Improve the Security of University Data Assets by Restricting Access via Virtual Private Network

Executive Summary Contact: Henry Torres, (870) 972-3033

Background:

- The Security Task Force recognizes the importance of maintaining the integrity and security of ASU technology assets. VPN access to the ASU-J computer network is currently open to all Faculty/Staff. When connected to VPN, computers have direct access to the network without going through the external firewall. This unrestricted access to the network could increase its exposure to viruses, malware, and could allow hackers using compromised accounts greater access to the University's network.

Summary:

- users who don't access VPN in 12 months will be removed
- Chair/Dean/Dept. Head approval will be required for access
- Devices failing security scan may be denied VPN access

Consequences:

- Failure to secure approval will result in termination of VPN privileges
- Inactivity of 12 months will result in termination of the VPN account

VPN Access Procedure

VPN access allows users unrestricted to access the Arkansas State University computer network from locations external to the Jonesboro campus. This unrestricted access to the network could increase the University's exposure to viruses, malware, and could allow hackers using compromised accounts greater access to the ASU network.

In light of the above, ASU has adopted the following procedures for VPN access:

- Remove users who haven't accessed VPN in the past 12 months from the data this procedure is approved
- Chair/Dean/Dept. Head approval for all remaining accounts
- Chair/Dean/Dept. Head approval for all new access
- 12 month renewal of access approval
- Connections must support Layer 2 Tunneling Protocol (L2TP) as a minimum standard
- Access may be suspended/terminated by ITS at anytime if access could cause security issue
- VPN access is logged and the logs will be retained for 5 years
- Logging may include connection/disconnection times, IP address received from DHCP, connecting IP address, IP address(es) accessed, username that opened the connection
- ITS may require devices connecting via VPN to be scanned for patch levels of OS/software, current antivirus software, or other security related issue. Users can check/download updates for their operating system by clicking on Windows Update in the Control Panel for Windows based machines and Software Updates under System Preferences on iOS based machines.
- Devices failing security scan may be denied VPN access