# Information Security Standard 12.2a

**Controls Against Malicious Software**

***Initially Approved: April, 17, 2015***
***Revised: July 30, 2020 (as the Controls Against Malicios Software Standard)***
***Administering Office: Office of the CIO***

## I. STANDARD STATEMENT

This standard operates under University Policy 117 Information Security. The purpose of this standard is to establish controls that ensure that WCU employees who use university IT systems and networks do so in a manner that does not compromise the security and integrity of the systems and networks.

## II. SCOPE AND APPLICATION OF THE STANDARD

This standard applies to all employees, vendors and agents operating on behalf of Western Carolina University.

## III. DEFINITIONS

*Malicious software or malware* is software intended to damage or disrupt operation of a computing system or network, gather sensitive information, gain unauthorized access to private computer systems, or to take partial control over its operation.

## IV. CONTROLS AGAINST MALICIOUS SOFTWARE

a. Each user is responsible to ensure that the Internet is used in an effective, ethical, and lawful manner. Additionally, employees are cautioned to limit their web surfing to reputable web sites and avoid opening e-mails and attachments received from unknown individuals or are otherwise suspicious in nature.
b. It is best practice that employees do not install shareware, freeware, commercial, or personally developed software without authorization from their department manager or the IT Division. This includes Java and ActiveX-based programs run within a web browser. Additionally, department managers may establish internal department policy rleated to this activity.
c. Confidential information must only be transmitted over the Internet when protected by approved encryption, in accordance with University Policy 97 and the Data Handling Procedures.
d. University-owned production servers and personal computers will be protected from viruses and known malicious software. The IT Division will ensure that all software used for scanning for malicious software is updated in a timely

manner. Additionally, the IT Division will operate and maintain systems to reduce the chances of malicious Email being delivered.

e. All university-owned computer equipment connected to the WCU network/system shall be up to date with the manufacturer's operating systems security software patches as authorized unless there is a specific reason approved by the IT Division.
f. Any WCU workforce member suspecting malicious software infections must immediately report their suspicions to their department manager and to the IT Division.

## V. ENFORCEMENT

Failure to comply with this standard will increase the chance of a data breach which may result in the imposition of fines, or other significant penalties against WCU, and disciplinary action against employees.

## VI. REFERENCES

International Standards Organization (ISO/IEC 27002, 12.2 Controls against malware)

*University Policy 117 Information Security*
*University Policy 97 Data Security and Stewardship*

45 CFR Part 164, Subpart C, Security and Privacy