Virtual Private Network/Remote Access Policy

Purpose
The purpose of this policy is to provide guidelines and define standards for remote access, IPSec and L2TP Virtual Private Network (VPN) connections to Texas Woman’s University (TWU) funded networks. These standards are designed to minimize the potential exposure to TWU from damages which may result from unauthorized use of TWU resources. Damages include the loss of sensitive or University confidential data, intellectual property, damage to public image, damage to critical TWU internal systems, etc.

Scope
This policy applies to all TWU employees, contractors, consultants, temporaries, and other workers, including all personnel affiliated with third parties utilizing VPNs to access TWU networks with TWU owned or personally-owned computers. This policy applies to implementations of VPN that are directed through a VPN Concentrator to do work on behalf of TWU including, but not limited to, reading or sending email and viewing intranet web resources.

Policy

General
1. Approved TWU 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.

2. It is the responsibility of TWU employees, contractors, vendors and agents with VPN privileges to TWU networks to ensure that their remote access connection is given the same consideration as the user's on-site connection to TWU.

3. Please review the Computer and Software Use Policy (Policy #9.01) for details regarding acceptable use of TWU information resources.

Requirements
1. It is the responsibility of employees with VPN privileges to ensure that unauthorized users are not allowed access to TWU internal networks.

2. At no time should any TWU employee provide their login or email password to anyone, not even family members.

3. TWU employees and contractors with VPN privileges to TWU networks must not use non-TWU email accounts (i.e.: Hotmail, Yahoo, AOL), or other external resources to conduct TWU business, thereby ensuring that official business is never confused with personal business.

4. When actively connected to TWU’s network, the VPN connection will force all traffic to and from the PC over the VPN tunnel; all other traffic will be dropped.

5. Dual (split) tunneling is NOT permitted; only one network connection is allowed. If non-work related network access is needed, first disconnect the VPN connection.

6. All computers connected to TWU internal networks via VPN must use the most up-to-date antivirus software that is the University standard (http://norton.twu.edu); this includes personal computers.
7. VPN users will be automatically disconnected from TWU's network after thirty minutes of inactivity. The user must then logon again to reconnect to the network. Pings or other artificial network processes are not to be used to keep the connection open.

8. The VPN concentrator is limited to an absolute connection time of 24 hours.

9. Users of computers that are not TWU-owned equipment must configure the equipment to comply with TWU's VPN and Network policies.

10. The only VPN client software supported is Cisco's VPN client v4.03A and above. A copy may be obtained from the 'VPN' section located under 'My Tools' in your portal. You will have access to this link after this request has been approved.

11. By using VPN technology with personal equipment, users must understand that their machines are a de facto extension of TWU's network and as such are subject to the same rules and regulations that apply to TWU-owned equipment, i.e.: their machines must be configured to comply with University security policies.

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

**Definitions**

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remote Access</td>
<td>Any access to TWU's network through a non-TWU controlled network, device, or medium.</td>
</tr>
<tr>
<td>IPSec</td>
<td>Short for IP Security, a set of protocols developed by the Internet Engineering Task Force (IETF) to support secure, encrypted exchange of packets at the IP layer.</td>
</tr>
<tr>
<td>L2TP</td>
<td>Short for Layer 2 Tunneling Protocol, a protocol that establishes a point-to-point connection (tunnel) through the internet.</td>
</tr>
<tr>
<td>VPN</td>
<td>A Virtual Private Network is a method for accessing a remote network (TWU network) via an encrypted tunnel through the Internet.</td>
</tr>
<tr>
<td>VPN Concentrator</td>
<td>An Information Service managed device that negotiates and manages VPN connections (tunnels) between a remote host and TWU's internal networks.</td>
</tr>
<tr>
<td>Dual (Split) tunneling</td>
<td>Simultaneous direct access to a VPN connection and a non-TWU network (such as the Internet, or a home network) from a remote host in order to bypass the VPN tunnel.</td>
</tr>
</tbody>
</table>