PROCEDURE MANUAL

ARIZONA WESTERN COLLEGE			**PROCEDURE 223.008**
			Page 1 of 3
			Last Revision Date: 04/13/2026
			Effective Date: 03/22/2022
			Last Review Date: 04/13/2026
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 and to define the processes for preventing, detecting, and responding to computer viruses and malware.

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 against malware.

2. Virus Controls
   - 2.1 Users (Employee and/or Student) are not permitted to 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 are not permitted to alter the security configuration of the College's equipment.
   - 2.3 Users are not permitted to 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 are permitted to delete spam, chain e-mail, and other junk e-mail without forwarding, consistent with the College Acceptable Use Procedure (223.001).
   - 2.5 Users are not permitted to 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.
   - 2.7 Users shall not input, process, or generate College data using artificial intelligence tools in ways that bypass security controls, expose PII and/or sensitive information, or violate College procedures and policies.

3. Virus Scanning of Servers and Workstations
   - 3.1 All workstations and servers connected to Arizona Western College internal networks, or that process, store, and college data, will have college approved anti-virus software. This equipment will run the current version with the most recent updates available.
   - 3.2 TSS is responsible for ensuring antivirus deployment, updates, and monitoring across all systems and configured to run a full scan of the machine regularly, as frequently as 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. Incident Response (223.017) 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 whether 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 Reference Incident Response (223.017) for notification requirements and process.
   - 6.2 ITSS staff should notify the Chief Information Officer (CIO) or their designee of any new potential viruses currently being spread via email or the Internet.
   - 6.3 The CIO 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.
   - 6.4 Depending on severity, the CIO may engage the Crisis Communications Team or Emergency Response Team to assist, address, and contain the incident.
   - 6.5 The CIO 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.

HISTORY

IT Reviewer Name	Update Date	AWC Reviewer	Approval Date
Tyler Vodehnal	1-24-2023	Dr. Daniel Corr	5-23-2023
Scott Estes, Caleigh Flores, Tyler Vodehnal	11-20-2023		
Tyler Vodehnal	04-01-2024	Ashley Herrington	04-01-2024
Scott Estes, Tyler Vodehnal, Mercedes Soto	02-04-2025	Dr. Daniel Corr	05/06/2025
Scott Estes, Tyler Vodehnal	02/04/2026	Dr. Reetika Dhawan	04/13/2026