ADMINISTRATIVE PROCEDURE 3721

DESERT COMMUNITY COLLEGE DISTRICT

VIRTUAL PRIVATE NETWORK (VPN)

Virtual Private Network (VPN) connections provide a convenient way for authorized individuals to access internal network resources remotely over the network. It also provides a mechanism to provide support for applications and software remotely. Like any remote connection, they must be carefully managed and secured.

This procedure provides guidelines, standards, and steps required to request, establish, retain, and effectively manage a Virtual Private Network (VPN) connection to the District network.

Only individuals with demonstrated need and manager approval will be considered for VPN usage. VPN may be granted for a District employee, or in limited circumstances, a non-employee, with a college business related need for access. To be considered for access through VPN:

I. **Connection/Access Protocols, User Responsibility, and General Guidelines:**
   - **a.** User Responsibility:
     1. Select an Internet Service Provider (ISP), coordinating installation, installing software, and paying associated fees.
     2. Ensure no other individual accesses their assigned VPN account.
     3. Must utilize District-issued equipment to access VPN network; exceptions may be granted by Superintendent/President. Users with an equipment-exception must acknowledge that their equipment are a de-facto extension of the District's network and are subject to the same rules and regulations that apply to all District-owned computer equipment.
     4. Acknowledge, understand, and comply with Appropriate Use of Technology policy and applicable District procedures.
     5. Understand and acknowledge that VPN access may be granted, rescinded, revoked, or denied at the District's discretion.
   - **b.** Connection/Access Protocols and General Guidelines:
     1. All devices connected to the District network via VPN must use up-to-date antivirus software. VPN connections on devices where antivirus software is not available will not be permitted.
     2. VPN use is controlled using password authentication.
     3. When actively connected to the college network, VPN will direct all traffic to and from the equipment through the VPN portal.
     4. Dual or split tunneling is not permitted.
     5. All VPN gateways are managed by District IT.
     6. VPN requests or access shall not constitute a District obligation to provide equipment or purchase new equipment.

II. Requests and Process

a. Requests must be initiated by a District manager via the VPN Access Request Form.

   1. Requests shall include, but is not limited to, the following:

      1. The reason for requesting VPN access and the anticipated duration of the need.
      2. The name of the individual needing VPN access.
      3. The best contact phone and email address of the individual.

b. Requests must be approved by the Vice President.

c. Information Technology (IT) will review the request.

d. Executive Cabinet will approve/deny request.

e. If approved, IT will process VPN request. If not approved, area Vice President will communicate with requesting manager.

III. Review/Renewal

a. VPN access will not automatically be granted nor renewed.

b. By May 31st, IT will review all VPN accounts.
and will make a recommendation for renewal/non-renewal to Executive Cabinet.

c. Executive Cabinet will evaluate all VPN accounts to determine feasibility of continued access.

d. Once determined, area Vice President will communicate with requesting manager of those not being renewed

Administrator: VP Administrative Services

Executive Cabinet Review/Approval: April 11, 2023
College Planning Council Review/Approval, 1st Reading: April 28, 2023
College Planning Council Review/Approval, 2nd Reading: May 12, 2023
Board Meeting/Information Item: June 15, 2023
Next Review: July 2028