills

Whatever the source, the result of a successful security breach is that the organisation and its stakeholders are affected, sometimes seriously, and harm is caused.

One of the primary tools used by such attackers is malware, and it is essential that effective precautions are taken by Funds-Axis to protect itself against this threat.

This document sets out the organisations policy about defence against malware.

This control applies to all systems, people and processes that constitute the organisations information systems, including board members, directors, employees, supplies and other third parties who have access to Funds-Axis systems.

The following policies are relevant to this document:

- \ Mobile Device Policy
- \ Acceptable Use Policy
- \ Electronic Messaging Policy
- \ Software Policy

2. The Malware Threat

There is no single definition of the term “malware” in use but, for the purposes of this policy, the following definition is used:

“Malware is any code or software that may be harmful or destructive to the information-processing capabilities of Funds-Axis”

The term is derived from the phrase “malicious software” and may also be called malicious code or commonly (but inaccurately) a virus.

Malware comes in many forms and is constantly changing as previous attack routes are closed and new ones are found. The most common types of malware found today are:

- \\ **Virus:** a program that performs an unwanted function on the infected computer. This could involve destructive actions or the collection of information that can be used by the attacker.
- \\ **Trojan:** a program that pretends to be legitimate code but conceals other unwanted functions. Often disguised as a game or useful utility program
- \\ **Worm:** a program capable of copying itself on to other computers or devices without user interaction.
- \\ **Logic bomb:** malicious code set to run at a specified date and time, or when certain conditions are met.
- \\ **Rootkit:** a program used to disguise malicious activities on a computer by hiding the processes and files from the user.
- \\ **Keylogger:** code that records keystrokes entered by the user.
- \\ **Backdoor:** a program that allows unauthorised access at will to an attacker.

Often, these types of malware will be used in combination with each other. For example, an attacker will encourage an unwitting user to infect a computer with a virus which will allow unauthorised access. This initial access will then be used to install a rootkit to disguise further activities, a keylogger to capture keystrokes and a backdoor to allow future access without detection.

For malicious software to carry out its intended purpose, it needs to be installed on the target device or computer. There are a number of key ways in which malware infects computers and networks, although new ways are being created all the time.

Phishing involved tricking the user into taking some action that causes a malicious program to run and infect the computer. It is usually achieved via the blanket of sending of unsolicited emails (spam) with file attachments or web links included in them. When the user opens the file or clicks on the link, the malicious action is triggered.

Phishing attacks have become more sophisticated in recent years and can be believable and enticing to the user. More targeted versions of phishing have appeared, such as spear phishing (aimed at a particular organisation) and even whaling (aimed at one individual).

The widespread use of mobile code such as JavaScript on websites has provided attackers with another route to infect computers with malware. Often, websites will be created to host the malware, which is activated wither upon clicking a link or, in some cases, simply by visiting the website.

Increasingly, legitimate websites are being compromised and made to host malware without the owners knowledge, making this type of attack difficult for the user to avoid.

USB memory sticks, CDs, DVDs and other removable media devices provide an effective way of spreading malware on to additional computers. When the media is inserted into the machine, the malware will either run and infect the target or will copy itself onto the removable media in order to prepare to inject the next machine it is plugged into.

Hacking, or “cracking” as it is more accurately known, is a more targeted and therefore less common method of introducing malware on to a computer or network by gaining unauthorised access to the network from outside (and sometimes inside) the organisation. This method requires more knowledge on the part of the perpetrator and often exploits existing vulnerabilities in the software or network devices being used. Once access has been gained, malware will be installed remotely onto the compromised machine.

3. Anti-malware Policy

To prevent the infection of Funds-Axis computers and networks, and avoid the potentially dire consequences of such an infection, there are a number of key controls that will be adopted as policy.

The key concept adopted in this policy is that no single control should be relied upon to provide adequate protection. This is therefore not a choice between controls but a list of controls, all of which should be implemented where possible to guard against the threats outlined in the previous section.

A firewall will be installed at all points at which the internal network is connected to the Internet. Where possible, individual firewalls will be enabled on client computers. Access permissions must be set such that the user cannot disable the firewall.

3.1 Anti-malware software

A commercial, supported antivirus platform will be installed within the organisation at key locations:

- \ Firewall
- \ Email Servers
- \ Proxy Servers
- \ All other servers
- \ All user computers
- \ Mobile devices, including laptops, phones and tablets where possible

All antivirus clients will be set to obtain antivirus signature updates on a regular basis, either directly from the vendor website or from a central server with the organisation.

By default, real time scanning must be permanently enabled to provide protection. Regular full scans must also be carried out regularly.

Users must not be able to disable the protection which is configured centrally.

A system will be installed to filter out unsolicited and potentially harmful emails (spam). Types of attachments known to often contain malware must be blocked or removed before delivery to the user.

3.2 Application Installation

Users must not have sufficient administrative access to their computer to allow them to install unauthorised software onto it. Only approved software will be allowed, and this must be installed upon authorised request, except in the case of software made available via an approved app store, which may be installed by the user directly with no involvement from the technical team.

A whitelist of permitted software applications will be maintained and configured on systems that support this type of control.

Regular scanning of user computers to detect unauthorised software must be carried out.

Where available, application installations that support code-signing will be used, to guarantee the integrity and origin of the provided software.

3.3 Application Sandboxing

Where available, software applications that provide sandboxing capabilities will be used. Sandboxing is a security mechanism for separating running programs, providing additional protection against system failures and the exploiting of software vulnerabilities. This means that the impact of running untrusted software can be minimised, and its behaviour examined with less risk.

3.4 Software Vulnerabilities

Information on software vulnerabilities will be collected from vendors and third-party sources, and updates applied where available. If possible, and if permitted by the organisational policy, updates will be applied automatically as soon as they are released.

Vulnerability scanning must be carried out regularly, particularly on business-critical servers and networks.

For new vulnerabilities identified by Funds-Axis employees, a co-ordinated disclosure policy will apply.

3.5 Threat Awareness

Users must be made aware when starting with the organisation of the information security policy and be trained in ways to avoid falling victim to attacks such as phishing.

This awareness training must be repeated on a regular basis to all employees who make use of IT equipment.

Information about emerging threats will be obtained from appropriate sources and users alerted proactively of potential attacks giving as much detail as possible to maximise the chance of recognition.

Regular reviews will be carried out of business-critical servers and networks to identify any malware installed since the last review.