NAME: Remote Network Access
ISSUING DEPARTMENT Campus Technologies
ISSUED DATE: July 2015
REVIEWED DATE:
APPROVING AUTHORITY: President
DATE REVISED:

DEFINITION

Remote network access involves setting up a secure conversation, called a virtual private network (VPN) connection, between the remote computer and a special gateway device that allows access to the university network over the Internet. Access is granted using university credentials, authenticated through Active Directory.

The client software that initiates the VPN connection will provide an encrypted connection between the user and the University network, so activity over this connection is secure and private. By utilizing the public Internet for data transport, VPN provides a low cost solution for users to connect remotely. In effect, this allows members of the University community to access the Mansfield network resources as if they were on campus.

PURPOSE

This remote access policy is designed to prevent damage to the University network or computer systems and to prevent compromise or loss of data. It is the intention of this policy to define standards and outline acceptable safeguards for use of privately owned and/or remote devices accessing Mansfield University's network. A privately-owned device is one that is not owned by the University, but still requires access to the University network and/or resources. These standards are designed to minimize the potential exposure to Mansfield University from damages which may result from unauthorized use of University resources.

Personnel engaged in activity that requires remote access should adhere to the guidelines outlined below. The VPN software will be programmed to query the connecting device to ensure that the virus software definitions are up-to-date as well as patches for the Microsoft operating system. Users should also take care when accessing sensitive data from public networks. Violations of the remote access guidelines will result in escalating repercussions:

1st violation – user will be cautioned and educated as to proper remote access procedure.

2nd violation – remote access will be subject to revocation.

3rd violation – user will be referred to Human Resources for discipline, up to and including suspension or termination of employment.