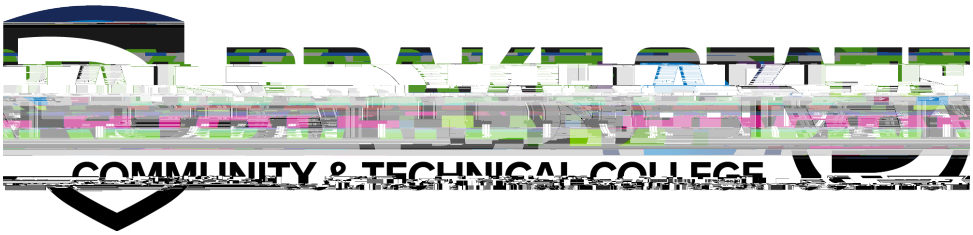

Virtual Private Network (VPN) Policy

1.0 Purpose

The purpose of this policy is to provide guidelines for Remote Access Network (VPN) connections to the Drake State Community and Technical College enterprise network.

As a general rule, remote access is not provided to Drake State employees. Remote access will only be allowed with the consent of the employee's manager and the Information Technologies Department.

2.0 Scope

This policy applies to all Drake State Community and Technical College employees, contractors, consultants, temporaries, and other workers including all personnel affiliated with third parties utilizing VPNs to access the Drake State network.

3.0 Policy

Approved Drake State employees and authorized third parties (customers, vendors, etc.) may utilize the benefits of VPNs, which are a "user managed" service. This means that the user is responsible for selecting an Internet Service Provider (ISP), coordinating installation, installing any required software, and paying associated fees. Further details may be found in the Remote Access Policy.

Additionally,

1. It is the responsibility of employees with VPN privileges to ensure that unauthorized users are not allowed access to Drake State Community and Technical College internal networks.
2. VPN use is to be controlled using either a one-time password authentication such as a token device or a public/private key system with a strong passphrase in addition to multifactor authentication
3. When actively connected to the corporate network, VPNs will force all traffic to and from the PC over the VPN tunnel: all other traffic will be dropped.
4. Dual (split) tunneling is NOT permitted; only one network connection is allowed.
5. VPN gateways will be set up and managed by the Drake State Community and Technical College Information Technologies department.

6. All computers connected to Drake State's internal networks via VPN or any other technology must use the most up-to-date anti-