PROCEDURE MANUAL

ARIZONA WESTERN COLLEGE

PROCEDURE 223.007

Page 1 of 3	
Last Revision Date:	3-4-2025
Effective Date:	03-07-2022
Last Review Date:	05-06-2025

Section:	Technology	**Subject:**	Virtual Private Network (VPN) and Remote Access

PURPOSE

The purpose of this procedure is to outline how Arizona Western College's Information Technology Services & Support (ITSS) ensures secure Virtual Private Network (VPN) access and remote access methods. It aims to protect the College's IT assets and data, including network infrastructure, servers, workstations, financial, HR, student information, and other data vital for the College's operations. The procedure establishes approved remote access methods, guidelines for managing and securing College resources, and procedures for implementing the policy.

The procedure's core philosophy is to keep College data within the internal network while allowing remote access to necessary resources for users to perform their jobs. It prohibits actions like moving or copying protected information from the College network to remote systems. The procedure focuses on access methods and authentication but does not define approved users or access privileges, which are granted by Data Custodians, Data Owners, or Business unit managers.

SCOPE

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

PROCEDURE

1. Remote Access
   - 1.1 Remote access must be strictly controlled. Control will be enforced via domain passphrase and Multi-Factor Authentication. For information related to Multi-Factor Authentication please refer to Multi-Factor Authentication procedure 223.012.
   - 1.2 General responsibilities for the use of devices on Arizona Western College's network (on-campus or remote) are included in the Acceptable Use Procedure 223.001.
   - 1.3 At no time should any Arizona Western College user provide their login or email password to anyone, including family members.
   - 1.4 For users that wish to access our secure resources remotely with elevated privileges, they will be required to submit a Privileged Access Application via our ITSS department.

2. VPN
   - 2.1 VPN is software that enables employees to remotely access the AWC network. This procedure applies to all employees and contracted vendors utilizing VPN to remotely access the network to support the college's operation.

2.2 It is the responsibility of employees with VPN privileges to ensure that unauthorized users are not allowed access to AWC internal networks.

2.3 VPN use is to be controlled using a username / password authentication. It is required each time a user wants to remotely connect to the AWC Network. All username/ password combinations are stored within the college network's active directory. As per general practice, this password should never be shared with another individual.

i VPN will be configured to use Multi-Factor Authentication. The End User will be required to use a second device to confirm identification.

2.4 VPN users will be automatically disconnected from the AWC network after 16 hours of inactivity. The user must then log on again to reconnect to the network.

2.5 All AWC employees must connect to the VPN service only on college computers. VPN will only be installed on college-owned computers. All account requests must be approved by the requestor's Cabinet Member, or designee. Requests for access should be sent from the Cabinet Member, or their designee's office to the Information Technology Services & Support (ITSS) service desk for review and setup. Along with the request, justification and/or business cases should accompany the request.

2.6 AWC Information Technology Services & Support (ITSS) Leadership may, in an individual case, allow third party vendor access to college resources after verification of the policies and procedures pertinent to the computer issued to the third party by their IT department.

i All third-party access will be disabled after the work is completed.

ii ITSS will review disabled third-party VPN accounts and purge accounts as defined in SOP account review process.

2.7 To ensure a successful VPN experience, user connections must have Broadband / high speed internet connection. For employees on slower connections, they may not allow consistent access to the college systems.

2.8 VPN Access can be revoked for several reasons below, but not limited to:

i User has returned to campus from remote work assignment.

ii User moved to another position within college that doesn't require VPN.

iii User violates Acceptable Use Procedures.