

PROCEDURE MANUAL

	PROCEDURE 223.013		
	Page 1 of 2		
	Last Revision Date:	04/13/2026	
	Effective Date:	03/22/2022	
Last Review Date:	04/13/2026		
Section:	Technology	Subject:	Screen and Application Lock Procedure

PURPOSE

The purpose of this procedure is to define screen and application locking requirements to protect Arizona Western College (AWC) systems and data from unauthorized access when devices are unattended.

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. This control is implemented to reduce the risk of unauthorized access to unattended systems.
 - 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 223.010.
 - 3.2. Other applications that will support time-outs 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's 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

HISTORY

IT Reviewer Name	Update Date	AWC Reviewer	Approval Date
Scott Estes	03-08-2023	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	2-4-2025	Dr. Daniel Corr	05-06-2025
Scott Estes, Tyler Vodehnal	02/04/2026	Dr. Reetika Dhawan	04/13/2026