PROCEDURE MANUAL

ARIZONA WESTERN COLLEGE		**PROCEDURE 223.013**	
		Page 1 of 3	
		Last Revision Date:	04-01-2024
		Effective Date:	03-22-2022
		Last Review Date:	05-06-2025
Section:	Technology	**Subject:**	Screen and Application Lock Procedure

PURPOSE

The purpose is to outline the procedure Arizona Western College's (AWC) Information Technology Services & Support (ITSS) measures to secure Arizona Western College (AWC) computers from unauthorized access to college computers while employees are away from their desks.

SCOPE

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

PROCEDURE

1. Definition
   - 1.1. Screen Saver/Lock Screens are a security measure initiated by the computer's operating system when a user is not active on their computer.
   - 1.2. Application Timeouts are a security measure initiated by the application to end a session when there is no user activity.
2. Screen Savers or Lock Screens
   - 2.1. AWC requires a screen saver or lock screen to "lock" after 15 minutes of employee inactivity.
   - 2.2. Each AWC computer is configured for automatic lock screen activation after the maximum time of inactivity has been exceeded.
   - 2.3. Employees are not permitted to manage their own time limit.
   - 2.4. Classrooms and Instructional Labs have their own timeout, which is a 90-minute time frame to better facilitate instruction.
3. Application Timeouts
   - 3.1. Colleague sessions will follow Inactivity Expirations as set forth in Procedure 223.10
   - 3.2. Other applications that will support timeouts and contain sensitive information will be configured in accordance with this procedure.
4. Employee Responsibilities
   - 4.1. Employees must comply with this standard and all procedures referenced within this standard.
   - 4.2. Employees must activate the screen saver or lock screen when stepping away or leaving their workstation. The screen saver or lock screen may be activated by using Ctrl, Alt, & Delete, and selecting "Lock this computer", or by using the Windows key and the "L" key.

4.3. Employees using non-Windows Operating Systems (Mac, LINUX, etc.) must ensure their desktop session is locked when stepping away or leaving their workstation.

4.4. If an employee computer fails to "lock" automatically after 15 minutes of inactivity that user must notify the AWC Service Desk immediately.

4.5. Employees must be aware of other individuals in and around your workstation when looking at or discussing confidential information. Employees should position their computer screens such that unauthorized individuals cannot easily see the sensitive information displayed. When appropriate, equipment to obscure screen view will be installed at workstations potentially viewable by unauthorized persons.

REFERENCE

1. National Institute of Standards and Technology. (2020). NIST Special Publication 800-53, Revision 5: Security and Privacy Controls for Information Systems and Organizations