Anti-Virus & Malware Policy
IT Knowledge Hub LLC (dba "Knowledge Hub Media")

1. General Policy

- Knowledge Hub Media systems **shall** run effective anti-virus and anti-malware software.

- Knowledge Hub Media IT anti-virus and anti-malware software **shall** be configured to detect and remove known viruses and malware.

- All Knowledge Hub Media IT systems (servers, desktops, laptops) **shall** run one of the NHS approved and supported anti-virus and anti-malware software packages.

- All servers, desktops and laptops **shall** be configured to run only one of the approved products at any time.

- Anti-virus and anti-malware software **shall** be kept up to date.

- Anti-virus and anti-malware definition files **shall** be kept up to date.

- Anti-virus and anti-malware software updates **shall** be deployed across the network automatically following their receipt from the vendor.

- Virus and malware signature updates **shall** be deployed across the network automatically following their receipt from the vendor.

- Anti-virus and anti-malware software **shall** be configured for real time scanning and regular scheduled scans.

- Tamper protection **shall** be enabled to prevent end users or malware altering the anti-virus and anti-malware software's configuration or disabling the protection.

- All IT equipment and removable media **shall** be scanned for viruses and malware before being introduced to the Knowledge Hub Media network, system or device.

- IT systems infected with a virus and malware that the anti-virus or anti-malware software has not been able to deal with **shall** be quarantined from the NHS network until virus free.

- Any instance of virus or malware infection or detection **shall** be documented and raised as a security incident.

2. Administrative Processes

- Changes that are required to the settings of any of anti-virus or anti-malware products **shall** follow the formal Knowledge Hub Media change control process.

- Knowledge Hub Media **shall** ensure that all anti-virus and anti-malware products are regularly and correctly updated from the vendor service.

- Knowledge Hub Media **may** periodically test anti-virus and anti-malware defences by deploying a safe and non-malicious test file.

- A log **shall** be kept of all scans undertaken, these logs **should** record as a minimum:

- Date.

- Time.

- Addresses of areas scanned.

- Malware found.

- Any action taken by the anti-virus and anti-malware software (e.g. quarantine or delete).

- To prevent misuse and tampering by unauthorised staff, all administrative settings in the deployed anti-virus and anti-malware products **shall** be secured by means of a password.

3. Important Keywords

Malware - Malware, or "malicious software," is an umbrella term that describes any malicious program or code that is harmful to systems.

Hostile, intrusive, and intentionally nasty, malware seeks to invade, damage, or disable computers, computer systems, networks, tablets, and mobile devices, often by taking partial control over a device's operations. Like the human flu, it interferes with normal functioning.

Malware is all about making money off you illicitly. Although malware cannot damage the physical hardware of systems or network equipment, it can steal, encrypt, or delete your data, alter or hijack core computer functions, and spy on your computer activity without your knowledge or permission.

Virus - A type of malicious code or program written to alter the way a computer operates and is designed to spread from one computer to another. A virus operates by inserting or attaching itself to a legitimate program or document that supports macros in order to execute its code. In the process, a virus has the potential to cause unexpected or damaging effects, such as harming the system software by corrupting or destroying data.

Software - A set of instructions or programs instructing a computer, mobile device, or server to do specific tasks. Software is a generic term used to describe computer programs. Scripts, applications (apps), programs and a set of instructions are all terms often used to describe software.

Systems - Electronic data processing, information, recordkeeping, communications, telecommunications, account management, inventory management and other computer systems (including all computer, server and mobile device applications, programs, software, databases, firmware, hardware and related documentation) and Internet websites.

4. Terminology

Shall - This term is used to state a **Mandatory** requirement of this policy.

Should - This term is used to state a **Recommended** requirement of this policy.

May - This term is used to state an **Optional** requirement.