DRAKE STATE
COMMUNITY & TECHNICAL COLLEGE

Remote Access Policy

1.0 Purpose
The purpose of this policy is to define standards for connecting to Drake State Community and Technical College's network from any host. These standards are designed to minimize the potential exposure to Drake State from damages which may result from unauthorized use of DSCTC resources. Damages include the loss of sensitive or company confidential data, intellectual property, damage to public image, damage to critical Drake State internal systems, etc.

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 employees, contractors, vendors and agents with a Drake State-owned or personally-owned computer or workstation used to connect to the Drake State network. This policy applies to remote access connections used to do work on behalf of DSCTC, including reading or sending email and viewing intranet web resources.

Remote access implementations that are covered by this policy include, but are not limited to, dial-in modems, frame relay, ISDN, DSL, VPN, SSH, and cable modems, etc.

3.0 Policy
3.1 General
1. It is the responsibility of Drake State employees, contractors, vendors and agents with remote access privileges to Drake State Community and Technical College's enterprise network to ensure that their remote access connection is given the same consideration as the user's on-site connection to Drake State Community and Technical College.
2. The Drake State employee is responsible to ensure family members does not violate any DSCTC policies, does not perform illegal activities, and does not use the access for outside business interests while remote access is active. The DSCTC employee bears responsibility for the consequences should the access be misused.
3. Please review the following policies for details of protecting information when accessing the corporate network via remote access methods, and acceptable use of the DSCTC network:
    a. *Virtual Private Network (VPN) Policy*

b. *Computer/Technology Usage Agreement or Acceptable Use Policy*
c. *CHANCELLOR'S PROCEDURES FOR POLICY 223.01 Information Security (INFOSEC)*

3.2 Requirements

1. Secure remote access must be strictly controlled.
2. At no time should any Drake State employee provide their login or email password to anyone, not even family members.
3. Drake State employees and contractors with remote access privileges must ensure that their DSCTC-owned or personal computer or workstation, which is remotely connected to DSCTC's enterprise network, is not connected to any other network at the same time, with the exception of personal networks that are under the complete control of the user.
4. Drake State employees and contractors with remote access privileges to DSCTC 's corporate network must not use non- DSCTC email accounts (i.e., Hotmail, Yahoo, Gmail), or other external resources to conduct DSCTC business, thereby ensuring that official business is never confused with personal business.
5. Reconfiguration of a home user's equipment for the purpose of split-tunneling or dual homing is not permitted at any time.
6. Non-standard hardware configurations must be approved by DSCTC IT.
7. All hosts that are connected to Drake State internal networks via remote access technologies must use the most up-to-date anti-virus, this includes personal computers.
8. All home wireless infrastructure devices that provide direct access to a DSCTC network, such as those behind a VPN, must adhere to the following:
    a. Enable WiFi Protected Access Pre-shared Key (WPA-PSK), EAP-FAST, PEAP, or EAP-TLS
    b. Disable broadcast of home wireless SSID
    c. Change the default SSID name
    d. Change the default login and password
9. Personal equipment that is used to connect to DSCTC's networks must meet the requirements of DSCTC-owned equipment for remote access.
10. Organizations or individuals who wish to implement non-standard Remote Access solutions to the Drake State network must obtain prior approval from DSCTC IT.

4.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.