Virtual Private Network (VPN) Policy

Virtual Private Network (VPN) Policy

In an effort to increase the security of Wright State University's information technology systems Computing and Telecommunications Services (CaTS) provides Virtual Private Network (VPN) services to the University community. The VPN offers secure access for faculty/staff/students/consultants (clients) who need access to information technology systems that are not otherwise available to clients from off-campus or on-campus (wireless) networks.

I. Purpose

The purpose of this policy is to provide guidelines for VPN connections to Wright State University's internal network. Wright State's VPN service is designed to provide secure/encrypted access to network resources on the Wright State Network. Using the VPN server to access Internet resources external to Wright State is not recommended.

II. Policy

VPN gateways will be set up and managed only by Wright State University CaTS.

Only VPN software that is approved by and/or distributed by CaTS may be used to connect to the Wright State University VPN servers.

Faculty and Staff are granted general VPN access. Additional approval is required for access to sensitive systems. Students are granted access upon request. VPN applications will be available for the management of equipment and servers, access to departmental managed computers and access to internal information resources. If additional access is required beyond general access privileges, please contact the Help Desk at helpdesk@wright.edu.

By using VPN technology with personal equipment, users must understand that their machines are a de facto extension of Wright State University's network, and as such must comply with Wright State University's Information Technology Policies.

All computers connected to Wright State University's internal networks via VPN or any other technology must use the most up-to-date anti-virus, anti-spyware, operating system patches, and firewall software. Sponsored third parties such as software consultants or vendor support personnel, can gain access to campus systems using the VPN. A Wright State University employee must sponsor the application by the third party. In addition, the third party must complete and sign an agreement with Wright State University. Employees needing the necessary forms may contact the CaTS Help Desk at 937-775-4827.

It is the responsibility of the users with VPN privileges to ensure that unauthorized persons are not allowed access to Wright State University internal networks.

The VPN connection provides secure access into the Wright State Network. VPN does not, by itself, provide Internet connectivity. When off campus, users are responsible for providing their own Internet service in order to use Wright State's VPN service.

VPN users will be automatically disconnected from Wright State University's network after thirty minutes of inactivity. The user must then log on again to reconnect to the network. Artificial network processes should not be used to keep the connection open.

Only one active VPN connection is allowed per user and the VPN concentrator is limited to a total connection time of 8 hours per user in one session.

The VPN client is currently available for Windows 2000/XP/Vista and Mac OS X. Approved users are responsible for the installation of the VPN software.

Wright State University has configured the VPN service to not allow the bridging of networks (split tunneling). Communication back to a device on the private network other than the computer making the original connection is not allowed.

III. Enforcement
Any user found to have violated this policy may be subject to loss of certain privileges or services, including but not necessarily limited to loss of VPN services.