PROCEDURE MANUAL

ARIZONA WESTERN COLLEGE			**PROCEDURE 223.008**
			Page 1 of 2
			Last Revision Date: 04-01-2024; 05-22-2023; 03-21-2022
			Effective Date: 03-22-2022
			Last Review Date: 04-01-2024
Section:	Technology	**Subject:**	Computer Virus Management

PURPOSE

The purpose is to outline the procedure Arizona Western College's (AWC) Information Technology Services & Support (ITSS) defines antivirus setup on all college computers and servers.

SCOPE

This procedure applies to all users of AWC technology assets including employees, students, volunteers and contractors.

PROCEDURE

1. Antivirus is software installed on all college computers to protect them against malware.

2. Virus Controls
   - 2.1 Users (Employee and/or Student) shall not disable anti-virus software, or any other protective measure put in place to ensure the safety of our computing environment, such as desktop firewall, or laptop encryption, In accordance with the College Acceptable Use Procedure (223.001).
   - 2.2 Users must not alter the security configuration of the College's equipment.
   - 2.3 Users must not open files or macros attached to e-mail from unknown, suspicious, or untrustworthy senders. Users should delete these e-mails and attachments immediately and clear them from 'Deleted Items.'
   - 2.4 Users shall delete spam, chain e-mail, and other junk e-mail without forwarding, consistent with the College Acceptable Use Procedure (223.001).
   - 2.5 Users shall not visit sites or download files from unknown, suspicious, or untrustworthy sources.
   - 2.6 The college's email system will have a separate antivirus and spam filtering system to help identify and eliminate threats before they reach the end-user.

3. Virus Scanning of Servers and Workstations
   - 3.1 All workstations and servers that connect to Arizona Western College internal networks or that process, store, college data shall run college approved anti-virus software. This equipment shall run the current version with the most recent updates available.
   - 3.2 Workstations and laptops will have current anti-virus software configured to run a full scan of the machine weekly.

3.3 Servers will have current real-time anti-virus software configured.

3.4 Files that have been identified as infected will be automatically deleted. The event will be logged. Log files are reviewed during ticket resolution or if additional factors indicate if investigation is necessary.

4. Virus Incident or Suspicious Activities

4.1 Users must immediately report all suspected information technology/security problems, vulnerabilities, and incidents to the Information Technology Services & Support (ITSS) department. In the case of a vendor, they will contact their college contact. If a virus scan indicates that a file or workstation is infected, the event must be reported regardless of if the file has been 'cleaned' by the anti-virus software or not. Messages for known events with signatures may only be suppressed at the discretion of the ITSS department.

4.2 Employee's Outlook is configured with a Phishing Alert button so that employees can report suspicious emails, attachments, or other concerns identified by the employee.

5. Virus Updates

5.1 The virus program will be set to update daily.

6. Virus Incident Notification

6.1 ITSS staff shall notify the Chief Information Officer (CIO) and the Chief Information Security Officer (CISO) or their designee, of any new potential viruses currently being spread via email or the Internet.

6.2 The CISO shall determine if there is a potential threat to internal users and will assign responsibility to an ITSS staff person to determine if the current latest available update for the antivirus program can detect the virus in question.

6.3 The CISO will determine if there is a need to notify users of the virus and if necessary, contact will be made via email to all users.