WGTC 1.7

Virtual Private Network (VPN)

Purpose

The purpose of this policy is to provide guidelines for Remote Access Virtual Private Network (VPN) connections to the West Georgia Technical College network.

Definition and Scope

A Virtual Private Network (VPN), is defined as the process of encryption and tunneling to connect users over a public network, usually the Internet. This policy applies to all WGTC employees, contractors, consultants, and other workers including all personnel affiliated with third parties utilizing VPNs to access the WGTC network. This policy applies to implementations of VPN that allow direct access to the WGTC secured network from outside the WGTC secured network.

Policy

Requests to use the VPN must be approved by employee's supervisor and the Director of Information Technology. Approved WGTC 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, and installing any required software.

1. The VPN is an IP only resource. Other protocols are not supported.
2. Users accounts will be created only at the request of a user's supervisor or manager (WGTC employee), or departmental representative (contractors, consultants, and vendors) by submitting the appropriate VPN Access Request form. Additionally, the user must have read and understood this policy before using the VPN service.
3. Accounts for non-WGTC personnel (customers, vendors, etc.) must be approved by the Director of Information Technology. Additionally, a copy of the VPN Request Form (including VPN Policy, and the confidentiality agreement) must be signed by the designated company Approving Authority and filed. Accounts will not be issued until this process has been completed.
4. It is the responsibility of the employee or company with VPN privileges to ensure that unauthorized users are not allowed access to WGTC secured networks.
5. VPN access is controlled using ID and password authentication. For West

Georgia Technical College employees, the ID must be in the form of their network ID. The password must comply with the WGTC Computer and Internet Use Policy. Additionally, the user is responsible for maintaining the security of their id and password.

6. All users are subject to auditing at any time as requested by the Director of Information Technology or the State Security Officer.
7. When actively connected to the WGTC secured network, the VPN will force all traffic to and from the remote node through the VPN tunnel. To prevent potential 'back-doors' to the network dual (split) tunneling is NOT permitted. Only one network connection is allowed.
8. WGTC secured network access for non-WGTC personnel will be limited to the resources to which they need access. Open access for these accounts will not be permitted.
9. All VPN gateways will be set up and managed by WGTC Information Technology Department. User created VPN gateways will not be permitted on the secured network.
10. All computers connected to WGTC secured networks via VPN must use up- to-date virus-scanning software with the virus definitions. Additionally, all relevant security patches must be installed; this includes personal computers.
11. VPN users will be automatically disconnected from the WGTC network after thirty minutes of inactivity. The user must then logon again to reconnect to the network. Artificial network processes are not to be used to keep the connection open. User connections to the VPN will be limited to an absolute connection time of eight (8) hours per day.
12. Users of computers that are not the property of WGTC must configure the equipment to comply with the WGTC VPN policy and/or desktop security policy, whichever is applicable to the device. By using VPN technology with personal equipment, users must understand that their machines are a de facto extension of the WGTC network, and as such are subject to the same rules and regulations that apply to WGTC owned equipment, i.e., their machines must be configured to comply with all WGTC security policies. If the network is compromised, the users are subject to the search and seizure policy.
13. Only WGTC approved VPN clients may be used.
14. Users of this service are responsible for the procurement and cost associated with acquiring basic Internet connectivity, and any associated service issues.
15. The WGTC Information Technology Department does not have a time reserved for regularly scheduled maintenance. Emergency downtime will be scheduled as needed.

Enforcement

This policy regulates the use of all VPN services to the WGTC secured network. To maintain security, VPN services will be terminated immediately if any suspicious activity is found. Service may also be disabled until the issue has been identified and resolved. Any West Georgia Technical College employee found to have intentionally violated this policy might be subject to disciplinary action. Non-WGTC employees and vendors are directly responsible for

damage as a direct result of policy violation. Intentional and non-intentional violation will result in termination of service and may result in revocation of contract.

Policy Source: West Georgia Technical College	Policy Manager: Director, Information Technology	Effective: 3/2009
Division: Information Technology	Reviewed: 9/2021 Revised: 9/2021	