Virtual Private Network Guidelines

Virtual Private Networks (VPN) allow a remote user to connect to the Sul Ross network and have the same or similar experience they would have if they were on one of our campuses and connected directly to a network port or the wireless system. Due to the risk associated with this kind of access, certain technology items must be in place before a user is allowed to access the institution's VPN.

1. Only state-owned assets, desktops, laptops and tablets, are permitted to connect to the institution's VPN. No personal devices are permitted to connect to the network via this method nor are they allowed to connect to services that are not already available through the internet.
2. Any asset that connects to the VPN must have updated security software installed with a valid and up to date license. This prevents the introduction of malware or other unwanted programs into the Sul Ross State University environment.
3. An Operating System (OS) with a valid and up to date license is required to connect to the VPN. This is an issue that is at the discretion of the CIO/ISO and the Information Security team. If the asset you intend to connect to VPN does not meet this requirement, OIT will assist to update the asset.
4. A special account is to be used for this access. Your regular LoboID will not allow you to connect to VPN. If you need an account to connect to VPN and the previous three requirements have been met, OIT will create the specific account and password for you. Please be aware these special VPN accounts have a different password expiration date than normal AD accounts. You are expected to keep this password changed frequently and use complex and lengthy passwords for this account.
5. Coming Soon: the use of a VPN account at Sul Ross State University requires Two Factor Authentication (2FA) using an approved multi-factor engine.