PROCEDURE MANUAL

ARIZONA WESTERN COLLEGE		**PROCEDURE 223.012**	
		Page 1 of 3	
		Last Revision Date:	04/13/2026
		Effective Date:	3/07/2023
		Last Review Date:	04/13/2026
Section:	Technology	**Subject:**	Multi-Factor Authentication

PURPOSE

The purpose is to outline the procedure Arizona Western College's (AWC) Information Technology Services & Support (ITSS) takes to enable Multi-Factor Authentication (MFA) connections to information systems on and off campus. These standards are designed to minimize the potential security exposure to AWC from damage which may result from unauthorized use of college resources. MFA, in alignment with applicable security standards and regulatory requirements, adds a layer of security which helps deter the use of compromised credentials.

SCOPE

This procedure applies to all users of AWC technology assets including employees, students, volunteers, and contractors. This procedure applies to any system accessing information systems where MFA is utilized regardless of location. MFA is enforced according to FTC.gov guidelines to protect any individual accessing AWC customer information.

PROCEDURE

1. All individuals, regardless of connection method or location, must take one additional step beyond the normal login process to access campus information systems. 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, when supported. Enforcing MFA through a directory service or SSO provider is a satisfactory implementation of this safeguard.
4. MFA is required for all administrative access accounts, when supported by systems, on all enterprise assets, whether managed on-site, remote, or through a third-party provider. Additionally, all employees with elevated permissions will be required to use a multi-protocol security key (i.e. YubiKey) to enforce MFA for direct access to local machines.
5. 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.

6. 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.
    b. Additionally, some employees may be issued a multi-protocol security key (i.e. YubiKey) to enforce MFA if they do not have access to devices or other means to MFA.
    c. MFA exemption requests will be submitted via form and approved by the CIO and/or Director of Infrastructure and documented. https://wkf.ms/3yxZkfB
    d. In most cases, the exemption will only be granted for 30 days, but some exemptions can be extended on a case by case need basis.

REFERENCES

https://www.ftc.gov/business-guidance/resources/ftc-safeguards-rule-what-your-business-needs-know

HISTORY

IT Reviewer Name	Update Date	AWC Reviewer	Approval Date
Tyler Vodehnal	1-24-2023	D Corr	5-22-2023
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	3/4/2025	Dr. Daniel Corr	05/06/2025
Scott Estes, Tyler Vodehnal	02/06/2026	Dr. Reetika Dhawan	04/13/2026