PROCEDURE MANUAL

	PROCEDURE 223.12	
	Page 1 of 2	
	Last Revision Date:	5-22-2023; 03-07-2023
	Effective Date:	3-07-2023
	Last Review Date:	5-22-2023
Section: Technology	**Subject:**	Multi-Factor Authentication

PURPOSE

The purpose is to outline the procedure Arizona Western College's (AWC) Information Technology Services & Support (ITSS) enables for Multi-Factor Authentication (MFA) connections to the network and information systems on and off campus. These standards are designed to minimize the potential security exposure to AWC from damages which may result from unauthorized use of college resources. MFA adds a layer of security which helps deter the use of compromised credentials.
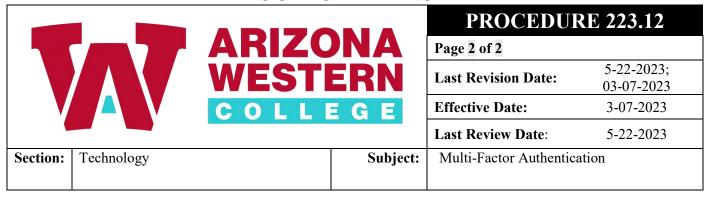
SCOPE

The procedure applies to all members of the AWC community, including affiliates, students, faculty, staff, retired employees, and volunteers that use their AWC account to connect to the College's network or technology resources. This procedure applies to any system accessing college data where MFA is utilized.

PROCEDURE

1. All individuals must engage in one additional step beyond the normal login process to access campus resources and the campus network while off the college network. Individuals are required to register a second approved device or a secondary means to authenticate their identity.

2. MFA is required on all existing and new accounts created.

3. MFA is required for all externally-exposed enterprise or third-party applications, where college supported. Enforcing MFA through a directory service or SSO provider is a satisfactory implementation of this safeguard.

4. MFA is required for all remote network access.

5. MFA is required for all administrative access accounts, where supported by college, on all enterprise assets, whether managed on-site or through a third-party provider.

6. Responsibilities
    a. It is the user's responsibility to promptly report compromised credentials to the Information Technology Support and Services department.
    b. It is the user's responsibility to promptly report a lost or stolen MFA device to the Information Technology Support and Services department

7. Exemptions
    a. There may be situations in which a college community member has a legitimate need to use technology resources outside this procedure's scope. The Chief Information Officer may approve, in advance, exception requests based on balancing the benefit versus the risk to the College.

PROCEDURE MANUAL

Section:	Technology	**Subject:**	Multi-Factor Authentication

IT Reviewer Name	Update Date	AWC Reviewer	Approval Date
Tyler Vodehnal	1-24-2023	A Herrington	3-7-2023
		D Corr	5-22-2023