<< Company Logo>>

<< Anti Malware Policy >>

Version: 1.0
Date

Revision History

Date	Version	Author	Summary of Changes

Approvals

Name	Signature	Title	Issue Date	Version

Version: xx   **Date: xx**   **Company Name: xx**

Security Level: Internal   **Page 2 of 5**
NetHost Legislation- Cyber Essentials and ISO Standard Management System Certification Company, Scotland/England

info@nethostlegislation.co.uk,   **www.nethostlegislation.co.uk**

Contents

Contents

NetHost Legislation- Cyber Essentials and ISO Standard Management System Certification Company, Scotland/England

info@nethostlegislation.co.uk,   www.nethostlegislation.co.uk

INTRODUCTION

DOCUMENT PURPOSE

[Organisation] are increasingly dependent upon their usage of ICT networks as a key tool for managing and delivering services.

A major threat to the delivery of ICT services is malicious software (malware) which has the potential to undermine the confidentiality, integrity and availability of those services/data hosted on ICT systems or can adversely impact the underlying infrastructure hosting these systems and thus prevent access to the resources.

SCOPE

All the [organisation]'s information assets, including hardware, software, mobile devices and peripherals [including memory devices, PDAs, mobile phones] and all [employees/staff], contractors, temporary workers and third parties who use, work with or connect to organisational information processing facilities are within the scope of this procedure

POLICY

Below statements shall be complied with.

Policy Statements

No:	Statements
	The anti-malware software is capable of detecting and removing all known forms of malware, including viruses, Trojans, worms, spyware, adware, and rootkits.
	The anti-malware software is installed on all organisational information systems and devices, including workstations, laptops, servers, mobile devices, gateways and firewalls, and is configured with automatic updating in respect of the software and the virus definitions, and to carry out regular scans of the network environment. Alternatively, protection from malware by limiting installation of applications to an approved set or by application sandboxing
	The anti-malware software generates an audit log

	The anti-malware software is configured to scan at regular intervals
	The anti-malware software should have current signatures
	The anti-malware software scans all internet downloaded files
	The anti-malware software is configured for on access scan
	The anti-malware can scan web pages and warns about suspected malicious websites
	Ensure that anti-malware mechanisms are actively running and cannot be disabled or altered by staff, unless specifically authorized by management on a case-by-case basis for a limited time period.
	Where app-store or application signing is used, [organisation staff] are restricted from installing unsigned applications. Also that [organisation staff] only install applications that have been approved by [organisation] via a list of approved applications
	Where app-store or application signing, ensure that staff only install applications that have been approved by [organisation] and all list of approved applications should be documented.
	Where application sandboxing is used, ensure that applications within the sandbox are unable to access data stores, sensitive peripherals and local network

Version: xx   **Date: xx**   **Company Name: xx**

Security Level: Internal   **Page 5 of 5**
NetHost Legislation- Cyber Essentials and ISO Standard Management System Certification Company, Scotland/England

info@nethostlegislation.co.uk,   www.nethostlegislation.co.uk