VIRUS PROTECTION POLICY

Introduction

1. The objective of this Policy is to protect the integrity and availability of the Organisation's information by means of effective antivirus measures.
2. The Organisation is committed to protecting itself from the harm that is caused by malicious software.
3. Similarly the Organisation is aware of its third party responsibilities and takes all steps to avoid passing viruses and the like to other users.

Responsibilities

1. The CEO is responsible for selecting and deploying antivirus software for use on the Organisation's servers, PCs and laptops, and for arranging the necessary updates.
2. The organisation take responsibility for the deployment and management of antivirus on company owned systems. Users of home computing equipment who have remote access rights to the Organisation's internal systems must ensure that there is sufficient and current antivirus protection on their equipment.
3. The responsibility for monitoring the relevant event logs and responding to incidents as outlined in the Organisation's Network Systems Monitoring Policy.
4. Virus warnings are raised by automated tickets, dealt with by the Help Desk.
5. Suspected infections should be reported to the Help Desk.

Organisation-wide Antivirus Measures

1. To protect against virus infection via e-mail, all inbound e-mails are scanned on the e-mail server and/or individual PCs using antivirus software that is in addition to the one installed on other servers and clients.
2. To protect against virus infection via physical media or web download, on-access antivirus software is deployed on the Organisation's servers and client PC's.
3. The antivirus software on the Organisation's servers and clients' servers is automatically updated daily.
4. In the event of a threat of infection by a virus that might not be isolated by the software, e.g. very new viruses, the Internal IT Manager will issue a warning to alert all users. The warning will include a description of characteristics to watch for.
5. To enable data to be recovered in the event of a virus outbreak in the Organisation's systems, server backups are carried out in accordance with the Organisation's Backup Policy.
6. The Organisation's E-mail and Internet Acceptable Usage Policy includes instructions concerning virus protection. Any serious breach of the Organisation's Antivirus Protection Policy will result in the withdrawal of e-mail and Internet privileges in addition to any other disciplinary action.

Employee responsibilities with regard to protecting against infection by malicious software

The Organisation is aware that the only truly effective defence against the harm caused by malicious software is a combination of technology and user awareness. Therefore all of the relevant employees of the Organisation have been instructed as follows:

1. Inform the Help Desk immediately on receipt of a suspicious file or e-mail attachment. Leave the attachment closed and await further instructions
2. If required, macros are disabled whenever the relevant dialogue box appears, unless absolutely certain of the source of the document
3. Save downloads to disk rather than opening them from current location. This gives the antivirus software a better chance of detecting any malicious code. Large downloads that are no longer required should be deleted to save system storage space
4. Switch off any device that is suspected of being infected by a virus and ensure isolation from any network, and immediately inform the Help Desk
5. Do not open any unexpected e-mail attachments, even if the e-mail appears to come from a known source
6. Do not open an e-mail or instant messaging attachment from an unknown or suspicious source, or one with a double extension, such as *.file.txt.scr*
7. Do not download any software or executable file whatsoever from the Internet without prior permission from the Internal IT Manager
8. The only exception to the above is the downloading of drivers or patches by authorised engineers or the Internal IT Manager
9. Do not flood the Organisation's system by passing on unconfirmed virus warning messages. The only virus warnings within the Organisation must come from the Internal IT Manager.

Policy Sign-off

Date of Issue:	27/10/2020
Date of Next Review:	15/09/2021
Name:	Tim Barber
Signed:	

Amendment History

Version	Modified On	Modified By	Comments
1.0	15/09/2020	Jo Holloway	
2.0	27/10/2020	Jo Holloway	Updating responsibilities and date