1.0 Introduction

In an effort to increase the security of Baylor University's information technology systems, off campus access to many information technology resources has been limited. Baylor University offers Virtual Private Network (VPN) access for faculty/staff/consultants (hereinafter users) who need access to information technology systems that are not available to users from off-campus networks. Exceptions to the approved list of users will be considered on a case by case basis.

2.0 Purpose

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

3.0 Policy

3.1 VPN gateways will be set up and managed only by Baylor University ITS Networking Services Group.

3.2 Approved users can download the VPN client and installation instructions from the VPN page at https://www.baylor.edu/its/index.php?id=957861.

3.3 Only VPN client software that is approved by and/or distributed by ITS networking services may be used to connect to the Baylor University VPN concentrators.

3.4 By using VPN technology with personal equipment, users must understand that their machines are a de facto extension of Baylor University's network, and as such must comply with Baylor University's Information Technology Policies https://www.baylor.edu/its/index.php?id=40538.

3.5 Baylor University ITS has created a VPN application for sponsored third parties such as software consultants or support personnel, to gain VPN access to support on campus systems. A Baylor University employee must sponsor the application by the third party. In addition, the third party must complete and sign a non-disclosure agreement with Baylor University. Employees needing the necessary forms may contact the Helpline x4357.

3.6 VPN provides secure access into the Baylor Network. VPN does not, by itself, provide Internet connectivity. Users
are responsible for providing their own Internet service via cable modem, DSL, or other means to be able to use Baylor’s VPN service.

3.7 Currently VPN software is available for Windows 7, 8, 10 and Mac OS X. Approved users are responsible for the installation of the VPN software.

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

3.9 Baylor University has configured the VPN service to not allow the bridging of networks (split tunneling). As a result, when connected to VPN, all network traffic from the users computer will travel through the Baylor University network which will not allow communication back to a device on the private network other then the computer making the original connection.

3.10 All computers, including personal computers, connected to Baylor University’s internal networks via VPN or any other technology must use the most up-to-date anti-virus software approved by the University.

3.11 VPN users will be automatically disconnected from Baylor University's network after thirty minutes of inactivity. The user must then logon again to reconnect to the network. Pings or other artificial network processes should not be used to keep the connection open.

3.12 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.

4.0 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.

Last updated 1/2/19