


PROCEDURE MANUAL

		PROCEDURE 223.007	
		Page 1 of 2	
		Last Revision Date:	04-01-2024; 05-22-2023; 03-07-2022
		Effective Date:	03-07-2022
		Last Review Date:	04-01-2024
Section:	Technology	Subject:	Virtual Private Network (VPN)

PURPOSE

The purpose is to outline the procedure Arizona Western College's (AWC) Information Technology Services & Support (ITSS) takes to support Virtual Private Network (VPN) access.

SCOPE

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

PROCEDURE

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. It is the responsibility of employees with VPN privileges to ensure that unauthorized users are not allowed access to AWC internal networks.
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.
 - 3.1 VPN will be configured to use Multi-Factor Authentication. The End User will be required to use a second device to confirm identification.
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.
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 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.

6. AWC Information Technology Services & Support (ITSS) Leadership may, on 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.

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

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

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

8. VPN Access can be revoked for a number of reasons below, but not limited to:

8.1 User returns to campus from remote work.

8.2 User moves to another position within college that doesn't require VPN.

8.3 User violates Acceptable Use Procedures.