ANTI VIRUS POLICY

Executive Sponsor & Function:

Director of Workforce and Organisational Development

Document Author:

BISSU Senior Manager

Approved by:

[HEIW Executive Team]

Approval Date:

Date of Equality Impact Assessment:
14/03/2019

Equality Impact Assessment Outcome:
This policy has been screened for relevance to equality. No potential negative impact has been identified so a full equality impact assessment is not required.

Review Date: April 2020

Version: v1

EXECUTIVE SUMMARY
Anti Virus Policy

Overview:	To raise everyone's awareness of software viruses impacting core functions and to minimise the risks for Health Education and Improvement Wales (HEIW) and other NHS Wales organisations.
Who is the policy intended for:	Everyone who is employed or engaged by HEIW including part time workers, temporary and agency workers and those holding honorary contracts.
Key Messages included within the policy:	The key objectives are: • To ensure that everyone working for HEIW are aware of the dangers of malicious code (Spyware, Malware, Worms & Trojans etc.) and their responsibilities to minimise the likelihood and impact of viruses to the HEIW and NHS Wales • To protect business continuity • To comply with the Information Security policy • To effectively manage software resources The main routes of a computer virus infection are: • Downloading unauthorised software from the Internet • Virus's hidden in e-mail attachments from un-trusted or unexpected sources (e.g. the email sender can sometimes be impersonated or "spoofed") • Using non-NHS internet based e-mail systems without approval of your local IT Department / Service Desk (as their use is normally prohibited in Email Policy) • Insertion of removable media, that may have been used outside the HEIW, into a HEIW computer without checking for viruses (e.g. CDs, DVDs, memory sticks / USB memory devices, floppy disks and any other removable media capable of carrying data or programs) • Connecting a non-NHS HEIW laptop or PC (that does not have anti-virus software with up to date virus definition files) to HEIW's network

PLEASE NOTE THIS IS ONLY A SUMMARY OF THE POLICY AND SHOULD BE READ IN CONJUNCTION WITH THE FULL POLICY DOCUMENT

CONTENTS **Page Number**

1. Introduction

For the purpose of this Policy, all forms of malicious computer code created with the specific intent of disrupting the operation of networks, computer systems or computer controlled equipment, will be referred to as viruses.

As a result, of becoming infected by a virus, HEIW's capability of day to day operation may be compromised, or depending upon the virus's capability to traverse interconnecting networks NHS Wales may be negatively impacted as a whole.

This policy is aimed at raising awareness amongst HEIW employees; and by complying with the policy and associated anti-virus procedures, we can minimise the risks to the HEIW and other NHS Wales organisations.

The main routes of infection are listed below:

- Downloading unauthorised software from the Internet
- Virus's hidden in e-mail attachments from un-trusted or unexpected sources (e.g. the email sender can sometimes be impersonated or "spoofed")
- Using non-NHS internet based e-mail systems without approval of your local IT Department / Service Desk (as their use is normally prohibited in Email Policy)
- Insertion of removable media or wireless transmission, that may have been used outside HEIW, into a HEIW computer without checking for viruses (e.g. CDs, DVDs, memory sticks / USB memory devices, floppy disks and any other removable media capable of carrying data or programs)
- Connecting a non-NHS HEIW laptop or PC (that does not have anti-virus software with up to date virus definition files) to the HEIW's network
- The Software, E-mail and Internet Policies provide further detail on the risks and guidance on risk mitigation.

2. Scope

The scope of this policy includes (but is not restricted to):

- All HEIW computers (PCs, laptops, servers, PDA's and mobile phones)
- All HEIW employees
- People under guidance / direction of HEIW employees (e.g. learners, visiting colleagues, engineers etc.)
- All HEIW Honorary Contract holders

3. Objectives

- To ensure all persons employed or engaged by HEIW are aware of the dangers of malicious code (Spyware, Malware, Worms & Trojans etc.) and their responsibilities to minimise the likelihood and impact of viruses to HEIW and NHS Wales
- To protect HEIW's reputation.
- To comply with the Information Security policy.
- To effectively manage software resources.

4. Responsibilities

4.1 Users

Users are responsible for their own actions and must:

- Adhere to this policy and associated policies and procedures
- Report incidents to appropriate managers as quickly as possible
- Discuss any identified risks and security issues with the service to the appropriate managers.

Comply with local anti-virus procedures and in particular:

- All suspected occurrences of a virus detected by any means MUST be reported to your local IT Department / Service Desk, and the computer switched off until a technical representative have carried out action according to the local anti-virus procedure and confirmed that the computer is free from infection

- Unauthorised software from whatever source (e.g. screen savers; internet; memory sticks, floppy disks, CD-ROMs, or web sites, etc.) must not be used on HEIW computers without approval of your local IT Department / Service Desk (refer to HEIW Software Policy for further details

- All removable media or downloaded files from outside the HEIW must be processed in accordance with local anti-virus procedures before being accessed

- Comply with the HEIW E-mail and Internet policies to minimise risk of infection

- Users must follow local IT Department / Service Desk procedures to ensure PCs and laptops and other portable computing devices receive regular virus definition updates (e.g. PCs left powered on (but logged off) overnight and portables returned to base at least weekly).

Users must not allow Third party IT hardware to be connected to the network without approval from their local IT Department / Service Desk, who will ensure appropriate anti-virus software is installed with the latest virus definitions.

4.2 Managers

All Managers are directly responsible, ensuring that:

- Staff are aware of this policy
- Staff are made aware of any changes to the policy
- Staff are trained appropriately
- Suspected incidents are reported and investigated

4.3 HEIW Executive

- Ensure everyone working for HEIW are made aware of this policy and that they comply with it.
- Ensure this policy is part of HEIW's generic induction process.

- Ensure the HEIW has the resources to purchase, deploy and maintain anti-virus software or appropriately outsourced (NWIS)

4.4 HEIW Board

The Board's responsibilities are:

- To provide appropriate resources to fully implement this policy
- To fully endorse, support and implement the controls outlined in this policy

4.5 Local IT department

Comply with local anti-virus procedures and in particular:

- Ensure portable computers etc. are brought back and connected to the HEIW network for regular updates of virus definition files (once every two weeks - minimum)
- Ensure Users awareness is maintained in regard to the recognition and danger of viruses, and anti-virus procedures by regular briefings and publicity
- Record occurrences of viruses according to local information security incident procedures. (Note: in the event that a potentially significant infection is identified, management must be made aware that critical services may be affected or systems / services shutdown to avoid further spread of the infection)

4.6. NHS Wales Informatics Service

- Ensure appropriate HEIW anti-virus procedures are in place and updated in accordance with new threats and vulnerabilities.
- Ensure that anti-virus software is reviewed for efficiency and re-licensed on an ongoing basis.
- Deployment of the anti-virus solution appropriately including each new release of the software from the software supplier.
- Set-up facilities to automatically update virus definition files for all computers on the network.
- Check Third Party machines for appropriate anti-virus software and virus definition files before allowing connectivity to segregated areas of the HEIW network.

5. Further Information

Further information can be obtained from the local IT Helpdesk / service desk.

6. References

This policy should be read in conjunction with the following documents:

- Information Security Policy
- IT Software Policy
- Internet / Intranet Access Policy
- Email Policy
- Information Governance Policy