University of Ghana

Anti-Malware Policy

1. Purpose

University of Ghana Computing Systems is mandated to ensure IT systems and facilities of the University are secure and not subject to improper use. A malware infection is costly to the University and often time-consuming for individuals. This may be through the loss of data or access to IT systems, staff time to recover a system, or the delay or loss of important work. This Policy sets out the responsibilities of all users, including users of privately owned devices that connect to the University IT facilities, in relation to malicious software. These measures do not guarantee security, but they will help to significantly reduce the risk of widespread malware infection at the University.

All users need to read, understand, and comply with this Policy.

2. Objectives

The objectives of this document are:

- To set out user responsibilities with regard to malicious software prevention
- To set out the rules governing the application and use of malicious software prevention systems at the University

3. Scope

This Policy applies to all users and other users of privately owned devices that connect to the University IT facilities. By following this Policy, users will help to protect themselves and other University users against malicious software. The University IT Policy, on which this Policy expands, require everyone to take the practical steps needed to keep this protection active and up to date.

4. Policy Statements

a. All University personal computers and servers that are connected to the University network or otherwise using the IT facilities must run an **approved** and **up-to-date** anti-virus product that continually monitors for malicious software. Details of the approved products can be found at http://ugcs.ug.edu.gh/ITSecurity

b. All personal computers, devices and servers connected to the University network must run a version of the Operating System and installed applications with the tested latest available patches applied.

c. Computers supplied by University will be supplied with an approved anti-virus product.
d. Any non-University owned devices must run an appropriate anti-virus product.
e. Do not try to uninstall or disable anti-virus software. Any messages suggesting that anti-virus protection has been disabled should be reported to servicedesk@ug.edu.gh.
f. If users experience difficulties with a recommended anti-virus product, requests for technical support may be made through servicedesk@ug.edu.gh
g. Users are prohibited from proceeding with any activity intended to create and / or distribute malicious code (viruses, worms, etc) on the University network or IT facilities.
h. The University reserves the right to disconnect any device from the network if an infection is found or suspected. The device will be disconnected until the infection is removed and suitable preventative tools have been installed on the device.
i. If you suspect that a device is infected with a virus, report the incident to the servicedesk@ug.edu.gh and / or to local IT staff as soon as possible.
j. Email attachments may be scanned by an anti-virus product before delivery.
k. The University recommends that all applications are installed from known sources
l. UGCS shall deploy necessary tools to protect the university community and its information resources from malware and associated threats.
m. Individuals may be subject to disciplinary action if this Policy is breached.

5. Scams and Hoaxes

Many spam emails are sent with dire warnings about messages with topical subjects or attachments. The receiver is often asked to forward the email to all colleagues and friends around the globe or to volunteer their credentials onto some platform. If you are unsure whether an email you receive is a hoax or scam, you can report at servicedesk@ug.edu.gh. Do not forward these messages on or respond to these emails. If you receive such a message, just delete it.
Some websites you visit will suggest your PC or tablet is infected with a new virus and hence you need to run / install / purchase their anti-virus software. Do not click this message. Instead, check that you have the latest signatures and updates in your existing anti-virus software and then run a manual scan.
If you download a fake anti-virus application, or think that your device has a virus, please report this to servicedesk@ug.edu.gh or to local IT staff as soon as possible, because it will be much easier to remove if reported promptly.

6. Definitions

User: The term “User” refers to any person authorized to use University ICT facilities.

Malware: The word ‘malware’ is used collectively to denote all types of malicious software, including viruses, worms, Trojans, macros, mail bombs and rootkits.

Virus: A virus is a piece of self-replicating computer program code that is designed to destroy or damage digital information, or to steal user or business data.

There are many potential sources of malicious software, including websites, social media, USB memory sticks, unsolicited CDs, electronic mail, and software or documents copied over networks such as the campus network or the internet.

Scam: The term scam is any message that is intended to perpetuate fraud on the recipient

Hoax: Hoaxes are deliberate fabricated falsehood meant to persuade intended recipients to take an some action which will be detrimental to the recipient.

7. Revision History

Version	Date	Change Description	Author
0.1	Sept. 2015	Initial Draft for review	Head, IT Security
0.2	Oct. 2015	Review	Deputy CITO, IT Planning, Security and Support.