Gaston College

Virtual Private Network (VPN) Policy

1.0 Purpose

The purpose of this policy is to define standards for connecting to Gaston College's network from a external host. These standards are designed to minimize the potential exposure to Gaston College from damages which may result from unauthorized use of Gaston College resources. Damages include the loss of sensitive or college confidential data, damage to public image, damage to critical Gaston College internal systems, etc. This policy is to provide guidelines for Virtual Private Network (VPN) connections to the Gaston College network.

2.0 Scope

This policy applies to all Gaston College employees, contractors, vendors and agents with a Gaston College-owned or personally-owned computer or workstation used to connect to the Gaston College network. This policy applies to remote access connections used to do work on behalf of Gaston College. This policy applies to implementations of VPN that are directed through an IPSec Concentrator.

3.0 Policy

Approved Gaston College employees and authorized third parties (customers, vendors, etc.) may utilize the benefits of VPNs, under the following condition.

3.1 General

1. It is the responsibility of employees with VPN privileges to ensure that unauthorized users are not allowed access to Gaston College internal networks.
2. When actively connected to the corporate network, VPNs will force all traffic to and from the PC over the VPN tunnel: all other traffic will be dropped.
3. Dual (split) tunneling is NOT permitted; only one network connection is allowed.
4. VPN gateways will be set up and managed by Gaston College network operational groups.
5. All computers connected to Gaston College internal networks via VPN or any other technology must use the most up-to-date anti-virus software that is the corporate standard (provide URL to this software); this includes personal computers.
6. VPN users will be automatically disconnected from Gaston College'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.
7. The VPN concentrator is limited to an absolute connection time of 24 hours.
8. Users of computers that are not Gaston College-owned equipment must configure the equipment to comply with Gaston College's VPN and Network policies.
9. Only InfoSec-approved VPN clients may be used.
10. By using VPN technology with personal equipment, users must understand that their machines are a de facto extension of Gaston College's network, and as such are subject to the same rules and regulations that apply to Gaston College-owned equipment, i.e., their machines must be configured to comply with InfoSec's Security Policies.

Gaston College * 201 Highway 321 South * Dallas, NC 28034 * Phone: 704-922-6420 Fax: 704-922-8923 * www.gaston.edu

3.2 Requirements

1. Secure remote access must be strictly controlled. Control will be enforced via strong password authentication.
2. At no time should any Gaston College employee provide their login password to anyone, not even family members.
3. Gaston College employees and contractors with remote access privileges must ensure that their Gaston College-owned or personal computer or workstation, which is remotely connected to Gaston College's network, is not connected to any other network at the same time, with the exception of personal networks that are under the complete control of the user.
4. Gaston College employees and contractors with remote access privileges to Gaston College's network must not use non-Gaston College email accounts (i.e., Hotmail, Yahoo, AOL), or other external resources to conduct Gaston College business, thereby ensuring that official business is never confused with personal business.
5. Reconfiguration of a home user's equipment for the purpose of split-tunneling or dual homing is not permitted at any time.
6. All hosts that are connected to Gaston College internal networks via remote access technologies must use the most up-to-date anti-virus software (Command Anti-virus), this includes personal computers.
7. Personal equipment that is used to connect to Gaston College's networks must meet the requirements of Gaston College-owned equipment for remote access.

4.0 Enforcement

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

5.0 Definitions

Term	Definition
IPSec Concentrator	A device in which VPN connections are terminated.
InfoSec	Information Security

Gaston College * 201 Highway 321 South * Dallas, NC 28034 * Phone: 704-922-6420 Fax: 704-922-8923 * www.gaston.edu

GASTON COLLEGE

Virtual Private Network (VPN) Request Form

REQUESTOR INFORMATION

Name: _____

Department: _____

E-mail: _____ Phone Number: _____

Duration of Access: _____ Date of Request: _____

Purpose of Access (Please be as detailed as possible): What Resources do you need access to?

GENERAL RULES

It is critical that your computer has the most recent security patches for your operating system(s). Contact Technology Services or visit https://update.microsoft.com for windows OS or https://www.apple.com/support/dwonloads/ for MAC OS)

Make sure that your computer has been checked for spyware (i.e. Mcafee anti-spyware, Spybot search and destroy, adaware etc.)

Please provide the information requested below. This information is needed for approval by Technology Services.

Type of device: ☐ Personal ☐ College-Owned

☐ Laptop ☐ Desktop ☐ Tablet

Operating System: ☐ MAC ☐ Windows ☐ Other _____

Version of Operating System (i.e. Windows 7, 10, etc.): _____

Antivirus Vendor: _____

If you need assistance insuring that your computer meets the above requirements, please contact Technology Services at 704-922-6420.

Remember, each member of the Gaston College VPN plays an important role in maintaining the security and confidentiality of all Gaston College records.

I certify that the computer I use to connect via VPN has the most recent operating system updates, has been checked for spyware, and has a regularly updated anti-virus package installed and I will continue to keep these items maintained. I understand that the same Gaston College Acceptable Use Policy applies to this service.

_____ _____

Signature of Requestor / User *Date*

_____ _____

Print Name of Requestor / User *Email*

_____ _____

Signature of Supervisor *Date*

_____ _____

Print Name of Supervisor *Email*

Information below to be completed by Network Services

VPN ID: _____

Completed By (Print Name) : _____

Completel By (Signature) : _____ Date: _____

Department of Technology Services